GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at http://www.giac.org/registration/gsna

GIAC Auditing Networks, Perimeters, and Systems
GSNA Practical Assignment
Version 2.0

Mark Kimball

© SANS Institute 2000 - 2002, Author retains full rights.

Auditing an NFR Security NID 200 Intrusion Detection System: An Auditor's Perspective 4
Assignment One – Research in Audit, Measurement Practice, and Control 4
Identify the System to be Audited 4
Evaluate the Risk to the System 4
Current State of the Practice 5
How Can Current Methods and Techniques be Improved 6
Assignment Two – Create an Audit Checklist 6
Local Access 6
Local Console Authentication (Password Checking) 6
Reference 6
Control Objective 6
Risk 6
Compliance 6
Testing 7
Objective/Subjective 7
Assigning an IP Address to the Monitor Interface 7
Reference 7
Control Objective 7
Risk 7
Compliance 7
Testing 8
Objective/Subjective 8
Master Administrator Password Bounds Checking 8
Reference 8
Control Objective 8
Risk 8
Compliance 8
Testing 8
Objective/Subjective 8
CD-ROM Removable during Operation 8
Reference 8
Control Objective 9
Risk 9
Compliance 9
Testing 9
Objective/Subjective 9
Power Supply Interruption 9

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reference 9
Control Objective 9
Risk 9
Compliance 9
Testing 9
Objective/Subjective 10
Remote System Access 10
User Management - Forced Password Change after Install 10
Reference 10
Control Objective 10
Risk 10
Compliance 10
Testing 10
Objective/Subjective 10
User Management – Password Length/Complexity on Default NFR Account 10
Reference 10
Control Objective 10
Risk 10
Compliance 11
Testing 11
Objective/Subjective 11
User Management – Password Length/Complexity on New User Account 11
Reference 11
Control Objective 11
Risk 11
Compliance 12
Testing 12
Objective/Subjective 12
User Management – Superfluous User Accounts 12
Reference 12
Control Objective 12
Risk 12
Compliance 12
Testing 12
Objective/Subjective 13
User Management – User Permissions 13
Reference 13
Control Objective 13
Risk 13
Compliance 13
Testing 13
Objective/Subjective 13
User Management - Change Password Feature on Edit Menu 13
Reference 13
Control Objective 13
Risk 13
Compliance 14
Testing 14
Objective/Subjective 14
Security of Remote Management Communications Channel 14
Reference 14
Control Objective 14
Risk 14
Compliance 14
Testing 14
Objective/Subjective 15
Test Isolation of Management Network 15
Reference 15
Control Objective 15
Risk 15
Compliance 15

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Testing 15
Objective/Subjective 16
Implementation of Internet Connection for Management Station 16
Reference 16
Control Objective 16
Risk 16
Compliance 16
Testing 17
Objective/Subjective 17
Sensor Monitor Interface Detectability 17
Reference 17
Control Objective 17
Risk 17
Compliance 17
Testing 18
Objective/Subjective 18
Susceptibility to Denial of Service (DoS) Attack 18
Reference 18
Control Objective 18
Risk 18
Compliance 18
Testing 18
Objective/Subjective 18
Sensor Management Interface Open Ports 18
Reference 18
Control Objective 18
Risk 19
Compliance 19
Testing 19
Objective/Subjective 19
Sensor and Management Station Patches Up-to-Date 19
Reference 19
Control Objective 19
Risk 19
Compliance 19
Testing 19
Objective/Subjective 19
Package Updater Automatically Updates Signatures 19
Reference 19
Control Objective 19
Risk 20
Compliance 20
Testing 20
Objective/Subjective 20
Assignment Three – Conduct the Audit 20
Checklist Item 1 – Local Console Authentication 20
Checklist Item 2 – IP Address on Monitor Interface 20
Checklist Item 3 – Eject CD-ROM During System Operation 20
Checklist Item 4 – Default NFR Account Password 21
Checklist Item 5 – Security of Remote Communications Channel 21
Checklist Item 6 – Test Isolation of Management Network 61
Ping Sweep Results 61
Checklist Item 7 – Unnecessary User Accounts 62
Checklist Item 8 – Sensor Management Interface Open Ports 62
Checklist Item 9 – Sensor Monitor Interface Detectability 63
MAC Addresses 64
Subnet 172.16.0.0\255.255.0.0 64
MAC Addresses 64
Subnet 192.168.4.0\255.255.255.0 64
Checklist Item 10 – Forced Administrator Password Change After Install 65
Is the System Securable? (Evaluate the System) 65

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Is the System Auditable? (Evaluate the Audit) 65
Assignment Four – Follow Up 66
Executive Summary 66
Audit Findings 66
Background/Risk 67
Audit Recommendations 67
Costs 68
Compensating Control 68
References 68

Auditing an NFR Security NID 200 Intrusion Detection System: An Auditor's Perspective

Assignment One – Research in Audit, Measurement Practice, and Control

Identify the System to be Audited

This paper describes an audit for an NFR Security NID 200 intrusion detection system. The NFR Security NID 200 sensor is a dedicated network intrusion detection appliance. The NFR NID 200 consists of dual Pentium III 800MHz processors, 512MB of memory, two Intel EtherExpress Pro/100 NIC cards, a Toshiba 42x IDE CD-ROM drive, two 40GB EIDE hard drives, a 1.44MB floppy disk drive, and a PCI video card. The underlying system software is a hardened version of the OpenBSD UNIX operating system with a proprietary user interface and a customized libpcap packet capture driver.

You manage the NID 200 sensor through the NFR Administration Interface, or AI. The minimum system requirements for the Administration Interface are a Windows 2000, Windows NT 4.0 Client, or Windows NT 4.0 Server system.

This audit examines an NFR NID 200 sensor running Version 1.2 of the sensor software and Version 2.1.0 (Build 141) of the Administration Interface running on a Microsoft Windows 2000 client.

The NFR NID 200 intrusion detection system is designed to detect network-based attacks against an organization. In general terms a network intrusion detection system is a system with at least one network interface set in promiscuous mode, like a sniffer. The system captures all packets on the media to which it is attached and examines the packet payload or the packet header or both for strings or patterns that match entries in a database of known attack signatures.

When the system detects a match, it writes the entry to a log file and to the main system management console for human inspection, analysis, and action. You can configure the system to respond automatically to an intrusion event, although it is usually not enabled by default.
The NFR NID 200 intrusion detection system that we used for this audit is physically outside a simulated corporate firewall. The monitoring interface faces a simulated public Internet, while the management interface terminates in a physically isolated internal subnet inside the private network. The monitoring interface has no IP address assigned to it. The automated response functionality for the system is not enabled.

Evaluate the Risk to the System

The risks associated with this type of intrusion detection system are manifold:
First, the system itself can be compromised and used as a stepping-stone into a protected network. Because the system has a public-facing interface, it is not protected by any of the normal protective network devices, such as a packet filtering router, or firewall. The IDS is subject to all kinds of direct attacks from the outside.
Moreover, the system has a second network interface, the management interface, which is used to interrogate the operational status of the system and to receive alerts from the sensor. If the management system/console is directly on the main, internal, private network, an attacker who compromises the IDS can completely circumvent perimeter protections, such as firewalls. However, as we will see, steps have been taken to mitigate the risk of external attack, so while the consequences of such a security breach would be serious, the likelihood of it happening are very low.
The second major concern is this: If the IDS is compromised, its alerting functionality can be disabled. If the IDS's

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

alerting capability is disabled or somehow compromised, system management personnel may not be alerted to attacks that are launched against the organization's perimeter devices or internal network.
In the worst-case scenario, the IDS can be attacked, compromised, its intrusion alerting functionality disabled, and the system used as a stepping-stone into the organization's internal network.
In the case of the NFR Security NID 200, the system is very well protected against attacks that would allow the system to be taken over and used as a launch pad for further attacks.
First, the system runs from a CD-ROM that contains the operating system and application software. This means that the contents of the CD are loaded directly into system memory at boot time, and the operating system runs directly from system memory. Operating system data structures, configuration data, and processes cannot be permanently modified because the CD is a read-only device.
Second, the monitoring interface has no IP stack loaded, and only passively listens to network traffic. Furthermore, it is impossible to assign an IP address to the NID 200 monitoring interface. Because the monitoring interface does not recognize the TCP/IP protocol, standard IP devices, such as sockets, are not available to support the well-known ports that TCP/IP applications such as telnet, ftp, rlogin, or rsh require.
Finally, in the configuration in which we are auditing the system, the management interface terminates on a system that is on a network segment that is physically isolated from the private network that the IDS is deployed to protect. This is a very important factor in determining risk to the system: If the network on which the management interface and management system reside is not physically isolated from the rest of the private intranet, the consequences of a security breach rise dramatically.
In summary, the NFR Security NID 200 Intrusion Detection System is not very vulnerable to being compromised, taken over, and used as a stepping-stone from which to launch more invasive attacks. The most serious threat is that the system might be knocked out of service, either through a DoS (Denial of Service) attack or a system crash. If this type of attack succeeds, it allows an attacker to initiate attacks without being noticed as quickly, if at all. This scenario is analogous to a burglar or intruder disabling a home security system by cutting the power and phone lines to a house before attempting to break in. If the home security system cannot seize the phone line and dial out to the central monitoring station or police, the intruder stands a much better chance of entering the home undetected. In our opinion, the greatest threat would be from an insider attack launched through the internal network. The system's management interface is easily accessible to anyone who obtains the Administration Interface software and the system password. If an insider were to modify the attack signature recognition configuration so that a single exploit is ignored, he could open up a very small, subtle hole that could make the internal network vulnerable. As we will see, the NID 200 system has poor baseline configuration protection, so it would be difficult for a system administrator to notice the change.

Current State of the Practice

The NFR Security NID 200 intrusion detection system is a fairly recent product. It is a specialized, dedicated, network appliance. It is not very widely deployed compared to general-purpose computer systems, or even more specialized systems like mail servers, routers, DNS servers, or firewalls. For these reasons, the best practices for this device are not well defined. The first source we checked was the NFR Security Web site (nfr.com). The various products the company sells are listed under a link to Products. Under Products, there is a link to Network Intrusion Detection (NID). http://www.nfr.com/products/NID/ contains several documents, including a sales flyer, a system requirements document, a technical overview, a data sheet, and a case study. In addition https://support.nfr.com/nid-200/ contains comprehensive documentation for the product, including a *Getting Started Guide*[1], and a *User's Guide*[2]
The NSS Group (http://www.nss.co.uk/) a European-based, independent security and network testing organization tested the NFR NID 200 for usability and performance. The report, *Intrusion Detection Group Test*[3], does not address security auditing specifically, but provides useful background material that could contribute to developing an auditing checklist. The report is available for download from their web site after filling out a simple questionnaire.

The Information Systems Audit and Control Association (ISACA) has created a very useful set of guidelines, outlined in its publication, *CobiT 3rd Edition Audit Guidelines.*[4] While this publication does not address intrusion detection systems specifically, it does contain some useful information on maintaining the security of, and managing, user accounts. We used some information from section DS5 ENSURE SYSTEM SECURITY for some of the user account issues associated with the system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We used all of these sources to create the Audit Checklist in Assignment Two.

How Can Current Methods and Techniques be Improved

A quick perusal of the major Internet search engines (altavista.com, google.com, etc.) and the major security web sites (sans.org, cis.org, CERT) revealed that there are no audit checklists in existence for this product. Nevertheless, it is very easy to imagine how a comprehensive checklist could be developed for this product. By using the product documentation, in tandem with an audit framework like CobiT, one could assemble a fairly comprehensive checklist with which to audit the system.

Assignment Two – Create an Audit Checklist

The audit checklist is divided into two major parts:

- Local access to the system
- Remote access to the system

You can access the NFR Security NID 200 system in only one of two ways: At the local console, or remotely over a computer network using the Administration Interface (AI). In creating our audit checklist, we will consider each of these access methods separately. Furthermore, we will consider what initial configuration settings an administrator can choose during the installation process that could weaken security or lead to a system compromise.

Local Access

When the NFR product is first installed, one of the requirements for initial installation is the attachment of a local graphical video console. This local video console is only required during installation. You can remove it after you successfully install the system.

This point is important: Normally, you would install such a system in a locked data center or wiring closet, preventing casual physical access by unauthorized individuals. If physical security is still a concern despite these countermeasures, you can remove the means of locally logging on to the system through the main console. You can stop, start, and otherwise control the system through the Administration Interface (AI). If the local system console is left in place, the system can still be password-protected, although as we will see the password mechanism does not enforce long or hard-to-guess, or hard-to-break passwords.

Local Console Authentication (Password Checking)

Reference

CobiT 3rd Edition Audit Guidelines, July 2000.

Control Objective

This item is designed to see whether the system requires difficult to guess or difficult to break passwords, or if the system requires any password at all.

Risk

If the system does not enforce difficult to break passwords, or if it does not require any password at all, it is more likely that the system could be easily compromised. If the system can be easily compromised, intrusion detection capability can be defeated or disabled. If the intrusion detection capability can be defeated or disabled, malicious users can launch attacks or run exploits against the organization's network with less chance of being discovered. If there is less chance of malicious activity being discovered, there is more chance that valuable data can be lost or destroyed, or system resources misused, confidentiality compromised, proprietary information lost, and the organization's reputation tarnished.

Compliance

Compliance for this item is not binary: Password length and complexity enforcement can be quite arbitrary, depending on the organization's policies. One aspect of compliance that **is** binary is whether or not the system requires a password at all.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Aside from requiring **any** kind of password, the risk associated with this item depends on minimum password length and the use of upper case, lower case, numeric, and non-alphanumeric characters.

Testing

Testing for a null password, or minimum password length is quite simple: At the Administration screen on the main console, select Access Administration from the menu. This brings up a screen that contains three fields: Password, Repeat Password, and License Key. To test for a null password, remove all characters from the Password field and press Enter. Do the same for the Repeat Password field. If the system does not print an error message, a null password was accepted. To verify, return to the Status Monitor and type A or Admin to return to the administration screen. You will be prompted immediately for a password. Press the Enter key. If the Administration screen appears, the null password was accepted.

For minimum password/hard-to-guess password enforcement, use the same test methodology above, except using increasingly shorter text strings and common dictionary words until you can determine what the minimum password length is that the system accepts.

Because the system does not require long or hard-to-break passwords, you, as the auditor, must interview the system administrator to ensure that he or she has chosen a sufficiently difficult-to-break password. One should not ask what the password is, but a good test would be to ask if the admin uses upper and lower case characters, numbers, and non-alphanumeric characters. The best that can be done to verify this is to check the length of the password. You can do this by counting the number of asterisks that correspond to characters in the password string that appear in the password input box.

Objective/Subjective

These kinds of tests are somewhat subjective. The result of trying to set a null password, or a short password, or a password that is a dictionary word is easily verifiable, but the system administrator's chosen password cannot be independently verified unless you ask the administrator what the password is, assuming that you can trust the administrator to tell you the truth.

Assigning an IP Address to the Monitor Interface

Reference

The source of this item is from the SANS Institute course [8] on network intrusion detection systems. This is also known as an industry best practice for configuring network intrusion detection systems, and appears in popular text books [5],[6] on the subject.

Control Objective

The objective of this checklist item is to determine whether a user can assign an IP address to the monitoring interface of the NFR NID 200 system.

Risk

If a user is able to assign an IP address to the monitoring interface, this implies that the TCP/IP stack is loaded for that interface. If the TCP/IP stack is loaded for the monitoring interface, the public-facing network interface may be visible to the external, or public, network. If this interface is active, it can be found by scanning, and malicious users can run exploits against it like any other unprotected system. Buffer overflow attacks, brute-force password guessing against applications, and malicious ICMP traffic can all be used to compromise the system. If the system is compromised, it can be used to circumvent perimeter protection, and its intrusion detection capability can be disabled to allow other attacks to proceed against perimeter protection devices.

Compliance

Based on the user interface of the NID 200, this item appears to be binary. Either the system allows the administrator to assign an IP address to the monitoring interface or it does not.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Testing

Type A, for Admin, from the local console terminal. This brings up the local administration interface. Select the **Configure the System** menu item. This displays a page of different system settings. The first of these lets you select which one of the two network interfaces you wish to use as the management interface: FXP0 or FXP1. You can select either one of these interfaces to be the management interface. Once you make this selection, you can then assign an IP address to that interface. There is no way to assign an IP address to the monitor interface.

We could try to verify this by attempting to scan for this interface using a tool like nmap or ping, but this would be pointless as there is nothing to scan or ping. Also, because this is an appliance, the administrator cannot access the underlying operating system. You cannot gain access to a shell or command prompt to issue a standard UNIX network operating system command, such as **ifconfig**, to see if the interface is active and running without an IP address.

Objective/Subjective

This test item is objective. Either you can create an IP address for the monitoring interface, or you can't.

Master Administrator Password Bounds Checking

Reference

This is a standard checklist item from the COBIT auditing framework, *CobiT 3rd Edition Audit Guidelines*, July 2000.

Control Objective

This checklist item is designed to test whether the password-checking functionality of the system is resistant to extremely long and arbitrary strings of characters, non-alphanumeric characters, and control characters.

Risk

If a malicious or unauthorized user is able to gain physical access to the system console, is it possible to break out of the password-prompting program to gain access to a shell or command prompt that the underlying operating system is running? This type of attack would be very easy to attempt if there is a console video device attached to the system, and the consequences if it succeeded would be very serious indeed: The intrusion detection functionality could be disabled, putting the entire organization's network infrastructure at risk. Attackers could launch exploits with impunity. It is analogous to a hostile insider disabling the alarm system for a business, thereby allowing his cohorts to break in to the building later on that night without setting off the alarm and alerting the police.

Compliance

It may not be possible to completely test all aspects of this risk. Different combinations of keystrokes, characters, and non-alphanumeric characters could be entered to test for a vulnerability.

Testing

One could test the bounds checking of the Master Administrator Password prompt by sending an extremely long string of characters, perhaps hundreds of spaces, to the program that reads and processes the password, to see if you can overflow the buffer. In addition, spurious characters and control character sequences can be sent to see if the password-checking program is susceptible to out-of-bounds conditions.

Objective/Subjective

This item is mostly Objective, but it may be impossible to come up with a complete series of tests that would prove that the password-checking shell is immune to bizarre combinations of keystrokes.

CD-ROM Removable during Operation

Reference

Personal observations/experience.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Control Objective

This control objective determines whether the system CD-ROM can be removed while the system is running.

Risk

The NFR Security NID 200 intrusion detection system boots and runs from a removable CD-ROM that contains the operating system and intrusion detection application software. A malicious user, or a user who is simply ignorant of the functionality of the system, could either intentionally or accidentally press the button on the CD-ROM drive door. If the CD-ROM drive door opens, it most likely would cause the system to crash. This would effectively disable the intrusion detection capability of the system and the organization the system is in place to protect. While it may seem unlikely that this could happen, a bored night shift computer operator might be curious to see if he could play a copy of the latest *Butthole Surfers* CD in the IDS's CD-ROM drive, or a custodian cleaning the data center could accidentally bump the drive button with the his broom handle.

Compliance

Compliance with this checklist item is definitely binary: Either the CD-ROM drive door opens when pressed during system operation or it does not.

Testing

While the system is in its normal operational state, walk up to it and press the button that controls the CD-ROM drive door.

Objective/Subjective

This test can be objectively verified by pressing the button that controls the system's CD-ROM drive door.

Power Supply Interruption

Reference

Personal observations/experience.

Control Objective

This item tests whether power to the system can be easily interrupted.

Risk

Being able to easily pull the plug on the NFR NID 200 could lead to the same type of risk described above. While the likelihood of a cleaning person or technician accidentally pulling the power cord out the wall is admittedly small, there is still the possibility of it happening. If such an event did occur and it was not immediately noticed, the consequences of not being able to detect attacks on the organization's network are serious. For example, certain models of the Cisco PIX Firewall have a lockable metal front panel door that protects the power button and the floppy disk drive.

Compliance

It can easily be determined if the power supply to the system is vulnerable to this risk.

Testing

Examine the power supply cord and power supply fixture to see if someone could pull the power cord from the system box, wall outlet, or bus bar receptacle. Many home security systems use a type of screw assembly on the power supply housing that goes into the wall outlet which makes it impossible to remove accidentally and difficult to remove intentionally. Locate the power button on the front of the unit: does any type of enclosure protect it? Can someone turn the system off by accidentally bumping the button?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Objective/Subjective

This checklist item is mostly objective, as the ability to disconnect the power source or accidentally power off the system can be independently verified, although assessing how easily this can be done may be somewhat subjective.

Remote System Access

The NFR NID 200 IDS is normally managed through its remote Administration Interface. The system that implements this graphical user interface resides on a Windows-based (2000, NT Client/Server) host. The NID sensor is only as secure as the system on which the management software is installed. You need to audit the management client (separately) according to the established audit guidelines for that platform to determine whether the entire system is secure.

User Management - Forced Password Change after Install

Reference

CobiT 3rd Edition Audit Guidelines document.

Control Objective

Does the NFR Security NID 200 intrusion detection system force the system administrator to change the password on the default nfr administrator account when the system is first installed?

Risk

Most computer systems and devices that use authentication ship from the factory with default passwords set. The NID 200 is no exception. If a particular system does not force the administrator to change the factory default administrator password during or after installation, the system is at risk of compromise by anyone who knows what the factory default administrator is for that particular device. The likelihood of this type of event happening are quite high, and the consequences if it happens are quite serious, including the impairment or complete disabling of an organization's intrusion detection capability.

Compliance

You can test compliance for this item by installing the Administration Interface (AI) for the product and seeing if it forces the administrator to change the password for the default nfr account.

Testing

Install the NFR Security Administration Interface (AI) on a client workstation. Log in to the default nfr administrator account and see if the Administration Interface forces you to change the default administrator account password.

Objective/Subjective

This item is completely objective. Either the system forces you to change the password, or it doesn't.

User Management – Password Length/Complexity on Default NFR Account

Reference

CobiT 3rd Edition Audit Guidelines document.

Control Objective

This item tests whether one can set a null or trivial-to-guess password on the default nfr account on the sensor through the remote management GUI.

Risk

The NFR NID 200 intrusion detection system comes with a default user account (nfr) and password (nfr). If the IDS administrator can set a null or trivially short password on the sensor through the remote management GUI, he or she can render the system vulnerable to compromise. If a hostile internal user possesses the management GUI software, they can

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

connect to the sensor system simply by knowing its IP address. The likelihood of this happening, while not extremely high, is certainly possible and the consequences could be disastrous. If a malicious user on the internal network gains access to the sensor, he can partially or completely disable the NID 200's intrusion detection and alerting capability. The consequences of having your organization's IDS disabled should be obvious by now, but we will include them for completeness: Outside attackers can launch attacks and exploits with less chance of being detected or caught if the IDS is impaired or disabled. This is analogous to having your kid leave his window open or a door unlocked when you go out.

Compliance

Verifying the minimum password length for the default nfr account can test compliance for this item, although in reality it depends on the complexity of the password that the system administrator has designed.

Testing

To test the password length and null password risk, one needs to start the NFR Administration Interface (AI) GUI. Click on the Administration tab on the left hand slider panel. This displays four items: User Administration, Package Configuration, Alert Configuration, and Variable Configuration. This displays all of the user accounts on the system. Double click on the entry for the default nfr account. This brings up a dialogue box that contains the account name, the account password, the full name for the account, a description field for the account, and OK and Cancel buttons. First, attempt to blank out the existing account password by backspacing over the existing password string. Then, attempt to click on OK. If this works, the system accepts a null password for the default nfr account. Next, attempt to blank out the existing default nfr account password, and enter a one-character password, increasing the number of characters in the password until the system accepts the password string. This is the minimum password length that the system requires for the default nfr administrator account. Next, count the number of asterisks that appear in the change password field. This is the length of the password that the administrator has chosen.

Because the system does not require long or hard-to-break passwords, you, as the auditor must interview the system administrator to ensure that he or she has chosen a sufficiently difficult-to-break password. Instead of directly asking for the password perhaps ask if the administrator uses upper and lower case characters, numbers, and non-alphanumeric characters. The best way to verify this is to check the length of the password by counting the number of asterisks that correspond to characters in the password string that appear in the password input box.

Objective/Subjective

This item is entirely objective, as we can independently verify the minimum password length required for the default administrator account, although the complexity of the password depends on the system administrator's use of upper and lower case characters, numbers, and non-alphanumeric characters.

User Management – Password Length/Complexity on New User Account

Reference

CobiT 3rd Edition Audit Guidelines.

Control Objective

This item tests the minimum password length and complexity for a new user account.

Risk

Like the default administrator account (nfr), you can add a new user account that may have a short, easy-to-guess password. If the IDS administrator can set a null or trivially short password on a new user account on the sensor through the remote management GUI, he or she can render the system vulnerable to compromise. If a hostile internal user possesses the management GUI software, he can connect to the sensor system by simply knowing its IP address. The likelihood of this happening, while not extremely high, is certainly possible, and the consequences could be serious. If a malicious user on the internal network gains access to the sensor, he can partially or completely disable the NID 200's intrusion detection and alerting capability. The consequences of having your organization's IDS disabled should be obvious by now, but we will include them for completeness: Outside attackers can launch attacks and exploits with less

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

chance of being detected or caught if the IDS is impaired or disabled. This is analogous to having your kid leave his window open or a door unlocked when you go out.

Compliance

Verifying the minimum password length for the default nfr account can test compliance for this item.

Testing

To test the password length and null password risk, start the NFR Administration Interface (AI) GUI. Click on the Administration tab on the left hand slider panel. This displays four items: User Administration, Package Configuration, Alert Configuration, Variable Configuration, and all of the user accounts on the system. Click on the tab for **Add User…** . This brings up a dialogue box that contains the account name, the account password, the full name for the account, a description field for the account, and OK and Cancel buttons. First, attempt to create a new user account with a null password. Then, attempt to click on OK. If this works, the system accepts a null password for new user accounts. Next, attempt to enter a one-character password, increasing the number of characters in the password until the system accepts the password string. This is the minimum password length that the system requires for the new user accounts.

Because the system does not require long or hard-to-break passwords, you, as the auditor, must interview the system administrator to ensure that he or she has chosen a sufficiently robust password. Instead of asking directly what the password is, ask if the administrator uses upper and lower case characters, numbers, and non-alphanumeric characters. The best that can be done to verify this is to check the length of the password. You can do this by counting the number of asterisks that correspond to characters in the password string that appear in the password input box.

Objective/Subjective

This item is mostly objective, as we can independently verify the minimum password length required for the default administrator account, although the complexity of the password depends on the string of characters that administrator has chosen.

User Management – Superfluous User Accounts

Reference

CobiT 3rd Edition Audit Guidelines.

Control Objective

This item is designed to determine whether there are extraneous user accounts on the system.

Risk

All computer systems should limit the number of user accounts that are on the system. Extra, unnecessary accounts increase the likelihood of weak passwords being used and interactive accounts left logged in, which can in turn increase the chance of a system compromise.

Compliance

Enumerating the number of accounts that are active on the system and the purpose for each can test compliance for this item.

Testing

You can test for this item by first listing all of the accounts that are on the system. Go to the User Administration section to list all user accounts on the system. You will need to interview the system administrator and possibly the users of the accounts you find to determine if all of the accounts are absolutely required for the running and maintenance of the system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Objective/Subjective

This item is mostly subjective. While we can independently count and verify the number of accounts on the system and the purpose for each, the opinions of the system administrator and the users largely define the necessity of each account.

User Management – User Permissions

Reference

CobiT 3rd Edition Audit Guidelines.

Control Objective

This item is designed to determine whether there are unnecessary permissions associated with individual users accounts.

Risk

All computer systems should limit the number of user accounts on the system. Extra, unnecessary accounts increase the likelihood of weak passwords being used and interactive accounts left logged in, which can in turn increase the chance of a system compromise. In addition, the user accounts that are deemed necessary to the operation of the system should follow the principle of least privilege; they should only allow those operations that are absolutely necessary for the execution of that user's job duties.

Compliance

Enumerating the number of accounts that are active on the system, what each one is used for, and which permission are assigned to the account can test compliance for this item.

Testing

You can test for this item by first listing out all of the accounts that are on the system. Go to the User Administration section for a list of all user accounts on the system. You will need to interview the system administrator and possibly the users of the accounts you find to determine if all of the accounts are absolutely required for the running and maintenance of the system. Next, click on the permissions tab for each individual user account and examine the permissions that are assigned to each user. Again, you will need to interview the system administrator to ascertain what operations or actions each user on the system needs, and what permissions are needed to carry out those operations.

Objective/Subjective

This item is somewhat subjective. While we can independently count and verify the number of accounts on the system, what each one is used for, and what permissions are assigned, the decision about which permissions are absolutely necessary and which ones are not relies heavily on the system administrator and user's opinions. Common sense and a clear understanding of user roles and responsibilities should clarify any potential ambiguity.

User Management - Change Password Feature on Edit Menu

Reference

Personal experience/observations.

Control Objective

This checklist item is designed to determine if the system administrator knows that the logged in account user can set a one, two, or three character password, which is less than the four-character minimum required when creating new user accounts on the system.

Risk

The NFR Security Administration Interface (AI) for the NID 200 has a feature that allows the logged in user to change his password to something less than four characters; Four is the minimum password length for all existing and new user accounts. However, using the **Change Password…** feature from the Edit menu on the main page of the NFR

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administration Interface, a user can set a password with fewer than four characters. The implications of this should be obvious. If there are other users of the system besides the administrator, they could set sufficiently weak passwords that would allow a malicious user to compromise and disable the system.

Compliance

Compliance for this is difficult to test. Ask the system administrator for written policies that the organization has for minimum password length and audit each user account on the system for compliance.

Testing

To test this item, we would need to review every single user account on the system by methodically editing each user profile to see how long a password is in use for each account. We do this by selecting **Administration -> User Management**, editing each user profile, and counting the number of asterisks that appear in the password field for that user. However, even this approach has its weaknesses, as even though a user might have a long enough password, there is no way, short of interview the user, to determine whether they have constructed a password that is a mixture of upper and lower case characters and that contain numbers and non-alphanumeric characters. This is where it is important to audit the organization's policy on password length, complexity, and design.

Objective/Subjective

Testing for this is difficult, as it is almost entirely subjective. We must rely on the administrator and the organization to have a policy in place that dictates the creation and use of strong passwords. As auditors, the most that we can do objectively is to count the number of characters that are being used for each password for each user account on the system.

Security of Remote Management Communications Channel

Reference

CobiT 3rd Edition Audit Guidelines.

Control Objective

This checklist item is designed to validate the security of the network connection between the NID 200 sensor and the remote management workstation.

Risk

Can a malicious user with a network sniffer capture packets that are flowing between the NID sensor and the remote management workstation? While the chance of someone inside an organization using a sniffer to capture the NID 200 sensor's password is small, one cannot safely ignore the insider threat. Studies show that the threat from users inside the organization is usually greater than the threat from outside the organization. If an insider uses a sniffer to capture the remote management password, it can be used to gain access to the system and disable it. If the system is no longer functioning correctly, that is if recognition of certain attack signatures has been disabled, the organization or enterprise is vulnerable to a wide range of attacks. Again, this is akin to an employee turning off a store's alarm system so that his outsider friends can break into the store and rob it.

Compliance

Compliance for this checklist item is binary. Either the vendor uses an encrypted channel for remote management communications or it does not.

Testing

You can easily test for compliance for this checklist item by setting up a system running a commercial sniffer, such as Ethereal, or a system running tcpdump. Filter on the sensor's management interface IP address and the IP address of the management workstation. Then, with the sniffer program running in the background, remotely log into the NID 200 sensor using the remote management workstation client. All communications between the remote management

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

workstation client and the IDS sensor should be encrypted. If you can recover the sensor password the system is at risk for compromise by unauthorized third parties.

Objective/Subjective

This item is objective: It is either possible to capture the remote management password using a sniffer or it is not.

Test Isolation of Management Network

Reference

The source of this item is from the SANS Institute course [8] on network intrusion detection systems. This is also known as an industry best practice for configuring network intrusion detection systems, and appears in popular text books [5],[6] on the subject.

Control Objective

The objective of this test is to determine if the network on which the management station resides is physically isolated from the organization's internal, private network.

Risk

This audit checklist item examines the risk associated with an incorrectly designed management network. The NID 200 IDS has two network interfaces. One is the monitor network interface. This interface faces the public Internet, and analyzes traffic that is passing by the organization's perimeter. It has no IP address assigned to it, and as such is much less vulnerable to attack by outsiders. The second network interface is the management interface. This interface faces the organization's private, or internal, network. It has a fully functional IP stack loaded on it, and has an IP address which is used to communicate with the remote management workstation. Because the management interface is fully network aware and functional, it is important that the network on which the remote management workstation resides be physically isolated from the rest of the internal network.

While the likelihood of an attacker gaining access to the NID 200 sensor through the passive monitor interface is low, if that attacker were able to somehow gain access to the NID 200 sensor, they would be able to potentially leapfrog from the sensor to other systems on the internal network, using the sensor as a launch pad for other attacks. By physically isolating the network to which the management interface is attached, we can minimize the exposure to the internal network.

Compliance

Compliance in this case is fairly straightforward: It may be difficult and time consuming to validate that the network to which the sensor's management interface is connected is physically isolated, but it can be done. It is important to note that compliance in this case is not a one-time event: The isolated management network must be continually reinspected and revalidated, and the network connections must be recertified to ensure that backdoors are not intentionally or accidentally added. Often, system administrators will be tempted to add surreptitious connections for their own convenience. This temptation must be resisted. The next checklist item, *Implementation of Internet Connection of Management Station*, relates directly to the design of the management network.

Testing

Testing for this audit checklist item is twofold: First, it requires a rigorous physical inventory of all connections (including wireless ones) in the isolated management network. This means that someone must visually inspect all the systems and wiring that is used in this subnet. Special attention must be paid to wireless network cards, modems, phone lines, serial cables, printers, and fax machines; basically anything that could provide a back door into the organization's internal private network from the isolated management subnet.

Second, software techniques such as network ping sweeps and snmp-based network discoveries using tools such as NetScout's nGenius Capacity Planner (formerly NextPoint S3), mappings provided by tools such as Tivoli's Netview, or HP OpenView, can be used to validate and verify the results achieved by the physical inspection.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Objective/Subjective

This checklist item is strictly objective, but requires ongoing inspection and re-validation to be successful; in case someone modifies or adds new systems or network connections to the existing isolated network infrastructure.

Implementation of Internet Connection for Management Station

Reference

Personal experience/observation.

Control Objective

The NFR Security NID 200 intrusion detection system, like most commercial intrusion detection systems, has a mechanism for updating attack signatures automatically. On the NFR product, this feature is called the ***Package Updater***. The Package Updater runs on the Windows-based client station. Basically, at a predetermined interval, the Package Updater periodically interrogates the support.nfr.com web site, checking to see if the sensor system has the latest packages or exploit signatures in its database. Naturally, to do this, it must make a connection out to the Internet. Typically, this connection will be made through a firewall or some other type of perimeter defense. If the signature database is out-of-date, the Package Updater retrieves any new signatures over the Management station's Internet connection and then loads them onto the sensor system.

The configuration required for this type of automatic signature update runs completely counter to the objective of the preceding checklist item that required a verifiable isolated network for the management station. If we want to update signature packages automatically, we cannot have the management station on a physically isolated network. As we will see, there are several different approaches to solving this problem.

The risk, compliance, and testing for this item depends on the implementation, or approach that the system administrator chooses.

Risk

This item addresses the possibility that a compromised NID 200 IDS sensor could be used as a stepping-stone into an organization's private network if the Package Updater functionality is in use. If the Package Updater feature is in use, it requires a public Internet connection. If that public Internet connection is provided through the internal network, the internal network is at risk. The risk associated with this item depends on the implementation the system admin chooses to update packages. If a dedicated Internet connection is created for the isolated management network, the risk to the rest of the internal network is low: The likelihood of an attack succeeding through the sensor's monitoring interface is quite low to begin with. Even if an attack were successful, the only systems that would be put at risk would be the management workstations.

On the other hand, if the second approach is taken, where the main internal network Internet connection is used and we depend on the system administrator to physically disconnect the sensor's monitoring interface during package update operations, the risk rises **if the procedure is not followed exactly every time**. The consequences are far greater if an attacker compromises the sensor system, as the organization's entire internal network is exposed.

Compliance

There are two ways to test compliance with this checklist item, but only one is binary. If the Package Updater feature is in use, you can only achieve compliance in one of two ways: First, the isolated network on which the management station resides must have a dedicated connection to the Internet that does not pass over the organization's internal network. This is a binary condition: Either there is a dedicated Internet connection, or there isn't.

Second: the sensor's monitoring interface must be disconnected from the Internet during package update operations. This second alternative is more of a policy and procedures type of compliance and cannot be verified objectively, as it depends on operations personnel performing a series of discrete tasks in a particular order every single time they need to update the sensor's packages.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Testing

Testing for this checklist item depends on the approach the system administrator takes to update signatures on the IDS.

If the first approach is used, the testing for this checklist item is almost identical to the preceding checklist item, except that you need to verify that the network for the isolated management network has a dedicated Internet connection. This should include a dedicated perimeter protection device, such as a firewall. There are many small, inexpensive firewalls available for these types of applications. The auditor should examine the physically isolated management network to verify that the only connections into and out of it are the NID 200 sensor's management interface, and the public Internet connection for receiving package updates on the management workstation.

If the second approach is taken, testing can only be achieved by verifying that the organization has a written policy that is followed when updating signatures. In addition, the auditor must ask the administrator to perform a package update for him, and he must observe whether or not the necessary precaution of disconnecting the sensor's monitoring interface from the Internet is followed during the package update operation.

Objective/Subjective

This item is objective regardless of what approach or implementation the intrusion detection administrator selects. If the dedicated Internet connection on the isolated management network is followed, we can independently verify that there is indeed a separate Internet connection and that there are no backdoor connections present. If the second approach is taken, we can ask the intrusion detection system administrator to perform a package update operation for us to see whether they follow a standard written procedure for methodically disconnecting the sensor's monitor interface from the Internet during package update operations. There is an element of subjectivity to this second test scenario: Just because the system administrator follows a prescribed, documented security procedure in front of the auditor, it does not mean that he or she will follow this procedure every time. It is easy to imagine a harried system administrator skipping the step of disconnecting the monitoring interface during a package update operation, assuming that the likelihood of something happening is quite low.

Sensor Monitor Interface Detectability

Reference

The source of this item is from the SANS Institute course [8] on network intrusion detection systems. This is also known as an industry best practice for configuring network intrusion detection systems, and appears in popular text books [5],[6] on the subject.

Control Objective

This item is designed to determine whether the NID 200 sensor's monitor interface is detectable by responding to unsolicited stimulus.

Risk

This step determines whether an attacker can detect the presence of the intrusion detection system. This is important for one major reason: You cannot attack what you cannot see. If attackers know the intrusion detection system exists, they can try to compromise it or disable it. The likelihood of an attacker attempting these methods is low: It would require a very sophisticated hacker armed with sophisticated tools, such as L0pht Heavy Industries AntiSniff program. The consequences of an attacker locating the IDS are serious. If the IDS is identified, attacks can be launched directly against it, perhaps impairing it or completely disabling its attack detection capability.

Compliance

Determining whether the NID 200 sensor's monitor interface responds to any type of stimulus can check compliance for this item. While we can determine with near certainty whether the IDS responds to stimulus, every possible stimulus cannot be simulated, so at best we can only have a certain degree of certainty regarding this item.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Testing

Tools, such as Nmap, L0pht AntiSniff and others that can initiate ARP and ICMP traffic, can test this item.

Objective/Subjective

This item is almost entirely objective, save for the caveat that not every possible stimulus can be initiated against the sensor's monitor network interface.

Susceptibility to Denial of Service (DoS) Attack

Reference

The source of this item is from the SANS Institute course [8] on network intrusion detection systems. This is also known as an industry best practice for configuring network intrusion detection systems, and appears in popular text books [5],[6] on the subject.

Control Objective

The control Objective in this case is whether the IDS system is susceptible to denial of service type attacks.

Risk

Denial of Service attacks work by flooding a system or device with so many network connection requests or packets, that the system's processor or I/O subsystem cannot keep up with them. This means that legitimate requests or normal packet processing cannot be accomplished. If the intrusion detection system cannot keep up with normal packet processing operations, it cannot guarantee thorough analysis of all packets that might hit the organization's perimeter. If it cannot analyze all incoming packets, some malicious or mal-formed packets may get through the firewall or perimeter without being detected.

Compliance

Using tools such as nmap or nessus to flood the IDS's monitor interface with packets, fragments, and miscellaneous spurious requests can test compliance with this item. A well-designed ID system should be able to keep up with the amount of traffic for which it was designed without dropping packets.

Testing

This item would be extremely difficult to test. First we need to know whether the NID 200 has a feature to detect dropped packets. Unlike other ID systems such as Snort, the NID 200 does not seem to have this feature. To set up this test, configure a system with the freeware tool nmap (www.insecure.org). Set up a sniffer or system running tcpdump on the same network segment. Fire large combinations of strange or malformed packets at the network segment on which the IDS monitor interface resides. At the same time, fire off a real or simulated exploit mixed into the stream of garbage packets. See if the NID 200 detects the exploit and alerts.

Objective/Subjective

This test would be fairly subjective: The NID 200 may be able to detect exploits mixed into a DoS attack, or it might not.

Sensor Management Interface Open Ports

Reference

Personal experience/observation.

Control Objective

This item is designed to determine whether the NID 200 sensor's management interface has well-known ports open.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk

This step determines whether there are open ports on the sensor management interface that an attacker could use to compromise the system. Ports for services that are open on a system but not used represent an unnecessary security risk. Disabling these ports reduces the risk of malicious users being able to exploit weaknesses in the programs associated with these ports.

Compliance

Determining if ports on the NID 200 sensor's management interface respond to any type of port scans can check compliance for this item.

Testing

Using port scanning tools, such as Nmap, can test this item.

Objective/Subjective

This item is fairly objective: The NID 200 sensor management interface only communicates with the Administrative Interface (AI) over port 2010. No other ports are necessary, and as such, should not be active.

Sensor and Management Station Patches Up-to-Date

Reference

CobiT 3rd Edition Audit Guidelines.

Control Objective

This item is designed to determine whether the NID 200 sensor and management software have had all necessary patches applied.

Risk

This step determines whether there are any unpatched bugs or vulnerabilities on the sensor or management system, which an attacker could use to compromise the system to create an unnecessary security risk. Patching these vulnerabilities reduces the risk of malicious users being able to exploit weaknesses in the system.

Compliance

Interviewing the system administrator to see if all patches have been applied would test compliance for this item.

Testing

There appears to be no way to independently verify whether patches have been applied to the system other than asking the administrator.

Objective/Subjective

It would seem at first glance that this item is objective. Either the system patches are up-to-date, or they are not. However, the only way to verify this is by relying on the system administrator's word. Thus, I would argue that this item is actually subjective, because we as auditors cannot independently verify the information.

Package Updater Automatically Updates Signatures

Reference

NFR NID 200 *Getting Started Guide,* and *User's Guide.*

Control Objective

This item is designed to test whether the system administrator has enabled the package updater functionality to automatically download the latest attack signatures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk

New attacks, viruses, worms, and trojan horse programs are always being developed. An intrusion detection system administrator must constantly update the signature files on the IDS to protect his organization from attack. If we rely on the system administrator to do this manually, we increase our risk, because the system administrator may forget to download the packages or signatures or may not check for new signatures frequently enough.

Compliance

Compliance for this item can be checked easily. The NFR Security NID 200 has a very useful feature whereby one can automatically download new attack signatures from the NFR support web site on a daily basis. This way, as soon as a new attack or exploit signature is available, the NFR system downloads it.

Testing

To test for this item log on to the sensor system using the AI and click on **View** on the menu bar. Click on **Package Updater** on the **View** menu. Click on the Settings… button. This displays a screen that allows you to choose how often the system checks for new packages. The choices are **Never**, **Daily**, **Weekly**, **Bi-weekly**, and **Monthly**. If the selected interval is Never, the system is never checking for packages, and we must rely on the system administrator

Objective/Subjective

This item is objective: Either the package update functionality has been enabled to automatically update the signature database, or it has not.

Assignment Three – Conduct the Audit

Checklist Item 1 – Local Console Authentication

Approached the local console terminal. Local console terminal was in status monitoring mode. Pressed "A" to enter Admin mode. The system prompted for the current password. Entered password. The Main menu appeared. Selected **Access Administration** from main menu. System displays **Password** and **Repeat Password** field, with current password replaced by asterisk characters. Removed all characters in the Password and Repeat password fields by pressing the backspace key. Tab down to the **Save** field. Pressed Enter. System responded with the following message: **Password Missing Press Any Key to Continue**. I repeated the process with a single character password. The system accepted the single character password. The system does accept long passwords consisting of a mixture of upper case, lower case, numeric, and non-alphanumeric characters, so a secure password can be constructed. Unfortunately, the local console has no print screen functionality, so this behavior cannot be reproduced on paper or in an electronic format.

Checklist Item 2 – IP Address on Monitor Interface

Approached the local console terminal. Local console terminal was in status monitoring mode. Pressed "A" to enter Admin mode. The system prompted for the current password. Entered password. The Main menu appeared. Selected **Configure the System** menu item. The system lets you select one network interface, either FXP0 or FXP1, to be the management interface. Once you make this selection, you can assign an IP address to that interface (the management interface). There is no way for the user to bind an IP address to the monitoring interface. Because the local console has no print screen functionality, this checklist item cannot be reproduced on paper or in an electronic medium.

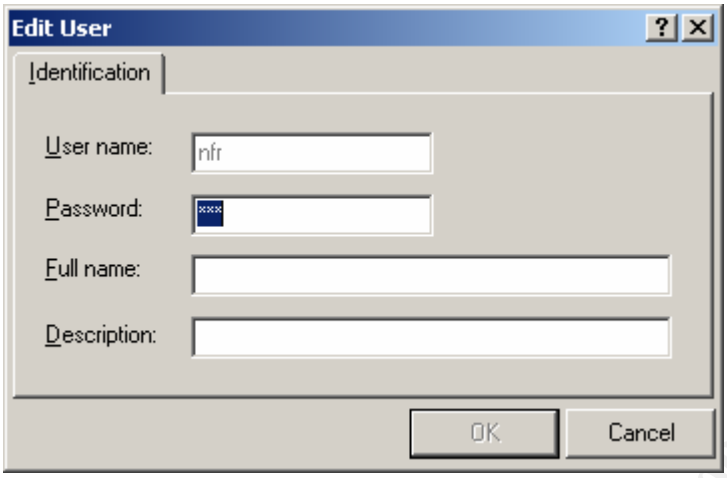
Checklist Item 3 – Eject CD-ROM During System Operation

Approached the sensor system unit. The system was running in normal operating mode as evidenced by the packet capture count on the Status monitoring screen on the main console terminal. I pressed the CD-ROM drive eject/open button several times. The system did not respond, and the CD drive did not open. There is no way to interrupt the normal operation of the system by pressing the CD-ROM drive eject/open button. This checklist item cannot be reproduced on paper on in an electronic medium.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Checklist Item 4 – Default NFR Account Password

The NFR NID 200 intrusion detection system comes with a default user account (nfr) with a default password of nfr. The object of this test was to determine whether or not the system administrator had changed the default password to something longer and more complex. The administrator admitted to not having changed the password from the factory set default password. Logging on to the NFR Administration Interface (AI) and clicking on the Administration tab verified this. We double clicked on User Administration. This displayed all of the user accounts on the system. We double clicked on the entry for the default nfr account. This brought up a dialogue box that contained the account name, the full name for the account, a description field for the account, and OK and Cancel buttons. The existing password was represented by a series of asterisks, each of which represented a character in the password. We could only conclude that the three asterisks in the field represented the letters n, f, and r. Even if they had changed the password to something other than nfr, the password would still be unacceptably short and simple.



Checklist Item 5 – Security of Remote Communications Channel

This test was designed to test the integrity of the communications channel between the NID 200 sensor and the remote management workstation. To accomplish this test, we set up a system running Snort in packet sniffer mode. We could also have used tcpdump to do this. We noted the IP address of the NID 200's management interface, and the IP address of the remote management workstation. We started Snort with the following command line and BPF filter:

./snort –v –i fddi0 host 10.0.9.75 and host 10.0.4.155 -X

Where 10.0.9.75 is the IP address of the management station and 10.0.4.155 is the IP address of the NID 200 sensor. This command contains a BPF filter that captures traffic between the NID 200 sensor and the management workstation only.

We then started the Administration Interface (AI) on the management workstation and logged into the sensor. We then stopped Snort and examined the trace. In summary, the password and all subsequent communication between the remote management workstation and the sensor was not sent in plain text, but was sent using an encrypted communications channel. The explanation of the trace follows.

As we will see, the NID 200 sensor has only a single tcp port open: 2010. It listens for incoming connections from a client running the Administration Interface software on this port. What is actually listening on this port is a web server. If we issue the following telnet command:

telnet 10.0.4.155 2010

The sensor responds with the following:

HTTP/1.0 400 Bad request

So we know that some type of program that recognizes the http protocol is listening there. Basically, the NID 200 sensor is running a Kerberized web server to communicate with a Kerberos client on the remote management workstation.

Communication between the sensor and the management workstation takes places in identical 11-packet phases. First, the management workstation opens a connection on a random high port (in the example below, this is 1478) to port 2010 on

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the sensor by sending a SYN request. The sensor responds with a SYN/ACK. The management station responds with an ACK and then an ACK/PUSH in which it sends data. The sensor ACKs this data, and the management station sends more data with another ACK/PUSH. The sensor responds with data of its own with an ACK/PUSH. The sensor then indicates its decision to end the session with an ACK/FIN. The management station acknowledges the FIN with an ACK of its own. The management station then sends an ACK/FIN to tear down or terminate its end of the connection. Finally, the sensor acknowledges the management station's FIN with an ACK.

However, while each phase is 11 packets in length, the information exchanged in each phase is different. First the client must authenticate itself with the sensor. This 11-packet sequence is repeated using the Kerberos ticket granting mechanism until the client is authenticated and all necessary conversation parameters have been exchanged. An explanation of the Kerberos ticket-granting authentication mechanism could be an entire paper in itself, so we will simply highlight the parts of the trace that show where critical authentication data is encrypted. This proves that the communication channel between workstation and sensor is secure.

```
Log directory =

        --== Initializing Snort ==--

Initializing Network Interface fddi0
Decoding FDDI on interface fddi0

        --== Initialization Complete ==--
04/04-10:43:28.171940 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2810 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D88FBF6  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0A FA 40 00 80 06 C1  .....E..0..@....
0x0020: BC 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FB  ....K...........
0x0030: F6 00 00 00 00 70 02 16 D0 17 1F 00 00 02 04 05  .....p..........
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

In this packet, the mangement workstation sends a TCP SYN packet to the sensor on port 2010.

```
04/04-10:43:28.172309 10.0.4.155:2010 -> 10.0.9.75:1478
TCP TTL:63 TOS:0x0 ID:26629 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627949E4  Ack: 0x1D88FBF7  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 05 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: B5 10 16 04 9B 10 16 09 4B 07 DA 05 C6 62 79 49  ........K....byI
0x0030: E4 1D 88 FB F7 60 12 44 70 52 17 00 00 02 04 05  .....`.DpR......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The NID 200 sensor responds to the management station with a SYN/ACK.

```
04/04-10:43:28.172679 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2811 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D88FBF7  Ack: 0x627949E5  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0A FB 40 00 80 06 C1  .....E..(..@....
0x0020: C3 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FB  ....K...........
0x0030: F7 62 79 49 E5 50 10 16 D0 97 74 00 00 02 04 05  .byI.P....t.....
0x0040: B4 01 01                                         ...
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

=+

The management workstation responds with an ACK.

```
04/04-10:43:28.172869 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2812 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1D88FBF7  Ack: 0x627949E5  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 3D 0A FC 40 00 80 06 C1  .....E..=..@....
0x0020: AD 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FB  ....K...........
0x0030: F7 62 79 49 E5 50 18 16 D0 C1 AE 00 00 50 4F 53  .byI.P.......POS
0x0040: 54 20 2F 74 69 6D 65 20 48 54 54 50 2F 31 2E 30  T /time HTTP/1.0
0x0050: 0D 0A                                            ..
```

=+

The management station then sends an ACK/PUSH with what version of HTTP it wants to talk, which in this case is HTTP V1.0 using the POST method.

```
04/04-10:43:28.268840 10.0.4.155:2010 -> 10.0.9.75:1478
TCP TTL:63 TOS:0x0 ID:26630 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627949E5  Ack: 0x1D88FC0C  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 06 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: B8 10 16 04 9B 10 16 09 4B 07 DA 05 C6 62 79 49  ........K....byI
0x0030: E5 1D 88 FC 0C 50 10 44 70 69 BF 00 00           .....P.Dpi...
```

=+

The NID 200 sensor then acknowledges this packet with an ACK of its own.

```
04/04-10:43:28.269392 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2813 IpLen:20 DgmLen:166 DF
***AP*** Seq: 0x1D88FC0C  Ack: 0x627949E5  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 A6 0A FD 40 00 80 06 C1  .....E.....@....
0x0020: 43 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FC  C...K...........
0x0030: 0C 62 79 49 E5 50 18 16 D0 03 C0 00 00 55 73 65  .byI.P.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 41 63 63 65 70 74 3A 20  ndows)..Accept:
0x0070: 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70  */*..Content-typ
0x0080: 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  e: application/x
0x0090: 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63  -www-form-urlenc
0x00A0: 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65  oded..Content-le
0x00B0: 6E 67 74 68 3A 20 30 0D 0A 0D 0A                 ngth: 0....
```

=+

Here we see the management workstation sends an ACK/PUSH that contains the information on who he is, specifically the NFR Console, version 2.1.

```
04/04-10:43:28.269835 10.0.4.155:2010 -> 10.0.9.75:1478
TCP TTL:63 TOS:0x0 ID:26631 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627949E5  Ack: 0x1D88FC8A  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 07 40 00 3F 06 A5  .....E..Lh.@.?..
0x0020: 93 10 16 04 9B 10 16 09 4B 07 DA 05 C6 62 79 49  ........K....byI
0x0030: E5 1D 88 FC 8A 50 18 44 70 CD 3E 00 00 48 54 54  .....P.Dp.>..HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 30 0D 0A 0D  me: 986400260...
0x0060: 0A                                               .
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

=+
The NID 200 sensor then replies with an ACK/PUSH that HTTP 1.0 is OK with a time stamp. This is characteristic of Kerberos.

```
04/04-10:43:28.269837 10.0.4.155:2010 -> 10.0.9.75:1478
TCP TTL:63 TOS:0x0 ID:26632 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x62794A09  Ack: 0x1D88FC8A  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 08 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: B6 10 16 04 9B 10 16 09 4B 07 DA 05 C6 62 79 4A  ........K....byJ
0x0030: 09 1D 88 FC 8A 50 11 44 70 69 1C 00 00           .....P.Dpi...
```

=+
The sensor terminates its end of the session with an ACK/FIN.

```
04/04-10:43:28.270366 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2814 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D88FC8A  Ack: 0x62794A0A  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0A FE 40 00 80 06 C1  .....E..(..@....
0x0020: C0 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FC  ....K...........
0x0030: 8A 62 79 4A 0A 50 10 16 AC 96 E0 00 00 55 73 65  .byJ.P.......Use
0x0040: 72 2D 41                                         r-A
```

=+
The management station ACKs the sensor's FIN.

```
04/04-10:43:28.270556 10.0.9.75:1478 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2815 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D88FC8A  Ack: 0x62794A0A  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0A FF 40 00 80 06 C1  .....E..(..@....
0x0020: BF 10 16 09 4B 10 16 04 9B 05 C6 07 DA 1D 88 FC  ....K...........
0x0030: 8A 62 79 4A 0A 50 11 16 AC 96 DF 00 00 55 73 65  .byJ.P.......Use
0x0040: 72 2D 41                                         r-A
```

=+
The management station sends a FIN of its own, terminating its end of the connection.

```
04/04-10:43:28.271048 10.0.4.155:2010 -> 10.0.9.75:1478
TCP TTL:63 TOS:0x0 ID:26633 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62794A0A  Ack: 0x1D88FC8B  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 09 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: B5 10 16 04 9B 10 16 09 4B 07 DA 05 C6 62 79 4A  ........K....byJ
0x0030: 0A 1D 88 FC 8B 50 10 44 70 69 1B 00 00           .....P.Dpi...
```

=+
The sensor ACKs the management station's FIN.

```
04/04-10:43:28.271359 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2816 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D8A2AAC  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 00 40 00 80 06 C1  .....E..0..@....
0x0020: B6 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2A  ....K..........*
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0030: AC 00 00 00 00 70 02 16 D0 E8 66 00 00 02 04 05  .....p....f.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The 11-packet communication process starts again with the management station using a different high port number, one number greater than that used in the previous communication.

```
04/04-10:43:28.271679 10.0.4.155:2010 -> 10.0.9.75:1479
TCP TTL:63 TOS:0x0 ID:26634 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627B9A4E  Ack: 0x1D8A2AAD  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 0A 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: B0 10 16 04 9B 10 16 09 4B 07 DA 05 C7 62 7B 9A  ........K....b{.
0x0030: 4E 1D 8A 2A AD 60 12 44 70 D2 F2 00 00 02 04 05  N..*.`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.272026 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2817 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8A2AAD  Ack: 0x627B9A4F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 01 40 00 80 06 C1  .....E..(..@....
0x0020: BD 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2A  ....K..........*
0x0030: AD 62 7B 9A 4F 50 10 16 D0 18 50 00 00 02 04 05  .b{.OP....P.....
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.272353 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2818 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D8A2AAD  Ack: 0x627B9A4F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 02 40 00 80 06 C1  .....E..9..@....
0x0020: AB 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2A  ....K..........*
0x0030: AD 62 7B 9A 4F 50 18 16 D0 24 5D 00 00 50 4F 53  .b{.OP...$]..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.368828 10.0.4.155:2010 -> 10.0.9.75:1479
TCP TTL:63 TOS:0x0 ID:26635 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627B9A4F  Ack: 0x1D8A2ABE  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 0B 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: B3 10 16 04 9B 10 16 09 4B 07 DA 05 C7 62 7B 9A  ........K....b{.
0x0030: 4F 1D 8A 2A BE 50 10 44 70 EA 9E 00 00           O..*.P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The next packet is what we are looking for regarding the security of the communications channel between the management workstation and the sensor system. We see the username, **nfr**, transmitted in clear text. However, after that, we see the string **Ticket**, followed by what appears to be an encrypted string. This is a Kerberos authentication ticket. We can only assume that the NFR system is using Kerberos as its authentication system. In any case, the password for the system, and the information flowing from the sensor to the management client is all encrypted.

```
04/04-10:43:28.369667 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2819 IpLen:20 DgmLen:476 DF
***AP*** Seq: 0x1D8A2ABE  Ack: 0x627B9A4F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0010: 00 00 00 08 00 45 00 01 DC 0B 03 40 00 80 06 C0  .....E.....@....
0x0020: 07 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2A  ....K..........*
0x0030: BE 62 7B 9A 4F 50 18 16 D0 3E 20 00 00 55 73 65  .b{.OP...> ..Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket: 
0x00C0: 25 39 39 3E 25 30 43 25 38 37 3C 25 44 42 25 41  %99>%0C%87<%DB%A
0x00D0: 36 25 42 33 25 44 33 25 45 36 25 42 38 4D 39 38  6%B3%D3%E6%B8M98
0x00E0: 25 38 46 33 25 46 42 25 43 32 25 39 45 6A 45 29  %8F3%FB%C2%9EjE)
0x00F0: 25 45 39 31 25 39 30 25 42 41 25 30 39 25 33 46  %E91%90%BA%09%3F
0x0100: 25 30 45 25 32 43 25 41 41 25 33 41 50 25 44 39  %0E%2C%AA%3AP%D9
0x0110: 7B 25 41 46 25 31 36 25 42 39 25 39 30 25 43 46  {%AF%16%B9%90%CF
0x0120: 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68  ..Content-length
0x0130: 3A 20 31 38 34 0D 0A 0D 0A 67 FA 81 CB D7 CD A5  : 184....g......
0x0140: 3A 8F BB 3D 4C 7F 4B 4C 5F 70 19 ED 21 C5 DE EB  :..=L.KL_p..!...
0x0150: 9E 4C 73 0A 1D F9 A7 DC B3 4B E4 00 FF 46 F5 9E  .Ls......K...F..
0x0160: 8A C8 7C 1C D5 26 C7 37 80 AE DB FB 20 C3 77 63  ..|..&.7.... .wc
0x0170: F4 04 B8 EB 20 B5 F2 6F 75 6C 0C 36 CF 35 04 B3  .... ..oul.6.5..
0x0180: FF 41 74 54 A3 62 81 58 AC 05 97 7C 90 59 69 AA  .AtT.b.X...|.Yi.
0x0190: 2F 02 DB 5F FD BC BF FC A9 48 7D 51 D0 D7 FD 33  /.._.....H}Q...3
0x01A0: 8F 1D 54 EB 85 58 6C 06 2F F1 5C 45 D9 51 79 BF  ..T..Xl./.\E.Qy.
0x01B0: 05 13 55 BB 43 A5 EB 4A 7D F9 BD B3 4F D8 22 DC  ..U.C..J}...O.".
0x01C0: 02 9C 9E 83 C7 B5 6E 69 A9 D4 6E 23 2E 97 99 BB  ......ni..n#....
0x01D0: FF 1A 91 DC C5 C3 08 31 32 5B 93 FB 26 56 0C 37  .......12[..&V.7
0x01E0: 98 92 DF 52 AA AE 17 CD 3B 0B E8 5C E2 69 90 10  ...R....;..\.i..
0x01F0: 83                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.370439 10.0.4.155:2010 -> 10.0.9.75:1479
TCP TTL:63 TOS:0x0 ID:26636 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627B9A4F  Ack: 0x1D8A2C72  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 0C 40 00 3F 06 A5  .....E..Lh.@.?..
0x0020: 8E 10 16 04 9B 10 16 09 4B 07 DA 05 C7 62 7B 9A  ........K....b{.
0x0030: 4F 1D 8A 2C 72 50 18 44 70 4C E7 00 00 48 54 54  O..,rP.DpL...HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.372832 10.0.4.155:2010 -> 10.0.9.75:1479
TCP TTL:63 TOS:0x0 ID:26637 IpLen:20 DgmLen:216 DF
***AP**F Seq: 0x627B9A73  Ack: 0x1D8A2C72  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 D8 68 0D 40 00 3F 06 A5  .....E...h.@.?..
0x0020: 01 10 16 04 9B 10 16 09 4B 07 DA 05 C7 62 7B 9A  ........K....b{.
0x0030: 73 1D 8A 2C 72 50 19 44 70 14 2C 00 00 7F E1 86  s..,rP.Dp.,.....
0x0040: CF D8 D3 E8 6D D0 F3 21 12 B6 5F E7 E4 6B 38 96  ....m..!.._..k8.
0x0050: 70 E5 1B D4 8A 15 7C 6D B0 FB E4 58 D7 5F 35 2E  p.....|m...X._5.
0x0060: 6C 36 0A 9F 92 79 DD 74 8F 6B 1F 50 AE CD B1 79  l6...y.t.k.P...y
0x0070: 1F D0 DA 1A 95 3E 88 0F B7 81 89 56 26 0B A2 10  .....>.....V&...
0x0080: 2E 85 4C FE AD B9 B6 53 23 E5 73 89 8C C4 F0 F6  ..L....S#.s.....
0x0090: 3F 24 B4 A4 E6 5D 00 38 5B 00 57 1E 10 45 E0 A5  ?$...].8[.W..E..
0x00A0: 72 B8 A7 2A 82 03 E2 CA A1 20 97 C2 99 93 DE 36  r..*..... .....6
0x00B0: D9 96 DE 8C ED D0 E2 01 A9 41 DE 75 21 B1 FC 4C  .........A.u!..L
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x00C0: 09 2B DE CD 5B 81 5F 73 7D 1B 28 AB 78 41 71 0A  .+..[._s}.(.xAq.
0x00D0: 4C A4 55 64 FF 8C 1D 22 1C BA AA 28 2D 83 2B 70  L.Ud..."...(-.+p
0x00E0: 63 37 4E B5 BC 6E 8C CD 89 EE 34 92 87           c7N..n....4..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.373380 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2820 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8A2C72  Ack: 0x627B9B24  Win: 0x15FC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 04 40 00 80 06 C1  .....E..(..@....
0x0020: BA 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2C  ....K..........,
0x0030: 72 62 7B 9B 24 50 10 15 FC 16 8A 00 00 50 4F 53  rb{.$P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.373792 10.0.9.75:1479 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2821 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D8A2C72  Ack: 0x627B9B24  Win: 0x15FC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 05 40 00 80 06 C1  .....E..(..@....
0x0020: B9 10 16 09 4B 10 16 04 9B 05 C7 07 DA 1D 8A 2C  ....K..........,
0x0030: 72 62 7B 9B 24 50 11 15 FC 16 89 00 00 50 4F 53  rb{.$P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.374115 10.0.4.155:2010 -> 10.0.9.75:1479
TCP TTL:63 TOS:0x0 ID:26638 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627B9B24  Ack: 0x1D8A2C73  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 0E 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: B0 10 16 04 9B 10 16 09 4B 07 DA 05 C7 62 7B 9B  ........K....b{.
0x0030: 24 1D 8A 2C 73 50 10 44 6F E8 15 00 00           $..,sP.Do....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.374508 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2822 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D8B1F74  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 06 40 00 80 06 C1  .....E..0..@....
0x0020: B0 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 1F  ....K...........
0x0030: 74 00 00 00 00 70 02 16 D0 F3 9C 00 00 02 04 05  t....p..........
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.374835 10.0.4.155:2010 -> 10.0.9.75:1480
TCP TTL:63 TOS:0x0 ID:26639 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627C2AF8  Ack: 0x1D8B1F75  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 0F 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: AB 10 16 04 9B 10 16 09 4B 07 DA 05 C8 62 7C 2A  ........K....b|*
0x0030: F8 1D 8B 1F 75 60 12 44 70 4D 7E 00 00 02 04 05  ....u`.DpM~.....
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
04/04-10:43:28.375211 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2823 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8B1F75  Ack: 0x627C2AF9  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 07 40 00 80 06 C1  .....E..(..@....
0x0020: B7 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 1F  ....K...........
0x0030: 75 62 7C 2A F9 50 10 16 D0 92 DB 00 00 02 04 05  ub|*.P..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.375444 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2824 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D8B1F75  Ack: 0x627C2AF9  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 08 40 00 80 06 C1  .....E..9..@....
0x0020: A5 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 1F  ....K...........
0x0030: 75 62 7C 2A F9 50 18 16 D0 9E E8 00 00 50 4F 53  ub|*.P.......POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.468852 10.0.4.155:2010 -> 10.0.9.75:1480
TCP TTL:63 TOS:0x0 ID:26640 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627C2AF9  Ack: 0x1D8B1F86  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 10 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: AE 10 16 04 9B 10 16 09 4B 07 DA 05 C8 62 7C 2A  ........K....b|*
0x0030: F9 1D 8B 1F 86 50 10 44 70 65 2A 00 00           .....P.Dpe*..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.469658 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2825 IpLen:20 DgmLen:477 DF
***AP*** Seq: 0x1D8B1F86  Ack: 0x627C2AF9  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 01 DD 0B 09 40 00 80 06 C0  .....E.....@....
0x0020: 00 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 1F  ....K...........
0x0030: 86 62 7C 2A F9 50 18 16 D0 99 4F 00 00 55 73 65  .b|*.P....O..Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket: 
0x00C0: 25 31 46 25 32 35 38 25 30 39 7D 5A 25 30 33 25  %1F%258%09}Z%03%
0x00D0: 31 46 25 44 30 29 25 30 38 25 31 36 25 43 42 25  1F%D0)%08%16%CB%
0x00E0: 39 44 25 31 36 5F 5B 46 5B 25 45 46 79 25 44 42  9D%16_[F[%EFy%DB
0x00F0: 4A 25 46 43 25 33 42 25 30 31 7C 6C 25 32 43 34  J%FC%3B%01|l%2C4
0x0100: 25 30 45 25 32 34 25 31 35 25 43 38 25 41 32 25  %0E%24%15%C8%A2%
0x0110: 43 42 25 43 34 76 25 43 35 25 44 30 0D 0A 43 6F  CB%C4v%C5%D0..Co
0x0120: 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 31 38  ntent-length: 18
0x0130: 39 0D 0A 0D 0A 7F A5 84 D0 08 CF B3 C6 85 ED 49  9..............I
0x0140: 70 50 9E 13 7C 9C E7 E3 07 3F B3 86 0C 4D 77 91  pP..|....?...Mw.
0x0150: D2 3E FD D6 AB 75 2C AF 68 5F B6 B1 B5 E6 28 D5  .>...u,.h_....(.
0x0160: 89 B7 26 5C 49 14 95 19 86 4D E0 34 C2 2E 79 55  ..&\I....M.4..yU
0x0170: C3 0A 6E 29 6D 3E 85 F4 38 49 1A 53 69 8F 25 2F  ..n)m>..8I.Si.%/
0x0180: E6 03 AA 23 7C 69 87 C3 6A 02 6F B7 D1 48 DD F2  ...#|i..j.o..H..
0x0190: 7E B6 80 EF D5 DA D6 B2 6E 6C EE 60 76 75 2D 81  ~.......nl.`vu-.
0x01A0: 08 11 D2 FB AF 98 D1 3E 00 BA DF A7 4D C3 37 38  .......>....M.78
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x01B0: 45 69 6A AF 3F EC 7D 6D CA F4 8B FB 5B B2 BC 13  Eij.?.}m....[...
0x01C0: 11 60 8B B9 1E 04 14 5E E1 23 4E 88 E2 A2 85 07  .`.....^.#N.....
0x01D0: 32 5A 0B CA 9C 45 BE C4 F5 A5 75 98 60 C1 AB 9B  2Z...E....u.`...
0x01E0: 85 96 3C 4B 40 12 2F DD 78 DC 3B 41 78 96 14 6C  ..<K@./.x.;Ax..l
0x01F0: E8 0F                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.470445 10.0.4.155:2010 -> 10.0.9.75:1480
TCP TTL:63 TOS:0x0 ID:26641 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627C2AF9  Ack: 0x1D8B213B  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 11 40 00 3F 06 A5  .....E..Lh.@.?..
0x0020: 89 10 16 04 9B 10 16 09 4B 07 DA 05 C8 62 7C 2A  ........K....b|*
0x0030: F9 1D 8B 21 3B 50 18 44 70 C7 71 00 00 48 54 54  ...!;P.Dp.q..HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.473540 10.0.4.155:2010 -> 10.0.9.75:1480
TCP TTL:63 TOS:0x0 ID:26642 IpLen:20 DgmLen:1484 DF
***AP**F Seq: 0x627C2B1D  Ack: 0x1D8B213B  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 05 CC 68 12 40 00 3F 06 A0  .....E...h.@.?..
0x0020: 08 10 16 04 9B 10 16 09 4B 07 DA 05 C8 62 7C 2B  ........K....b|+
0x0030: 1D 1D 8B 21 3B 50 19 44 70 44 29 00 00 67 BE 83  ...!;P.DpD)..g..
0x0040: D4 07 D1 FE 91 33 D5 6A FC 21 D0 40 3C CE 72 82  .....3.j.!.@<.r.
0x0050: BE 2B C9 CA 68 5E 96 FE E0 A4 F3 76 5A 06 CD 24  .+..h^.....vZ..$
0x0060: 23 C8 5A D1 AA 76 5E 38 5B E2 1E 33 CC 3D 64 9C  #.Z..v^8[..3.=d.
0x0070: 3A D8 02 27 7A B1 30 99 31 84 A2 16 05 88 E6 D1  :..'z.0.1.......
0x0080: 42 78 2C A8 8C AD 41 D5 3A A0 B1 FC D2 66 15 D9  Bx,...A.:....f..
0x0090: 19 62 DE 17 79 4C A9 B9 63 6F 7A 67 CF B3 71 0F  .b..yL..cozg..q.
0x00A0: 59 B9 DA C9 A3 BA 16 45 0D 33 BD A4 E4 A9 44 AB  Y......E.3....D.
0x00B0: 04 14 12 FB C5 D2 70 2C F0 09 5D 47 5E AE 19 11  ......p,..]G^...
0x00C0: A6 7D 05 AD 9C 78 07 E5 04 BC F4 2B 11 66 84 B2  .}...x.....+.f..
0x00D0: EB 0E 26 A7 37 1C FD D7 58 9C C2 A2 FE 33 CE 4B  ..&.7...X....3.K
0x00E0: 09 15 2D 03 24 AB 34 C6 8E 29 1F 69 8A 12 7A 4A  ..-.$.4..).i..zJ
0x00F0: 98 13 38 C9 95 4F 0F D3 BC 32 FC B7 8C 6F 41 15  ..8..O...2...oA.
0x0100: 19 2B 1F E4 7D 2D 6F AC 38 13 5E 0C 98 3E BC 24  .+..}-o.8.^..>.$
0x0110: 52 CE FC 91 29 07 34 95 60 5B 3A E5 9B 50 08 D6  R...).4.`[:..P..
0x0120: BF 77 98 8A AC E5 5F 6A B5 B9 B7 4D D1 34 E0 83  .w...._j...M.4..
0x0130: D6 90 55 6F CB 5C BF 86 4A 95 B3 6F 50 30 C0 10  ..Uo.\..J..oP0..
0x0140: 28 96 A2 2B AF 64 36 3F 1A 32 91 2B 39 49 2A E9  (..+.d6?.2.+9I*.
0x0150: 1A 33 86 52 46 76 35 78 AB 02 F0 FD CF F5 93 84  .3.RFv5x........
0x0160: A0 4C 59 FF AB 2B 3A 28 72 BB 6D 7E 23 94 58 47  .LY..+:(r.m~#.XG
0x0170: 55 D8 C1 A9 15 D0 18 59 69 5C 18 53 0F A4 58 FD  U......Yi\.S..X.
0x0180: B5 56 49 1F AD 47 AE 82 F3 07 54 08 1F 3F 0A D6  .VI..G....T..?..
0x0190: E9 76 57 81 52 6A 40 F7 59 69 41 56 12 9C 47 22  .vW.Rj@.YiAV..G"
0x01A0: 62 AB 8A EF 4D FE D2 EB 5A A0 1E BB 17 AB A2 D1  b...M...Z.......
0x01B0: 1B 35 98 F8 90 1A ED AD 44 69 B2 03 D2 C5 A9 5B  .5......Di.....[
0x01C0: 6C 03 9C B1 07 56 DB 19 EF D9 D6 7F 5A 2C 04 5F  l....V......Z,._
0x01D0: 88 AC AF 94 85 FD 1E 7D 86 36 E3 E3 7E B0 91 E4  .......}.6..~...
0x01E0: B7 26 25 0A 55 79 F8 A4 97 C2 00 6F EC 4B DE 0D  .&%.Uy.....o.K..
0x01F0: 1F 00 FE D2 D4 32 9E BB 32 29 2A 33 B1 5A 84 21  .....2..2)*3.Z.!
0x0200: F3 93 C3 E7 1E FC DB D4 8D 4D 0B 8B 44 C1 4B 03  .........M..D.K.
0x0210: A2 22 1D 0B CE 4E 4C BE 52 78 FD 60 AB 36 92 0D  ."...NL.Rx.`.6..
0x0220: 19 30 D2 8C D6 2C 93 43 5E D5 B7 E4 2A AC 8F 1F  .0...,.C^...*...
0x0230: 9B 76 9F B3 5F 10 F8 B5 80 93 2A C5 B7 D1 CB 1E  .v.._.....*.....
0x0240: 81 03 0E C3 9F BF AE 73 CA 61 AE 6B 78 0F 2D 99  .......s.a.kx.-.
0x0250: C7 59 E1 89 E3 EB 38 32 E4 10 5C AB 40 ED B6 DA  .Y....82..\.@...
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0260: DC DA 28 BE 88 32 33 96 DF FD 75 14 15 4C 86 A5  ..(..23...u..L..
0x0270: 7C 4F C0 EE 43 76 99 7D 7F 02 05 E3 6C 5B 90 50  |O..Cv.}....l[.P
0x0280: 66 23 2A BC EE 8C 4D 97 10 AE 3A 5A 7C 87 91 5E  f#*...M...:Z|..^
0x0290: FA 91 40 C8 26 A4 16 03 CB B6 05 78 D1 BE 5D D5  ..@.&......x..].
0x02A0: C1 83 7D 51 9D 25 5F A4 C5 6E 9A 50 C3 1E 78 DF  ..}Q.%_..n.P..x.
0x02B0: BF F1 DA A3 A9 AD 54 24 25 51 B1 10 0E 95 7C 60  ......T$%Q....|`
0x02C0: 42 A4 69 6A 9E 74 BC A2 54 12 03 0D 87 35 1C 2F  B.ij.t..T....5./
0x02D0: 22 AC 1B 6A EE 92 B1 57 D8 62 FC FD D5 8D 2E BB  "..j...W.b......
0x02E0: 01 52 97 26 5E 83 4B 15 B5 37 B8 AC C4 F1 64 20  .R.&^.K..7....d
0x02F0: A6 11 C8 87 28 AD D7 4E E6 DE 1B 9B D4 9A 72 C0  ....(..N......r.
0x0300: 25 20 C3 09 FB 88 C1 E0 2D 86 3B E9 05 33 D8 3C  % ......-.;..3.<
0x0310: 9E C5 E4 D0 63 60 59 63 66 46 C9 49 82 1B 34 59  ....c`YcfF.I..4Y
0x0320: C9 1C 49 1D 95 AC BA 24 42 7D F6 E2 2D D0 A6 B7  ..I....$B}..-...
0x0330: 1F 12 2C 3D 48 A8 B4 93 EC E5 38 ED 36 E4 77 74  ..,=H.....8.6.wt
0x0340: E1 13 BA 44 EB 64 2B 75 3A 88 9C C1 BA 72 23 4E  ...D.d+u:....r#N
0x0350: AE A5 FB F2 20 43 3C AF 0E C6 39 5D 7A C1 5E 18  .... C<...9]z.^.
0x0360: 60 67 B9 6E 36 16 27 57 59 F9 D3 04 4C AE 68 10  `g.n6.'WY...L.h.
0x0370: AE CB 44 EA A5 97 F5 E2 1D E9 6F FF 3C 71 65 33  ..D.......o.<qe3
0x0380: 6C E1 CE BE F1 87 A0 C4 2C 8A 33 00 29 15 BF 4E  l.......,.3.)..N
0x0390: 9E 20 6F 02 61 5A C0 3B 1F 68 69 C4 11 27 35 FA  . o.aZ.;.hi..'5.
0x03A0: 6C 75 F4 92 57 EB 5B DC 3B E0 7A B9 0A 50 00 D9  lu..W.[.;.z..P..
0x03B0: 9A F6 60 90 1F 45 67 65 74 33 7D C7 DB 95 6B DF  ..`..Eget3}...k.
0x03C0: 52 27 37 5B 36 01 7C 10 81 25 BC 76 BA 05 70 4F  R'7[6.|..%.v..pO
0x03D0: 90 CC CA 21 21 81 65 8A FF 5F 52 05 5B 02 B6 01  ...!!.e.._R.[...
0x03E0: D7 DC 21 35 F8 DD 87 01 DB 76 E4 0E 91 A7 C9 86  ..!5.....v......
0x03F0: 64 57 A0 9D 28 C5 E8 B2 05 7F E0 0D 72 8C A9 50  dW..(.......r..P
0x0400: A9 55 19 BF F6 BA 5B 19 42 23 DF E0 99 1E BF 6F  .U....[.B#.....o
0x0410: 9D 66 DE C5 91 7B 42 40 F4 BC 6A DB 75 FE 0C 5A  .f...{B@..j.u..Z
0x0420: C1 57 BC 9C AE BC BA 71 C3 5B 49 DA 9F 0E C5 82  .W.....q.[I.....
0x0430: 01 C6 89 20 64 5D 14 DD 84 65 D5 BD F2 D7 42 04  ... d]...e....B.
0x0440: F3 AF F2 5D 60 8F 84 D1 C2 04 9D 77 06 6F 1C 2E  ...]`......w.o..
0x0450: 32 54 7C F1 69 B8 50 C9 74 58 12 D6 93 73 99 95  2T|.i.P.tX...s..
0x0460: 92 0D 59 14 0C C6 A6 32 47 E8 CB 07 F0 FE A6 C4  ..Y....2G.......
0x0470: B3 10 01 EB 34 97 0E A4 58 43 0F DA 55 BD DB BB  ....4...XC..U...
0x0480: C1 AB 91 48 2C A1 93 BA 54 1F 00 A6 72 B9 59 57  ...H,...T...r.YW
0x0490: 1D 9E FE 23 1E 88 AE 67 5C 02 D9 A2 71 92 CC AD  ...#...g\...q...
0x04A0: AB 1B 67 64 88 7A 65 D2 F8 3F 4C E2 3D 72 96 57  ..gd.ze..?L.=r.W
0x04B0: 49 F0 3A 13 72 E6 04 93 31 63 E7 17 79 42 AB 48  I.:.r...1c..yB.H
0x04C0: D6 6A 6C C6 95 AB BA 55 7E 21 FB 7A 55 C1 CD C9  .jl....U~!.zU...
0x04D0: 69 2F A2 61 51 BC FA FE AC 7D DF 6C 6A BF E0 6B  i/.aQ....}.lj..k
0x04E0: 65 38 E5 A3 E4 67 8A 55 F4 94 10 4B 3A CB 79 D9  e8...g.U...K:.y.
0x04F0: F8 D2 E6 E9 F2 BB 91 DF 13 8B 29 54 56 45 CD B4  ..........)TVE..
0x0500: 3F 44 D6 BD 89 49 7D 00 51 42 2D 3B 45 0C 31 98  ?D...I}.QB-;E.1.
0x0510: A4 61 A6 C4 5C 44 A9 A7 F4 60 BA 9D 9E 0F 62 86  .a..\D...`....b.
0x0520: 94 A5 26 91 FC E7 27 A3 34 B5 E9 E6 B8 7D 21 D0  ..&...'.4....}!.
0x0530: 78 21 EE E4 9C C9 37 15 B6 F5 6F B7 1F EC 5A 31  x!....7...o...Z1
0x0540: BA 13 84 CB FE 9A 43 AB D4 06 E0 EF 8C 7E 51 BC  ......C......~Q.
0x0550: A3 F7 5B 54 6B 99 AD 29 80 CE 61 A2 ED 77 24 D7  ..[Tk..)..a..w$.
0x0560: EA FD 9F BF B1 94 E0 B3 E7 96 71 12 73 B0 BE 1A  ..........q.s...
0x0570: C4 B7 17 BC C8 E7 BF 4D 36 D3 09 5A 05 E4 42 DD  .......M6..Z..B.
0x0580: B4 06 1D 9F D7 A8 6E 64 58 A5 3F E7 70 E9 DB F6  ......ndX.?.p...
0x0590: 13 51 A5 4A 4B 3F 0F 2E 47 3B 68 CB 0E 05 D8 4C  .Q.JK?..G;h....L
0x05A0: 50 3B C0 94 79 D1 E6 17 3D 40 26 EF 0B EB 13 13  P;..y...=@&.....
0x05B0: D9 85 77 6C CE D2 DB DB D1 52 1E 9A 33 44 DC A4  ..wl.....R..3D..
0x05C0: 1B 65 E7 1F CA A1 39 C9 20 9B CC 0E 91 D3 97 7C  .e....9. ......|
0x05D0: 64 3B 7A 08 97 81 71 EF 98 3E B5 56 1A A4 60 85  d;z...q..>.V..`.
0x05E0: 30                                               0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.475217 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2826 IpLen:20 DgmLen:40 DF
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***A**** Seq: 0x1D8B213B  Ack: 0x627C30C2  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 0A 40 00 80 06 C1  .....E..(..@....
0x0020: B4 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 21  ....K..........!
0x0030: 3B 62 7C 30 C2 50 10 16 D0 8B 4C 00 00 50 4F 53  ;b|0.P....L..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.476650 10.0.9.75:1480 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2827 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D8B213B  Ack: 0x627C30C2  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 0B 40 00 80 06 C1  .....E..(..@....
0x0020: B3 10 16 09 4B 10 16 04 9B 05 C8 07 DA 1D 8B 21  ....K..........!
0x0030: 3B 62 7C 30 C2 50 11 16 D0 8B 4B 00 00 50 4F 53  ;b|0.P....K..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.476974 10.0.4.155:2010 -> 10.0.9.75:1480
TCP TTL:63 TOS:0x0 ID:26643 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627C30C2  Ack: 0x1D8B213C  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 13 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: AB 10 16 04 9B 10 16 09 4B 07 DA 05 C8 62 7C 30  ........K....b|0
0x0030: C2 1D 8B 21 3C 50 10 44 6F 5D AC 00 00           ...!<P.Do]...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.477613 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2828 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D8C77C1  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 0C 40 00 80 06 C1  .....E..0..@....
0x0020: AA 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 77  ....K..........w
0x0030: C1 00 00 00 00 70 02 16 D0 9B 4D 00 00 02 04 05  .....p....M.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.477935 10.0.4.155:2010 -> 10.0.9.75:1481
TCP TTL:63 TOS:0x0 ID:26644 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627D4212  Ack: 0x1D8C77C2  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 14 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: A6 10 16 04 9B 10 16 09 4B 07 DA 05 C9 62 7D 42  ........K....b}B
0x0030: 12 1D 8C 77 C2 60 12 44 70 DE 13 00 00 02 04 05  ...w.`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.478304 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2829 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8C77C2  Ack: 0x627D4213  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 0D 40 00 80 06 C1  .....E..(..@....
0x0020: B1 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 77  ....K..........w
0x0030: C2 62 7D 42 13 50 10 16 D0 23 71 00 00 02 04 05  .b}B.P...#q.....
0x0040: B4 01 01                                         ...
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.478538 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2830 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D8C77C2  Ack: 0x627D4213  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 0E 40 00 80 06 C1  .....E..9..@....
0x0020: 9F 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 77  ....K..........w
0x0030: C2 62 7D 42 13 50 18 16 D0 2F 7E 00 00 50 4F 53  .b}B.P.../~..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.578809 10.0.4.155:2010 -> 10.0.9.75:1481
TCP TTL:63 TOS:0x0 ID:26645 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627D4213  Ack: 0x1D8C77D3  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 15 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: A9 10 16 04 9B 10 16 09 4B 07 DA 05 C9 62 7D 42  ........K....b}B
0x0030: 13 1D 8C 77 D3 50 10 44 70 F5 BF 00 00           ...w.P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.579603 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2831 IpLen:20 DgmLen:477 DF
***AP*** Seq: 0x1D8C77D3  Ack: 0x627D4213  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 01 DD 0B 0F 40 00 80 06 BF  .....E.....@....
0x0020: FA 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 77  ....K..........w
0x0030: D3 62 7D 42 13 50 18 16 D0 6B 38 00 00 55 73 65  .b}B.P...k8..Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket:
0x00C0: 25 46 44 36 78 25 34 30 25 45 45 50 25 39 41 25  %FD6x%40%EEP%9A%
0x00D0: 32 30 25 38 37 25 42 46 36 7D 66 25 30 43 25 39  20%87%BF6}f%0C%9
0x00E0: 42 25 41 42 25 45 46 25 39 37 25 38 37 35 25 39  B%AB%EF%97%875%9
0x00F0: 30 25 39 41 60 76 25 45 46 25 32 30 25 38 35 25  0%9A`v%EF%20%85%
0x0100: 38 43 25 44 41 5E 25 45 46 25 31 30 25 30 39 25  8C%DA^%EF%10%09%
0x0110: 46 46 72 25 39 33 25 38 41 25 38 37 7B 25 42 37  FFr%93%8A%87{%B7
0x0120: 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67 74 68  ..Content-length
0x0130: 3A 20 31 38 35 0D 0A 0D 0A C8 71 DD 17 05 43 B9  : 185.....q...C.
0x0140: E9 78 36 46 63 AC 95 E3 EF 60 DD 0D CA 9E F5 6C  .x6Fc....`.....l
0x0150: 4F 7D 6C DE 1B 44 24 96 A2 EE 9D 7C CC 42 AE B8  O}l..D$....|.B..
0x0160: 7E 25 CE EC 73 C9 FA C7 AC E6 1F 64 7A 37 D2 49  ~%..s......dz7.I
0x0170: 99 37 1F 14 D7 40 72 2E A2 8A 02 89 B2 53 E4 62  .7...@r......S.b
0x0180: B7 7E E4 9B 84 82 0E 3C 0C 8B 73 2C F3 94 E4 85  .~.....<..s,....
0x0190: 4A E2 28 E4 0C 72 F5 F6 9F 2C 44 90 1B 8F 1C A1  J.(..r...,D.....
0x01A0: 02 AC D7 EF 02 9C 08 C8 2C D7 39 D8 09 FE FD 18  ........,.9.....
0x01B0: 13 EA C5 DD BF 12 6A 34 29 39 4D 43 35 A9 C5 B4  ......j4)9MC5...
0x01C0: 29 6E AA 15 26 E0 25 A3 56 30 D6 66 1E 6F 52 E6  )n..&.%.V0.f.oR.
0x01D0: 61 D1 A6 8E 05 CB C4 1C A7 D1 EF 52 52 BA D5 53  a..........RR..S
0x01E0: F8 59 63 21 13 77 B2 12 FA 9D F4 76 0F 1D 68 2E  .Yc!.w.....v..h.
0x01F0: 00 8D                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
04/04-10:43:28.580356 10.0.4.155:2010 -> 10.0.9.75:1481
TCP TTL:63 TOS:0x0 ID:26646 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627D4213  Ack: 0x1D8C7988  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 16 40 00 3F 06 A5  .....E..Lh.@.?..
0x0020: 84 10 16 04 9B 10 16 09 4B 07 DA 05 C9 62 7D 42  ........K....b}B
0x0030: 13 1D 8C 79 88 50 18 44 70 58 07 00 00 48 54 54  ...y.P.DpX...HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.583321 10.0.4.155:2010 -> 10.0.9.75:1481
TCP TTL:63 TOS:0x0 ID:26647 IpLen:20 DgmLen:1080 DF
***AP**F Seq: 0x627D4237  Ack: 0x1D8C7988  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 04 38 68 17 40 00 3F 06 A1  .....E..8h.@.?..
0x0020: 97 10 16 04 9B 10 16 09 4B 07 DA 05 C9 62 7D 42  ........K....b}B
0x0030: 37 1D 8C 79 88 50 19 44 70 3F 68 00 00 D0 6A DA  7..y.P.Dp?h...j.
0x0040: 13 0A 5D F4 BE 47 8A 20 94 66 86 81 BF 18 0F E8  ..]..G. .f......
0x0050: 19 F7 AD 20 E0 BC AC 3E D1 4C B4 10 7A BE 15 1D  ... ...>.L..z...
0x0060: F2 96 4B 4B 90 5C 03 F6 E0 E8 E2 A2 10 3C AC 6C  ..KK.\.......<.l
0x0070: CB CB 72 44 04 63 54 81 C0 38 1F E4 75 84 A4 64  ..rD.cT..8..u..d
0x0080: 94 BC 23 07 A6 D4 39 67 5F 3D 8E 9F 28 AF F7 DF  ..#...9g_=..(...
0x0090: 5C A6 89 7A 7D F2 53 A0 AE 0A E4 5F A3 6B 5B B7  \..z}.S...._.k[.
0x00A0: DD 8B 35 FA 3D 06 C7 18 5D A8 3F 12 C5 70 5E 76  ..5.=...].?..p^v
0x00B0: 00 F7 8E 84 28 4F 26 1F 6E 5C 58 A3 51 F9 E3 20  ....(O&.n\X.Q..
0x00C0: 32 52 A8 04 F2 C5 1F 4B D9 87 BB 71 98 13 17 D5  2R.....K...q....
0x00D0: EF 94 16 73 B1 CE BF 3B 68 88 95 7F A0 AC E6 A5  ...s...;h.......
0x00E0: D8 40 1E 73 05 F7 6B 6B 42 6A 4E 8C E3 AC AD 2E  .@.s..kkBjN.....
0x00F0: DC C5 22 C1 67 A3 E9 90 B0 90 E4 F6 A7 3E 17 B3  ..".g........>..
0x0100: 90 66 91 A2 1D A3 70 85 0E 83 8C 5C E5 73 F2 95  .f....p....\.s..
0x0110: 14 31 79 19 F6 08 02 D5 C4 A5 70 E4 22 A8 74 52  .1y.......p.".tR
0x0120: A9 3C 8A 67 05 87 1C F0 85 B0 00 19 F8 4E A5 01  .<.g.........N..
0x0130: 07 71 62 DD 52 30 E1 FA CF AE 4E B3 A7 3C FA 3E  .qb.R0....N..<.>
0x0140: D3 DF B5 7C DF 3A 34 E7 B3 A0 59 CA F4 9C A2 7C  ...|.:4...Y....|
0x0150: 32 25 0D F8 EB 63 91 32 9C A5 21 52 72 76 DA F3  2%...c.2..!Rrv..
0x0160: 5E 10 19 A0 8B 55 31 3B 96 68 BA 10 42 83 EF A8  ^....U1;.h..B...
0x0170: 42 BD 10 D4 7C 5A BF 11 A6 81 57 13 57 32 3A 4D  B...|Z....W.W2:M
0x0180: 09 40 24 A1 DF D4 01 7B 49 84 8A 13 06 C2 76 10  .@$....{I.....v.
0x0190: 05 1D 64 8B F0 72 72 23 A4 48 DA 9E 51 A3 E0 01  ..d..rr#.H..Q...
0x01A0: FE EC 6B B9 DC F5 EF 54 F9 1F 13 1E 33 CA B6 1D  ..k....T....3...
0x01B0: 97 30 8F 90 07 AB 44 96 A4 DC 01 10 F8 AA CC 33  .0....D........3
0x01C0: 3D A7 CE CD 0F 73 74 16 98 E3 A0 22 23 E5 5F FD  =....st...."#._.
0x01D0: D7 B7 BA A9 1F 1F 05 64 73 1B 84 AA 7C FB 64 18  .......ds...|.d.
0x01E0: 17 3D CF 3B DD 7B 9A A5 92 1F A4 0F EA 3B D8 34  .=.;.{.......;.4
0x01F0: 91 16 58 EC A4 4F 39 E6 75 93 9E 36 38 BC F4 F1  ..X..O9.u..68...
0x0200: DB C6 E4 17 7F B5 1F 3D BB 72 38 A5 6F 05 AF 01  .......=.r8.o...
0x0210: 19 C7 DF AE AF 27 B0 97 42 1E AE E3 E7 2A 48 92  .....'..B....*H.
0x0220: 04 6F 73 3F 31 69 5E 9B BB 20 88 59 79 FE F4 9B  .os?1i^.. .Yy...
0x0230: CB 8F 21 04 FC 67 B6 A0 5F 31 A4 02 09 E9 EE DC  ..!..g.._1......
0x0240: 49 2C 36 CC 64 1F A8 D4 E5 83 8F 31 C6 75 D0 4D  I,6.d......1.u.M
0x0250: 4B 25 0D EE D5 5C 28 83 11 63 99 BB 48 FC 48 FD  K%...\(..c..H.H.
0x0260: AF 8D A9 D5 36 00 E6 EE 3F 8A 92 9B 51 0A 4B A2  ....6...?...Q.K.
0x0270: 7C 63 38 C5 C7 47 C2 E9 F0 1B 48 4E 94 E8 95 DE  |c8..G....HN....
0x0280: 8B 57 22 8C FB CB E7 02 18 BC 67 2B B5 1D 3E B9  .W".......g+..>.
0x0290: DB CF C1 41 DE 06 16 BB 02 2D 34 E5 C6 E1 85 ED  ...A.....-4.....
0x02A0: CE 13 A0 52 91 AC 8C 84 45 0F 37 84 D8 FB B2 55  ...R....E.7....U
0x02B0: 47 2D EB 54 ED E7 E4 E9 E0 7A 90 AE 29 86 AB 2E  G-.T.....z..)...
0x02C0: 66 86 E9 23 C5 3F 94 C4 E7 F0 B0 8F 21 85 EE 98  f..#.?......!...
0x02D0: 5B 71 A6 11 82 1E 04 19 52 E6 BD 62 7D DD 47 81  [q......R..b}.G.
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x02E0: 84 37 2B 77 BC 27 D4 26 CB 1B 01 BD 2A 2E FE 78  .7+w.'.&....*..x
0x02F0: 1D 32 72 70 C4 BA 70 11 6E 40 25 F5 F3 A0 DB F3  .2rp..p.n@%.....
0x0300: F5 89 CC 89 10 91 84 DC 44 5E 15 CD 3C E1 DA BD  ........D^..<...
0x0310: 10 B7 49 E7 55 71 A8 B2 97 2C FF 8F 5B B2 4D CE  ..I.Uq...,..[.M.
0x0320: 4C 63 2B 13 4B 1F 89 82 C8 61 33 61 B5 59 6E B4  Lc+.K....a3a.Yn.
0x0330: 6A B0 B5 E3 0A A9 76 CA 8C 96 A6 0E 01 A3 CF A0  j.....v.........
0x0340: A9 55 DD 16 CE 9E 06 1D 87 DA D4 C2 69 3F B9 C7  .U..........i?..
0x0350: BA 01 67 43 95 C0 2D B1 D5 9D 0E 6A B0 01 40 B0  ..gC..-....j..@.
0x0360: 41 74 09 52 CA 81 E2 07 73 A7 DD C5 43 B6 2F 7E  At.R....s...C./~
0x0370: 24 74 1B 32 3E CE 99 BA 94 BD 61 5A 27 10 25 37  $t.2>.....aZ'.%7
0x0380: 23 24 C8 F4 3F E8 CB 1F 4D 3B 88 68 B8 D1 24 10  #$..?...M;.h..$.
0x0390: F5 79 46 67 4D 20 49 9F 9B 2E 2B BB 0B EB EB 09  .yFgM I...+.....
0x03A0: 2E 19 BE E4 BB 5C CA 86 99 09 64 18 1A 01 F0 9F  .....\....d.....
0x03B0: 7C A0 BB 16 A7 25 89 42 70 7E D5 87 B6 06 C5 6E  |....%.Bp~.....n
0x03C0: EE 5C 1F 6F C0 C9 26 13 D6 5E BF 94 9D C4 F5 6C  .\.o..&..^.....l
0x03D0: 67 81 42 62 46 25 A1 E5 6C B2 58 75 F5 AD E3 57  g.BbF%..l.Xu...W
0x03E0: F4 E1 0A 09 5E 2F 84 FF 77 FA 42 E9 C9 A8 DB 26  ....^/..w.B....&
0x03F0: 3A 40 2D 25 E5 04 0D A4 85 B0 CF 73 DF 13 CC 03  :@-%.......s....
0x0400: 42 71 41 A2 8A B4 B7 59 FD C1 F3 9A 4E 22 18 FE  BqA....Y....N"..
0x0410: 08 6C 15 A7 0B 52 D7 89 5D 8E 4D 52 E6 2C 5D 8D  .l...R..].MR.,].
0x0420: FA E3 50 46 12 2C B1 5E 3F 35 0D CD 8E 81 ED 70  ..PF.,.^?5.....p
0x0430: B2 B5 4B 0E BF B2 37 04 89 85 C9 A9 30 CA 5A 0D  ..K...7.....0.Z.
0x0440: EF 4D D4 D5 53 A7 6F 03 19 C8 A3 1E DB           .M..S.o......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.584650 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2832 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8C7988  Ack: 0x627D4648  Win: 0x129C  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 10 40 00 80 06 C1  .....E..(..@....
0x0020: AE 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 79  ....K..........y
0x0030: 88 62 7D 46 48 50 10 12 9C 21 AA 00 00 50 4F 53  .b}FHP...!...POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.585827 10.0.9.75:1481 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2833 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D8C7988  Ack: 0x627D4648  Win: 0x129C  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 11 40 00 80 06 C1  .....E..(..@....
0x0020: AD 10 16 09 4B 10 16 04 9B 05 C9 07 DA 1D 8C 79  ....K..........y
0x0030: 88 62 7D 46 48 50 11 12 9C 21 A9 00 00 50 4F 53  .b}FHP...!...POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.586170 10.0.4.155:2010 -> 10.0.9.75:1481
TCP TTL:63 TOS:0x0 ID:26648 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627D4648  Ack: 0x1D8C7989  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 18 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: A6 10 16 04 9B 10 16 09 4B 07 DA 05 C9 62 7D 46  ........K....b}F
0x0030: 48 1D 8C 79 89 50 10 44 6F EF D5 00 00           H..y.P.Do....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.586838 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2834 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D8D5E36  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 12 40 00 80 06 C1  .....E..0..@....
0x0020: A4 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  ....K..........^
0x0030: 36 00 00 00 00 70 02 16 D0 B4 D6 00 00 02 04 05  6....p..........
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.587232 10.0.4.155:2010 -> 10.0.9.75:1482
TCP TTL:63 TOS:0x0 ID:26649 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627DDF68  Ack: 0x1D8D5E37  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 19 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: A1 10 16 04 9B 10 16 09 4B 07 DA 05 CA 62 7D DF  ........K....b}.
0x0030: 68 1D 8D 5E 37 60 12 44 70 5A 46 00 00 02 04 05  h..^7`.DpZF.....
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.587616 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2835 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8D5E37  Ack: 0x627DDF69  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 13 40 00 80 06 C1  .....E..(..@....
0x0020: AB 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  ....K..........^
0x0030: 37 62 7D DF 69 50 10 16 D0 9F A3 00 00 02 04 05  7b}.iP..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.587808 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2836 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1D8D5E37  Ack: 0x627DDF69  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 3D 0B 14 40 00 80 06 C1  .....E..=..@....
0x0020: 95 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  ....K..........^
0x0030: 37 62 7D DF 69 50 18 16 D0 C9 DD 00 00 50 4F 53  7b}.iP.......POS
0x0040: 54 20 2F 74 69 6D 65 20 48 54 54 50 2F 31 2E 30  T /time HTTP/1.0
0x0050: 0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.678827 10.0.4.155:2010 -> 10.0.9.75:1482
TCP TTL:63 TOS:0x0 ID:26650 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627DDF69  Ack: 0x1D8D5E4C  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 1A 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: A4 10 16 04 9B 10 16 09 4B 07 DA 05 CA 62 7D DF  ........K....b}.
0x0030: 69 1D 8D 5E 4C 50 10 44 70 71 EE 00 00           i..^LP.Dpq...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.679383 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2837 IpLen:20 DgmLen:166 DF
***AP*** Seq: 0x1D8D5E4C  Ack: 0x627DDF69  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 A6 0B 15 40 00 80 06 C1  .....E.....@....
0x0020: 2B 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  +...K..........^
0x0030: 4C 62 7D DF 69 50 18 16 D0 0B EF 00 00 55 73 65  Lb}.iP.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
```

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0060: 6E 64 6F 77 73 29 0D 0A 41 63 63 65 70 74 3A 20  ndows)..Accept:
0x0070: 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70  */*..Content-typ
0x0080: 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  e: application/x
0x0090: 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63  -www-form-urlenc
0x00A0: 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65  oded..Content-le
0x00B0: 6E 67 74 68 3A 20 30 0D 0A 0D 0A                 ngth: 0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.679842 10.0.4.155:2010 -> 10.0.9.75:1482
TCP TTL:63 TOS:0x0 ID:26651 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627DDF69  Ack: 0x1D8D5ECA  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 1B 40 00 3F 06 A5  .....E..Lh.@.?..
0x0020: 7F 10 16 04 9B 10 16 09 4B 07 DA 05 CA 62 7D DF  ........K....b}.
0x0030: 69 1D 8D 5E CA 50 18 44 70 D5 6C 00 00 48 54 54  i..^.P.Dp.l..HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.679844 10.0.4.155:2010 -> 10.0.9.75:1482
TCP TTL:63 TOS:0x0 ID:26652 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x627DDF8D  Ack: 0x1D8D5ECA  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 1C 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: A2 10 16 04 9B 10 16 09 4B 07 DA 05 CA 62 7D DF  ........K....b}.
0x0030: 8D 1D 8D 5E CA 50 11 44 70 71 4B 00 00           ...^.P.DpqK..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.680345 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2838 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8D5ECA  Ack: 0x627DDF8E  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 16 40 00 80 06 C1  .....E..(..@....
0x0020: A8 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  ....K..........^
0x0030: CA 62 7D DF 8E 50 10 16 AC 9F 0F 00 00 55 73 65  .b}..P.......Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.680576 10.0.9.75:1482 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2839 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D8D5ECA  Ack: 0x627DDF8E  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 17 40 00 80 06 C1  .....E..(..@....
0x0020: A7 10 16 09 4B 10 16 04 9B 05 CA 07 DA 1D 8D 5E  ....K..........^
0x0030: CA 62 7D DF 8E 50 11 16 AC 9F 0E 00 00 55 73 65  .b}..P.......Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.680907 10.0.4.155:2010 -> 10.0.9.75:1482
TCP TTL:63 TOS:0x0 ID:26653 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627DDF8E  Ack: 0x1D8D5ECB  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 1D 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: A1 10 16 04 9B 10 16 09 4B 07 DA 05 CA 62 7D DF  ........K....b}.
0x0030: 8E 1D 8D 5E CB 50 10 44 70 71 4A 00 00           ...^.P.DpqJ..
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.681481 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2840 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D8EA1DB  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 18 40 00 80 06 C1  .....E..0..@....
0x0020: 9E 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A1  ....K...........
0x0030: DB 00 00 00 00 70 02 16 D0 71 2F 00 00 02 04 05  .....p...q/.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.681807 10.0.4.155:2010 -> 10.0.9.75:1483
TCP TTL:63 TOS:0x0 ID:26654 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x627E7A13  Ack: 0x1D8EA1DC  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 1E 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: 9C 10 16 04 9B 10 16 09 4B 07 DA 05 CB 62 7E 7A  ........K....b~z
0x0030: 13 1D 8E A1 DC 60 12 44 70 7B F3 00 00 02 04 05  .....`.Dp{......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.682178 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2841 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8EA1DC  Ack: 0x627E7A14  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 19 40 00 80 06 C1  .....E..(..@....
0x0020: A5 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A1  ....K...........
0x0030: DC 62 7E 7A 14 50 10 16 D0 C1 50 00 00 02 04 05  .b~z.P....P.....
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.682408 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2842 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D8EA1DC  Ack: 0x627E7A14  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 1A 40 00 80 06 C1  .....E..9..@....
0x0020: 93 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A1  ....K...........
0x0030: DC 62 7E 7A 14 50 18 16 D0 CD 5D 00 00 50 4F 53  .b~z.P....]..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.778793 10.0.4.155:2010 -> 10.0.9.75:1483
TCP TTL:63 TOS:0x0 ID:26655 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627E7A14  Ack: 0x1D8EA1ED  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 1F 40 00 3F 06 A5  .....E..(h.@.?..
0x0020: 9F 10 16 04 9B 10 16 09 4B 07 DA 05 CB 62 7E 7A  ........K....b~z
0x0030: 14 1D 8E A1 ED 50 10 44 70 93 9F 00 00           .....P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.779598 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2843 IpLen:20 DgmLen:483 DF
***AP*** Seq: 0x1D8EA1ED  Ack: 0x627E7A14  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0010: 00 00 00 08 00 45 00 01 E3 0B 1B 40 00 80 06 BF  .....E.....@....
0x0020: E8 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A1  ....K...........
0x0030: ED 62 7E 7A 14 50 18 16 D0 A7 EB 00 00 55 73 65  .b~z.P.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket: 
0x00C0: 7C 2F 25 44 45 66 25 32 42 7E 25 45 35 25 41 37  |/%DEf%2B~%E5%A7
0x00D0: 61 25 30 42 25 42 42 5A 47 25 44 30 25 46 34 2D  a%0B%BBZG%D0%F4-
0x00E0: 25 44 38 25 44 38 25 30 43 76 46 25 30 30 53 25  %D8%D8%0CvF%00S%
0x00F0: 32 43 21 25 41 35 50 25 42 46 25 45 38 51 25 39  2C!%A5P%BF%E8Q%9
0x0100: 31 7E 6A 2E 25 44 39 53 68 25 46 43 25 38 31 25  1~j.%D9Sh%FC%81%
0x0110: 33 46 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67  3F..Content-leng
0x0120: 74 68 3A 20 32 30 35 0D 0A 0D 0A 91 6D 7F CE 10  th: 205.....m...
0x0130: 41 30 BD F5 3D 63 91 AE CA 17 DE 26 9D AA BE 62  A0..=c.....&...b
0x0140: E9 DE FD B2 5B A8 B5 28 1B EA 51 59 6D CD DD 87  ....[..(..QYm...
0x0150: 15 91 B7 FF 6F 84 65 2E 4B 63 F9 B5 C7 B2 2C 84  ....o.e.Kc....,.
0x0160: 4A FB D5 B8 F0 EE 49 FC CA 13 FA 4F F9 73 91 2D  J.....I....O.s.-
0x0170: 9C 96 85 63 E5 E4 9D 64 12 DC 38 E2 82 36 07 AE  ...c...d..8..6..
0x0180: 35 92 F0 F9 62 52 20 FA 5A FD C4 98 FC 3C E6 67  5...bR .Z....<.g
0x0190: 97 72 11 EA 31 06 49 65 20 99 A8 8C 8C AE 6D BB  .r..1.Ie .....m.
0x01A0: 7B E9 B1 0A EF 0A 29 12 48 34 74 AB C4 10 FD 1B  {.....).H4t.....
0x01B0: A7 F1 22 90 64 C9 F8 C3 B8 81 C9 27 CA 40 76 EB  ..".d......'.@v.
0x01C0: 3D 66 77 A8 B8 C6 CA 5D 68 40 72 C2 03 4B BC A7  =fw....]h@r..K..
0x01D0: 1A 96 F7 EF 19 4E E4 FC 43 49 0B 37 A8 8B 43 FA  .....N..CI.7..C.
0x01E0: 3C BA 37 E3 A1 8B 55 EA 58 46 72 24 CB E0 7B EA  <.7...U.XFr$..{.
0x01F0: 07 41 45 B4 F0 7E C2 D3                          .AE..~..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.780376 10.0.4.155:2010 -> 10.0.9.75:1483
TCP TTL:63 TOS:0x0 ID:26656 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x627E7A14  Ack: 0x1D8EA3A8  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 20 40 00 3F 06 A5  .....E..Lh @.?..
0x0020: 7A 10 16 04 9B 10 16 09 4B 07 DA 05 CB 62 7E 7A  z.......K....b~z
0x0030: 14 1D 8E A3 A8 50 18 44 70 F5 E0 00 00 48 54 54  .....P.Dp....HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.783020 10.0.4.155:2010 -> 10.0.9.75:1483
TCP TTL:63 TOS:0x0 ID:26657 IpLen:20 DgmLen:360 DF
***AP**F Seq: 0x627E7A38  Ack: 0x1D8EA3A8  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 01 68 68 21 40 00 3F 06 A4  .....E..hh!@.?..
0x0020: 5D 10 16 04 9B 10 16 09 4B 07 DA 05 CB 62 7E 7A  ].......K....b~z
0x0030: 38 1D 8E A3 A8 50 19 44 70 52 35 00 00 89 76 78  8....P.DpR5...vx
0x0040: CA 1F 5F 7D EA B6 81 2C 5F 5A 50 AE 22 8E E5 43  .._}...,_ZP."..C
0x0050: E6 84 4A F5 7A FF A4 19 C6 45 FB 41 00 1D 78 4E  ..J.z....E.A..xN
0x0060: B5 C1 93 27 96 3D A0 10 E0 79 28 89 15 86 01 5F  ...'.=...y(...._
0x0070: BE 1A 0F 3E 0B AE B2 80 F9 D8 29 01 D2 64 09 C8  ...>......)..d..
0x0080: 5B E9 26 18 6A 69 DC 8D 97 72 08 E4 B3 39 EA 47  [.&.ji...r...9.G
0x0090: 4A A8 AE 72 61 EB A7 BB 68 32 BA D2 8B ED E4 F5  J..ra...h2......
0x00A0: BE 72 88 B2 5B 47 ED F4 F4 16 EE 23 68 71 FF 48  .r..[G.....#hq.H
0x00B0: 86 E4 C7 AD A8 DC 8A BA 6C A8 FA B5 8B 96 6C 22  ........l.....l"
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x00C0: 4D 5A 91 48 D5 0F 20 B2 AB 24 4B 82 9C F8 78 C5  MZ.H.. ..$K...x.
0x00D0: D7 E8 E4 47 8B E2 B3 C1 3A 10 27 73 38 8C 70 C1  ...G....:.'s8.p.
0x00E0: F2 23 A9 7C BC 94 2F 16 ED 19 D8 B5 36 38 BD 76  .#.|../.....68.v
0x00F0: BB 43 1B 7B 29 E5 F9 D3 5B 25 48 88 57 A1 C9 70  .C.{)...[%H.W..p
0x0100: 83 BC 41 48 10 0B 82 65 E7 5D 41 9E 84 E2 F4 F2  ..AH...e.]A.....
0x0110: 38 05 95 6B 8F 22 2C EE 47 64 E0 F2 66 E9 87 47  8..k.",.Gd..f..G
0x0120: F7 2F 38 68 B1 1F F8 39 E6 01 01 28 AD 2F F2 C8  ./8h...9...(./..
0x0130: 95 53 04 E8 89 AB 59 EA 69 CC 82 23 9E FA 86 D9  .S....Y.i..#....
0x0140: 89 A9 A1 6F 02 3D B4 91 AF 96 83 F1 F8 AF 61 77  ...o.=........aw
0x0150: E4 16 01 19 41 C2 C0 B0 75 B0 77 3F 18 6C EA 11  ....A...u.w?.l..
0x0160: AC 36 56 35 93 86 B7 08 4A 00 5B 79 BF 3D 17 89  .6V5....J.[y.=..
0x0170: 84 66 96 56 20 8D 08 94 AF AA 7C BF 7F           .f.V .....|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.783697 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2844 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D8EA3A8  Ack: 0x627E7B79  Win: 0x156C  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 1C 40 00 80 06 C1  .....E..(..@....
0x0020: A2 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A3  ....K...........
0x0030: A8 62 7E 7B 79 50 10 15 6C BF 83 00 00 50 4F 53  .b~{yP..l....POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.784193 10.0.9.75:1483 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2845 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D8EA3A8  Ack: 0x627E7B79  Win: 0x156C  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 1D 40 00 80 06 C1  .....E..(..@....
0x0020: A1 10 16 09 4B 10 16 04 9B 05 CB 07 DA 1D 8E A3  ....K...........
0x0030: A8 62 7E 7B 79 50 11 15 6C BF 82 00 00 50 4F 53  .b~{yP..l....POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:28.784517 10.0.4.155:2010 -> 10.0.9.75:1483
TCP TTL:63 TOS:0x0 ID:26658 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x627E7B79  Ack: 0x1D8EA3A9  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 22 40 00 3F 06 A5  .....E..(h"@.?..
0x0020: 9C 10 16 04 9B 10 16 09 4B 07 DA 05 CB 62 7E 7B  ........K....b~{
0x0030: 79 1D 8E A3 A9 50 10 44 6F 90 7F 00 00           y....P.Do....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.126261 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2846 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D9180FA  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 1E 40 00 80 06 C1  .....E..0..@....
0x0020: 98 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 80  ....K...........
0x0030: FA 00 00 00 00 70 02 16 D0 92 0C 00 00 02 04 05  .....p..........
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.126603 10.0.4.155:2010 -> 10.0.9.75:1484
TCP TTL:63 TOS:0x0 ID:26659 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62809F6C  Ack: 0x1D9180FB  Win: 0x4470  TcpLen: 24
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 23 40 00 3F 06 A5  .....E..,h#@.?..
0x0020: 97 10 16 04 9B 10 16 09 4B 07 DA 05 CC 62 80 9F  ........K....b..
0x0030: 6C 1D 91 80 FB 60 12 44 70 77 75 00 00 02 04 05  l....`.Dpwu.....
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.127033 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2847 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D9180FB  Ack: 0x62809F6D  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 1F 40 00 80 06 C1  .....E..(..@....
0x0020: 9F 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 80  ....K...........
0x0030: FB 62 80 9F 6D 50 10 16 D0 BC D2 00 00 02 04 05  .b..mP..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.127271 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2848 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1D9180FB  Ack: 0x62809F6D  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 3D 0B 20 40 00 80 06 C1  .....E..=. @....
0x0020: 89 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 80  ....K...........
0x0030: FB 62 80 9F 6D 50 18 16 D0 E7 0C 00 00 50 4F 53  .b..mP.......POS
0x0040: 54 20 2F 74 69 6D 65 20 48 54 54 50 2F 31 2E 30  T /time HTTP/1.0
0x0050: 0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.218716 10.0.4.155:2010 -> 10.0.9.75:1484
TCP TTL:63 TOS:0x0 ID:26660 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62809F6D  Ack: 0x1D918110  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 24 40 00 3F 06 A5  .....E..(h$@.?..
0x0020: 9A 10 16 04 9B 10 16 09 4B 07 DA 05 CC 62 80 9F  ........K....b..
0x0030: 6D 1D 91 81 10 50 10 44 70 8F 1D 00 00           m....P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.219308 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2849 IpLen:20 DgmLen:166 DF
***AP*** Seq: 0x1D918110  Ack: 0x62809F6D  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 A6 0B 21 40 00 80 06 C1  .....E....!@....
0x0020: 1F 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 81  ....K...........
0x0030: 10 62 80 9F 6D 50 18 16 D0 29 1E 00 00 55 73 65  .b..mP...)...Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 41 63 63 65 70 74 3A 20  ndows)..Accept:
0x0070: 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70  */*..Content-typ
0x0080: 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  e: application/x
0x0090: 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63  -www-form-urlenc
0x00A0: 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65  oded..Content-le
0x00B0: 6E 67 74 68 3A 20 30 0D 0A 0D 0A                 ngth: 0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.219728 10.0.4.155:2010 -> 10.0.9.75:1484
TCP TTL:63 TOS:0x0 ID:26661 IpLen:20 DgmLen:76 DF
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***AP*** Seq: 0x62809F6D  Ack: 0x1D91818E  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 25 40 00 3F 06 A5  .....E..Lh%@.?..
0x0020: 75 10 16 04 9B 10 16 09 4B 07 DA 05 CC 62 80 9F  u.......K....b..
0x0030: 6D 1D 91 81 8E 50 18 44 70 F2 9B 00 00 48 54 54  m....P.Dp....HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.219730 10.0.4.155:2010 -> 10.0.9.75:1484
TCP TTL:63 TOS:0x0 ID:26662 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x62809F91  Ack: 0x1D91818E  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 26 40 00 3F 06 A5  .....E..(h&@.?..
0x0020: 98 10 16 04 9B 10 16 09 4B 07 DA 05 CC 62 80 9F  ........K....b..
0x0030: 91 1D 91 81 8E 50 11 44 70 8E 7A 00 00           .....P.Dp.z..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.220265 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2850 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D91818E  Ack: 0x62809F92  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 22 40 00 80 06 C1  .....E..(."@....
0x0020: 9C 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 81  ....K...........
0x0030: 8E 62 80 9F 92 50 10 16 AC BC 3E 00 00 55 73 65  .b...P....>..Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.220499 10.0.9.75:1484 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2851 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D91818E  Ack: 0x62809F92  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 23 40 00 80 06 C1  .....E..(.#@....
0x0020: 9B 10 16 09 4B 10 16 04 9B 05 CC 07 DA 1D 91 81  ....K...........
0x0030: 8E 62 80 9F 92 50 11 16 AC BC 3D 00 00 55 73 65  .b...P....=..Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.220821 10.0.4.155:2010 -> 10.0.9.75:1484
TCP TTL:63 TOS:0x0 ID:26663 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62809F92  Ack: 0x1D91818F  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 27 40 00 3F 06 A5  .....E..(h'@.?..
0x0020: 97 10 16 04 9B 10 16 09 4B 07 DA 05 CC 62 80 9F  ........K....b..
0x0030: 92 1D 91 81 8F 50 10 44 70 8E 79 00 00           .....P.Dp.y..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.221494 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2852 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D92D202  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 24 40 00 80 06 C1  .....E..0.$@....
0x0020: 92 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D2  ....K...........
0x0030: 02 00 00 00 00 70 02 16 D0 41 02 00 00 02 04 05  .....p...A......
0x0040: B4 01 01 04 02                                   .....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.221771 10.0.4.155:2010 -> 10.0.9.75:1485
TCP TTL:63 TOS:0x0 ID:26664 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62819E0F  Ack: 0x1D92D203  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 28 40 00 3F 06 A5  .....E..,h(@.?..
0x0020: 92 10 16 04 9B 10 16 09 4B 07 DA 05 CD 62 81 9E  ........K....b..
0x0030: 0F 1D 92 D2 03 60 12 44 70 27 C7 00 00 02 04 05  .....`.Dp'......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.222140 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2853 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D92D203  Ack: 0x62819E10  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 25 40 00 80 06 C1  .....E..(.%@....
0x0020: 99 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D2  ....K...........
0x0030: 03 62 81 9E 10 50 10 16 D0 6D 24 00 00 02 04 05  .b...P...m$.....
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.222372 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2854 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D92D203  Ack: 0x62819E10  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 26 40 00 80 06 C1  .....E..9.&@....
0x0020: 87 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D2  ....K...........
0x0030: 03 62 81 9E 10 50 18 16 D0 79 31 00 00 50 4F 53  .b...P...y1..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.318718 10.0.4.155:2010 -> 10.0.9.75:1485
TCP TTL:63 TOS:0x0 ID:26665 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62819E10  Ack: 0x1D92D214  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 29 40 00 3F 06 A5  .....E..(h)@.?..
0x0020: 95 10 16 04 9B 10 16 09 4B 07 DA 05 CD 62 81 9E  ........K....b..
0x0030: 10 1D 92 D2 14 50 10 44 70 3F 73 00 00           .....P.Dp?s..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.319606 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2855 IpLen:20 DgmLen:519 DF
***AP*** Seq: 0x1D92D214  Ack: 0x62819E10  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 02 07 0B 27 40 00 80 06 BF  .....E....'@....
0x0020: B8 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D2  ....K...........
0x0030: 14 62 81 9E 10 50 18 16 D0 2A 06 00 00 55 73 65  .b...P...*...Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket:
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x00C0: 25 45 32 25 44 36 57 25 46 44 25 31 30 25 41 35  %E2%D6W%FD%10%A5
0x00D0: 25 44 45 69 25 38 39 7A 25 44 31 25 30 37 54 25  %DEi%89z%D1%07T%
0x00E0: 30 41 69 25 42 33 54 4F 25 38 35 25 30 42 33 25  0Ai%B3TO%85%0B3%
0x00F0: 45 31 7E 25 41 41 25 32 30 25 41 43 25 43 38 25  E1~%AA%20%AC%C8%
0x0100: 43 43 58 66 25 43 41 25 44 30 35 25 38 37 25 32  CCXf%CA%D05%87%2
0x0110: 30 25 38 30 25 30 46 4C 25 42 33 7B 0D 0A 43 6F  0%80%0FL%B3{..Co
0x0120: 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 32 33  ntent-length: 23
0x0130: 31 0D 0A 0D 0A 4B CB 02 2A 60 73 68 28 5F 31 00  1....K..*`sh(_1.
0x0140: 6E A5 54 20 87 26 53 B3 1C D7 32 00 99 14 8A D8  n.T .&S...2.....
0x0150: 96 E6 37 A6 ED D4 A9 54 F6 DF D9 04 BC C8 A9 91  ..7....T........
0x0160: B2 0C BB 92 A6 7A CF 42 C5 CE EA 0E 57 92 5D 21  .....z.B....W.]!
0x0170: 11 B0 5F 61 E6 99 B7 19 14 5F C0 98 CF BC 10 4E  .._a....._.....N
0x0180: B9 02 06 A0 EB 0D 2A FA 4E 15 E1 86 8D 58 60 CB  ......*.N....X`.
0x0190: 08 C6 41 42 C4 32 E3 5B 62 59 B8 88 27 BF A8 90  ..AB.2.[bY..'...
0x01A0: 4B 9F 2B 57 9B 6D 57 7C 9A DF 11 AD 5F D6 88 82  K.+W.mW|...._...
0x01B0: 5B 4C CF 02 6B 47 63 07 5B 61 6A 82 A1 8B DF 56  [L..kGc.[aj....V
0x01C0: F4 07 81 DF 90 FB FD 14 51 26 1C 2E 30 68 69 0B  ........Q&..0hi.
0x01D0: 1F 12 A2 27 FE 87 04 8F 9E 81 B9 E4 44 B6 85 C2  ...'........D...
0x01E0: 48 54 A3 90 2B F1 E0 45 20 60 98 38 02 F0 D9 84  HT..+..E `.8....
0x01F0: F1 C2 5C D6 56 31 BA 8D 6C 89 92 1D EB 7E 01 9C  ..\.V1..l....~..
0x0200: 7E C3 19 30 12 FC 80 F7 44 2A BE E3 53 09 14 28  ~..0....D*..S..(
0x0210: E0 14 0F 31 9D D8 BA 8A 91 4E 8F 30              ...1.....N.0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.320378 10.0.4.155:2010 -> 10.0.9.75:1485
TCP TTL:63 TOS:0x0 ID:26666 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x62819E10  Ack: 0x1D92D3F3  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 2A 40 00 3F 06 A5  .....E..Lh*@.?..
0x0020: 70 10 16 04 9B 10 16 09 4B 07 DA 05 CD 62 81 9E  p.......K....b..
0x0030: 10 1D 92 D3 F3 50 18 44 70 A1 90 00 00 48 54 54  .....P.Dp....HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 31 0D 0A 0D  me: 986400261...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.323422 10.0.4.155:2010 -> 10.0.9.75:1485
TCP TTL:63 TOS:0x0 ID:26667 IpLen:20 DgmLen:1288 DF
***AP**F Seq: 0x62819E34  Ack: 0x1D92D3F3  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 05 08 68 2B 40 00 3F 06 A0  .....E...h+@.?..
0x0020: B3 10 16 04 9B 10 16 09 4B 07 DA 05 CD 62 81 9E  ........K....b..
0x0030: 34 1D 92 D3 F3 50 19 44 70 E9 BF 00 00 53 D0 05  4....P.Dp....S..
0x0040: 2E 6F 6D 25 7F 25 84 AF EB 12 25 BB 00 FE 55 85  .om%.%....%...U.
0x0050: 76 49 49 C5 A9 93 B6 F4 6E 97 B3 D7 BA B0 F5 A1  vII.....n.......
0x0060: 2F DC C2 50 BE 10 0F 2E BD 61 7B 54 81 2B 18 A4  /..P.....a{T.+..
0x0070: A7 04 B8 E8 61 93 4C 4F D1 09 1B B7 B1 F9 4A 04  ....a.LO......J.
0x0080: 48 02 C4 B7 33 48 13 CF 78 55 E6 97 CE 99 1C B4  H...3H..xU......
0x0090: 04 FB E8 E2 26 C2 BA 89 4F D4 F7 71 66 B6 86 43  ....&...O..qf..C
0x00A0: 75 63 B2 CC CA 7B E1 C3 35 16 A1 D8 D8 25 5E 3A  uc...{..5....%^:
0x00B0: D1 F6 46 F0 E3 54 6B 43 EA 60 0B 76 C5 0D E6 F8  ..F..TkC.`.v....
0x00C0: AB E8 EF 2D 29 CE 45 7D 94 DD 97 99 B3 5D A4 05  ...-).E}.....]..
0x00D0: D0 FA 2F 62 47 BA 56 14 35 C2 19 94 0B 2A 15 F7  ../bG.V.5....*..
0x00E0: 3D C1 3F 60 90 89 8E 59 BD AE B3 6E AA 2A C5 F1  =.?`...Y...n.*..
0x00F0: A4 66 D9 73 B6 99 1A A7 AA 91 AB 6E B4 2F 2A AF  .f.s.......n./*.
0x0100: 62 A1 32 ED A2 72 FE 77 56 06 32 66 53 31 6E A8  b.2..r.wV.2fS1n.
0x0110: 33 42 01 7E 2C 88 F8 2D 1F D4 DA FA 70 8F B4 B2  3B.~,..-....p...
0x0120: 10 63 60 F9 94 90 9C EF 85 A2 FC CF 08 60 C0 97  .c`..........`..
0x0130: 37 80 38 EC 85 D1 25 A5 19 1B A9 13 81 EC 20 E5  7.8...%....... .
0x0140: D6 1C 48 67 95 2B 99 1A DF 76 E3 F2 7C 4B 12 76  ..Hg.+...v..|K.v
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0150: EB 52 D2 BA 5C A3 35 FC F9 8F A4 CD 46 5E 23 1F  .R..\.5.....F^#.
0x0160: 17 47 C7 30 42 C8 FB E8 DD 55 BB A2 FB E2 38 70  .G.0B....U....8p
0x0170: CB E8 B7 16 C4 F1 88 9B 2B 81 17 FD B2 7D A7 EB  ........+....}..
0x0180: 70 C4 61 ED 2F 1B 2B 78 FD FD 6B 80 19 58 45 28  p.a./.+x..k..XE(
0x0190: 4C 27 3A 17 BA 30 6D 90 62 FD C1 50 11 A0 1F 08  L':..0m.b..P....
0x01A0: 7D 33 AC A3 41 84 1A 5E 5E 1E BE 57 A5 57 4C 12  }3..A..^^..W.WL.
0x01B0: 00 B6 8D 9D 94 FD 47 A8 B0 07 A6 90 40 0B 4D A3  ......G.....@.M.
0x01C0: 31 C5 2A E7 55 77 BC 91 BC FD 96 B8 4B EF 49 CF  1.*.Uw......K.I.
0x01D0: 46 90 A2 D5 57 4C F9 8E 21 25 96 5D D0 A9 B4 A8  F...WL..!%.]....
0x01E0: AB 7D 2E BE 8A FE 15 31 61 9F 98 42 C4 B7 52 AB  .}.....1a..B..R.
0x01F0: 19 DD BB 05 27 CD 0A E5 B0 2A 70 00 42 97 ED 32  ....'....*p.B..2
0x0200: A2 23 4C A2 8E 42 13 73 88 46 07 32 FD CA 7D 50  .#L..B.s.F.2..}P
0x0210: 69 88 36 12 4E 60 D5 31 4D 34 B4 E0 71 93 09 78  i.6.N`.1M4..q..x
0x0220: 51 B2 09 5F F9 9C F7 83 A6 3C A3 07 EC 3D DC E5  Q.._.....<...=..
0x0230: 09 DC 15 DC 50 0C 46 E7 DE 56 3E 5F F4 96 12 B9  ....P.F..V>_....
0x0240: E1 2E AB B8 81 1E C4 68 5F 33 E0 C2 42 44 DD 0D  .......h_3..BD..
0x0250: DD 88 2A 0D BC 85 BF 5C B2 75 BD FC 54 71 74 43  ..*....\.u..TqtC
0x0260: 3E BB 08 98 4E 81 BD C6 CC 16 52 18 8F 4B 6E 71  >...N.....R..Knq
0x0270: 04 24 4C BE 46 A8 66 47 80 C7 EE 22 A2 A3 20 5F  .$L.F.fG..".. _
0x0280: 5D 4C A9 EA 40 A8 FB 29 01 C4 E3 C2 87 67 BA 41  ]L..@..).....g.A
0x0290: D2 50 AD E1 13 28 BC D5 51 27 51 9D DD 97 A5 DD  .P...(..Q'Q.....
0x02A0: 78 53 55 8A ED 97 0B FC 6E EC FC 37 98 51 88 EF  xSU.....n..7.Q..
0x02B0: 2F 6C A2 17 B1 03 34 D8 AA 42 0F 53 3C 47 CF DE  /l....4..B.S<G..
0x02C0: CD 74 EE 28 86 C8 8E 12 7C ED E3 2A 23 FD 91 36  .t.(....|..*#..6
0x02D0: 4B 4C A6 C8 83 E8 BE 3A 36 F2 6E 81 6E 48 1D DD  KL.....:6.n.nH..
0x02E0: DE 17 E9 40 9A 37 43 9E 8A 27 FE 51 83 94 BF 29  ...@.7C..'.Q...)
0x02F0: 4A 3E EC CD 63 BA 9B CE 51 5F 9D B7 C0 9F 2D E5  J>..c...Q_....-.
0x0300: 18 F7 41 B8 A9 54 79 EA C2 B6 E2 39 64 F0 86 29  ..A..Ty....9d..)
0x0310: C2 C9 12 D4 7A F6 FA 98 C8 15 57 77 81 76 FF 69  ....z.....Ww.v.i
0x0320: 41 85 9E DF D5 0C E6 9B 3B 74 1E F5 D3 BC 2D D2  A.......;t....-.
0x0330: 8D B9 24 6A 7C F4 3B 35 D0 10 90 78 A4 8D E0 4F  ..$j|.;5...x...O
0x0340: B1 79 14 88 9A 90 58 F7 A5 ED EF 92 95 0B 69 7F  .y....X.......i.
0x0350: 97 28 F3 65 39 DB 8A 0A D1 9B E6 5C D9 3E 90 03  .(.e9......\.>..
0x0360: 66 93 03 DC E9 05 8C 42 73 4C BB 2C 92 4E E5 79  f.......BsL.,.N.y
0x0370: E8 67 6A 94 05 61 ED 02 36 EE E3 A0 03 CA 2B 72  .gj..a..6.....+r
0x0380: 56 D6 80 95 B3 30 62 BF 01 06 10 56 6A A8 57 FF  V....0b....Vj.W.
0x0390: 03 E0 66 71 3C 5B AC 0B F0 68 41 91 2D 01 E7 61  ..fq<[...hA.-..a
0x03A0: 59 9D 3D 96 76 40 18 7B 01 E6 07 55 B5 31 CC 43  Y.=.v@.{...U.1.C
0x03B0: 10 ED 18 D9 D8 77 17 8D D4 6D B6 A9 D3 C3 98 02  .....w...m......
0x03C0: 36 DC DA 39 1A C7 3F 5D 6F DA 85 49 8E 57 D1 78  6..9..?]o..I.W.x
0x03D0: 36 87 08 6C 4A 9F 16 FF 06 04 95 6A DB 2A D0 6E  6..lJ.......j.*.n
0x03E0: 3C 1E DE 71 16 7D 87 4D 5D F8 E0 52 63 23 6E 41  <..q.}.M]..Rc#nA
0x03F0: 3E 43 15 D1 D3 CE 3D 1B 97 8D A4 22 C8 3E C4 EE  >C....=....".>..
0x0400: 35 C7 0D 7B 74 76 A5 65 8B E8 14 13 9E BC AB 78  5..{tv.e.......x
0x0410: 1A 22 3F 88 92 E6 D0 2E 69 66 EE EB 97 C4 CF 48  ."?.....if.....H
0x0420: 2E 68 F4 A0 10 92 BD 4F F8 2E 68 51 35 0C FD 43  .h.....O..hQ5..C
0x0430: E7 87 9E A2 B5 BB 56 C4 70 73 C2 23 91 4C 54 A2  ......V.ps.#.LT.
0x0440: E1 CD 17 72 ED 35 4E 34 3C 77 A7 CD 7F 3E 24 73  ...r.5N4<w...>$s
0x0450: FC 56 EE FD F8 B6 F4 98 4F 3F 29 46 2E 15 14 B9  .V......O?)F....
0x0460: 96 D1 5A AC CC A9 90 0F A3 50 EC 72 81 41 A7 E8  ..Z......P.r.A..
0x0470: 01 85 27 1E 33 22 A2 07 5E 3E B4 D9 4F 32 37 9E  ..'.3"..^>..O27.
0x0480: BA E1 28 DA 9F 4D 64 FB DC 1F 19 2B 47 4C CD 81  ..(..Md....+GL..
0x0490: 9F 9D D4 13 3B C6 AE CD C0 B1 83 ED 9E 38 7A 70  ....;........8zp
0x04A0: 6D AC E5 29 1E 8D 8E 79 F1 AA 77 00 C4 B2 41 C7  m..)...y..w...A.
0x04B0: B5 EE FB 6F D7 F3 37 5D 28 6F 75 AA 75 EF C1 5F  ...o..7](ou.u.._
0x04C0: 24 44 96 02 89 1A 2E A8 63 40 E2 E2 DE DC A9 60  $D......c@.....`
0x04D0: 9D 38 F6 EE D6 11 BB 9E CB 26 85 1E 84 9B 66 9E  .8.......&....f.
0x04E0: 3A 93 1E A1 0E 4A D6 A2 F4 8A 8C 00 D4 90 6C 91  :....J........l.
0x04F0: 51 CB 4A BA 91 30 AB 38 A8 3E 7E FE F0 1F B5 8F  Q.J..0.8.>~.....
0x0500: ED 93 4F F1 EE 79 58 13 02 1D D2 24 73 C6 EE 12  ..O..yX....$s...
0x0510: 4B CE 2F 4E 84 E2 C0 C3 67 DD 69 4C E9           K./N....g.iL.
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.324920 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2856 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D92D3F3  Ack: 0x6281A315  Win: 0x11CC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 28 40 00 80 06 C1  .....E..(.(@....
0x0020: 96 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D3  ....K...........
0x0030: F3 62 81 A3 15 50 10 11 CC 6B 33 00 00 50 4F 53  .b...P...k3..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.325919 10.0.9.75:1485 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2857 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D92D3F3  Ack: 0x6281A315  Win: 0x11CC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 29 40 00 80 06 C1  .....E..(.)@....
0x0020: 95 10 16 09 4B 10 16 04 9B 05 CD 07 DA 1D 92 D3  ....K...........
0x0030: F3 62 81 A3 15 50 11 11 CC 6B 32 00 00 50 4F 53  .b...P...k2..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.326231 10.0.4.155:2010 -> 10.0.9.75:1485
TCP TTL:63 TOS:0x0 ID:26668 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6281A315  Ack: 0x1D92D3F4  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 2C 40 00 3F 06 A5  .....E..(h,@.?..
0x0020: 92 10 16 04 9B 10 16 09 4B 07 DA 05 CD 62 81 A3  ........K....b..
0x0030: 15 1D 92 D3 F4 50 10 44 6F 38 8F 00 00           .....P.Do8...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.428374 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2858 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D9463BB  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 2A 40 00 80 06 C1  .....E..0.*@....
0x0020: 8C 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 63  ....K..........c
0x0030: BB 00 00 00 00 70 02 16 D0 AF 46 00 00 02 04 05  .....p....F.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.428699 10.0.4.155:2010 -> 10.0.9.75:1486
TCP TTL:63 TOS:0x0 ID:26669 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62839EE0  Ack: 0x1D9463BC  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 2D 40 00 3F 06 A5  .....E..,h-@.?..
0x0020: 8D 10 16 04 9B 10 16 09 4B 07 DA 05 CE 62 83 9E  ........K....b..
0x0030: E0 1D 94 63 BC 60 12 44 70 95 38 00 00 02 04 05  ...c.`.Dp.8.....
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.429114 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2859 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D9463BC  Ack: 0x62839EE1  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0010: 00 00 00 08 00 45 00 00 28 0B 2B 40 00 80 06 C1  .....E..(.+@....
0x0020: 93 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 63  ....K..........c
0x0030: BC 62 83 9E E1 50 10 16 D0 DA 95 00 00 02 04 05  .b...P..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.429389 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2860 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D9463BC  Ack: 0x62839EE1  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 2C 40 00 80 06 C1  .....E..9.,@....
0x0020: 81 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 63  ....K..........c
0x0030: BC 62 83 9E E1 50 18 16 D0 E6 A2 00 00 50 4F 53  .b...P.......POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.451984 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2861 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D955D96  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 2D 40 00 80 06 C1  .....E..0.-@....
0x0020: 89 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5D  ....K..........]
0x0030: 96 00 00 00 00 70 02 16 D0 B5 69 00 00 02 04 05  .....p....i.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.452288 10.0.4.155:2010 -> 10.0.9.75:1487
TCP TTL:63 TOS:0x0 ID:26670 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x6284608D  Ack: 0x1D955D97  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 2E 40 00 3F 06 A5  .....E..,h.@.?..
0x0020: 8C 10 16 04 9B 10 16 09 4B 07 DA 05 CF 62 84 60  ........K....b.`
0x0030: 8D 1D 95 5D 97 60 12 44 70 D9 AD 00 00 02 04 05  ...].`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.452702 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2862 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D955D97  Ack: 0x6284608E  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 2E 40 00 80 06 C1  .....E..(..@....
0x0020: 90 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5D  ....K..........]
0x0030: 97 62 84 60 8E 50 10 16 D0 1F 0B 00 00 02 04 05  .b.`.P..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.453115 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2863 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D955D97  Ack: 0x6284608E  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 2F 40 00 80 06 C1  .....E..9./@....
0x0020: 7E 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5D  ~...K..........]
0x0030: 97 62 84 60 8E 50 18 16 D0 2B 18 00 00 50 4F 53  .b.`.P...+...POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.528679 10.0.4.155:2010 -> 10.0.9.75:1486
TCP TTL:63 TOS:0x0 ID:26671 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62839EE1  Ack: 0x1D9463CD  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 2F 40 00 3F 06 A5  .....E..(h/@.?..
0x0020: 8F 10 16 04 9B 10 16 09 4B 07 DA 05 CE 62 83 9E  ........K....b..
0x0030: E1 1D 94 63 CD 50 10 44 70 AC E4 00 00           ...c.P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.529550 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2864 IpLen:20 DgmLen:475 DF
***AP*** Seq: 0x1D9463CD  Ack: 0x62839EE1  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 01 DB 0B 30 40 00 80 06 BF  .....E....0@....
0x0020: DB 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 63  ....K..........c
0x0030: CD 62 83 9E E1 50 18 16 D0 2A 19 00 00 55 73 65  .b...P...*...Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket: 
0x00C0: 25 39 39 3E 25 30 43 25 38 37 3C 25 44 42 25 41  %99>%0C%87<%DB%A
0x00D0: 36 25 42 33 25 44 33 25 45 36 25 42 38 4D 39 38  6%B3%D3%E6%B8M98
0x00E0: 25 38 46 33 25 46 42 25 43 32 25 39 45 6A 45 29  %8F3%FB%C2%9EjE)
0x00F0: 25 45 39 31 25 30 31 25 30 44 52 25 42 38 76 25  %E91%01%0DR%B8v%
0x0100: 42 44 25 42 38 25 41 32 25 39 45 25 38 45 77 25  BD%B8%A2%9E%8Ew%
0x0110: 38 37 55 25 41 33 25 30 33 25 39 41 0D 0A 43 6F  87U%A3%03%9A..Co
0x0120: 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 31 38  ntent-length: 18
0x0130: 37 0D 0A 0D 0A 67 FA 81 CB D7 CD A5 3A 8F BB 3D  7....g......:..=
0x0140: 4C 7F 4B 47 49 90 6F EB 86 C3 75 23 47 BF EB D1  L.KGI.o...u#G...
0x0150: 89 76 04 B5 D4 E9 5F 2B 79 F1 FC 4C D8 47 64 B2  .v...._+y..L.Gd.
0x0160: 46 A7 91 86 80 9E ED B6 F8 D9 EE F0 5C 5A 2B FF  F...........\Z+.
0x0170: B0 AD 91 3C 73 8C F4 68 6A CC E4 BE A6 9D 55 7B  ...<s..hj.....U{
0x0180: DF 6A 31 DB FC B0 84 17 12 99 6B 8F 5E 7B C5 5B  .j1.......k.^{.[
0x0190: 5F EC 46 D7 B1 69 5E 7D 43 53 C7 DC 2D CA FF 1D  _.F..i^}CS..-...
0x01A0: 07 71 37 43 8E 1A 8E 98 30 BF 21 F8 D9 7D 69 0B  .q7C....0.!..}i.
0x01B0: DC A9 90 5D 2B 5A 8A 27 EF EF 57 07 86 A8 CF F3  ...]+Z.'..W.....
0x01C0: 99 FB 15 BE 74 33 A9 3A C1 4A 8D C9 90 F8 E2 DB  ....t3.:.J......
0x01D0: 0B 2B 1E 06 0D 3A E2 BF 3B B8 C4 74 FD 2B 4C 4D  .+...:..;..t.+LM
0x01E0: CC 66 6A 48 76 51 89 04 B4 D1 12 14 1A 0F CA 8B  .fjHvQ..........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.530351 10.0.4.155:2010 -> 10.0.9.75:1486
TCP TTL:63 TOS:0x0 ID:26672 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x62839EE1  Ack: 0x1D946580  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 30 40 00 3F 06 A5  .....E..Lh0@.?..
0x0020: 6A 10 16 04 9B 10 16 09 4B 07 DA 05 CE 62 83 9E  j.......K....b..
0x0030: E1 1D 94 65 80 50 18 44 70 0F 2D 00 00 48 54 54  ...e.P.Dp.-..HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
04/04-10:43:29.548666 10.0.4.155:2010 -> 10.0.9.75:1487
TCP TTL:63 TOS:0x0 ID:26673 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6284608E  Ack: 0x1D955DA8  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 31 40 00 3F 06 A5  .....E..(h1@.?..
0x0020: 8D 10 16 04 9B 10 16 09 4B 07 DA 05 CF 62 84 60  ........K....b.`
0x0030: 8E 1D 95 5D A8 50 10 44 70 F1 59 00 00           ...].P.Dp.Y..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.549485 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2865 IpLen:20 DgmLen:484 DF
***AP*** Seq: 0x1D955DA8  Ack: 0x6284608E  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 01 E4 0B 31 40 00 80 06 BF  .....E....1@....
0x0020: D1 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5D  ....K..........]
0x0030: A8 62 84 60 8E 50 18 16 D0 C8 15 00 00 55 73 65  .b.`.P.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket:
0x00C0: 25 42 30 74 25 45 35 25 30 44 21 25 31 38 25 39  %B0t%E5%0D!%18%9
0x00D0: 44 79 25 41 33 25 44 42 25 43 38 70 25 45 32 25  Dy%A3%DB%C8p%E2%
0x00E0: 38 41 2D 25 30 41 25 31 35 77 25 30 39 5B 25 38  8A-%0A%15w%09[%8
0x00F0: 30 25 43 34 25 46 38 25 33 42 25 41 36 43 25 31  0%C4%F8%3B%A6C%1
0x0100: 42 25 42 42 6D 25 41 46 25 43 34 25 38 39 25 45  B%BBm%AF%C4%89%E
0x0110: 33 25 31 32 25 32 36 25 43 43 31 64 25 38 32 25  3%12%26%CC1d%82%
0x0120: 31 34 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65 6E 67  14..Content-leng
0x0130: 74 68 3A 20 31 39 30 0D 0A 0D 0A 1E 58 4C 4A C2  th: 190.....XLJ.
0x0140: EF 43 AA 66 3A FE 69 36 22 26 0F 4C 72 6C 09 9C  .C.f:.i6"&.Lrl..
0x0150: 0E BC 09 72 9B 38 E8 B3 C4 62 A5 62 17 E3 DC 70  ...r.8...b.b...p
0x0160: 8C 65 F3 C5 53 75 3D E4 83 56 9D EB 38 7E 45 7F  .e..Su=..V..8~E.
0x0170: 2D C2 F3 5B C3 4C 83 72 DB 24 A1 4C F7 8B 94 F2  -..[.L.r.$.L....
0x0180: 2A D6 42 F4 86 AB 5D F0 BA 6B 0B 8C 4E A6 2E 6F  *.B...]..k..N..o
0x0190: 39 80 76 5E B3 63 FF 4C FA E4 F4 55 E7 3C 30 20  9.v^.c.L...U.<0
0x01A0: 7B C5 5C 03 61 05 BA BD 82 08 43 61 78 47 20 87  {.\.a.....CaxG .
0x01B0: C9 4D D9 4C 40 1A 5B 3D F9 CE 71 48 03 9A C2 64  .M.L@.[=..qH...d
0x01C0: 1B EF 94 29 85 41 F6 42 EC 19 50 30 75 BF 21 93  ...).A.B..P0u.!.
0x01D0: C0 2F 7B CB 93 50 E4 1C EC 3F C3 5E 73 CB AD B4  ./{..P...?.^s...
0x01E0: FB 09 26 42 75 44 4C 6C B6 86 F4 23 BC 79 BE 59  ..&BuDLl...#.y.Y
0x01F0: C0 BE 78 B8 4F 70 6F 53 31                       ..x.OpoS1

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.550240 10.0.4.155:2010 -> 10.0.9.75:1487
TCP TTL:63 TOS:0x0 ID:26674 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x6284608E  Ack: 0x1D955F64  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 32 40 00 3F 06 A5  .....E..Lh2@.?..
0x0020: 68 10 16 04 9B 10 16 09 4B 07 DA 05 CF 62 84 60  h.......K....b.`
0x0030: 8E 1D 95 5F 64 50 18 44 70 53 99 00 00 48 54 54  ..._dP.DpS...HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.552598 10.0.4.155:2010 -> 10.0.9.75:1487
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:63 TOS:0x0 ID:26675 IpLen:20 DgmLen:156 DF
***AP**F Seq: 0x628460B2  Ack: 0x1D955F64  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 9C 68 33 40 00 3F 06 A5  .....E...h3@.?..
0x0020: 17 10 16 04 9B 10 16 09 4B 07 DA 05 CF 62 84 60  ........K....b.`
0x0030: B2 1D 95 5F 64 50 19 44 70 81 E7 00 00 06 43 4B  ..._dP.Dp.....CK
0x0040: 4E CD F1 0E FD 04 F6 90 2A 4D 6D FB 86 D4 C0 64  N.......*Mm....d
0x0050: 54 64 27 E7 D4 F6 53 D3 81 C1 0A 04 57 AB 24 A2  Td'...S.....W.$.
0x0060: 5E 7E C3 3C BF A1 D4 A5 EC 2C 4B B5 85 57 B6 D7  ^~.<.....,K..W..
0x0070: 98 8E 97 83 5F D0 9B 67 DF 4B 23 65 94 FF D9 36  ...._..g.K#e...6
0x0080: D8 E9 11 17 A7 20 29 33 B2 A4 C2 5A 74 EC 97 D7  ..... )3...Zt...
0x0090: FC 9A BB A5 B1 1B A2 27 07 A4 DB EE 35 DE 1D F6  .......'....5...
0x00A0: 2D 09 DB F3 2F B9 D2 09 CA F4 56 D9 EE E6 B6 3F  -.../.....V....?
0x00B0: FB                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.553094 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2866 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D955F64  Ack: 0x62846127  Win: 0x1638  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 32 40 00 80 06 C1  .....E..(.2@....
0x0020: 8C 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5F  ....K.........._
0x0030: 64 62 84 61 27 50 10 16 38 1D 3D 00 00 50 4F 53  db.a'P..8.=..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.553550 10.0.9.75:1487 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2867 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D955F64  Ack: 0x62846127  Win: 0x1638  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 33 40 00 80 06 C1  .....E..(.3@....
0x0020: 8B 10 16 09 4B 10 16 04 9B 05 CF 07 DA 1D 95 5F  ....K.........._
0x0030: 64 62 84 61 27 50 11 16 38 1D 3C 00 00 50 4F 53  db.a'P..8.<..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.553826 10.0.4.155:2010 -> 10.0.9.75:1487
TCP TTL:63 TOS:0x0 ID:26676 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62846127  Ack: 0x1D955F65  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 34 40 00 3F 06 A5  .....E..(h4@.?..
0x0020: 8A 10 16 04 9B 10 16 09 4B 07 DA 05 CF 62 84 61  ........K....b.a
0x0030: 27 1D 95 5F 65 50 10 44 6F EF 04 00 00           '.._eP.Do....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.555620 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2868 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D9659C9  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 34 40 00 80 06 C1  .....E..0.4@....
0x0020: 82 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 59  ....K..........Y
0x0030: C9 00 00 00 00 70 02 16 D0 B9 34 00 00 02 04 05  .....p....4.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.555945 10.0.4.155:2010 -> 10.0.9.75:1488
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:63 TOS:0x0 ID:26677 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62853FD6  Ack: 0x1D9659CA  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 35 40 00 3F 06 A5  .....E..,h5@.?..
0x0020: 85 10 16 04 9B 10 16 09 4B 07 DA 05 D0 62 85 3F  ........K....b.?
0x0030: D6 1D 96 59 CA 60 12 44 70 FE 2E 00 00 02 04 05  ...Y.`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.556343 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2869 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D9659CA  Ack: 0x62853FD7  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 35 40 00 80 06 C1  .....E..(.5@....
0x0020: 89 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 59  ....K..........Y
0x0030: CA 62 85 3F D7 50 10 16 D0 43 8C 00 00 02 04 05  .b.?.P...C......
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.556489 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2870 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1D9659CA  Ack: 0x62853FD7  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 3D 0B 36 40 00 80 06 C1  .....E..=.6@....
0x0020: 73 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 59  s...K..........Y
0x0030: CA 62 85 3F D7 50 18 16 D0 6D C6 00 00 50 4F 53  .b.?.P...m...POS
0x0040: 54 20 2F 74 69 6D 65 20 48 54 54 50 2F 31 2E 30  T /time HTTP/1.0
0x0050: 0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.648641 10.0.4.155:2010 -> 10.0.9.75:1488
TCP TTL:63 TOS:0x0 ID:26678 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62853FD7  Ack: 0x1D9659DF  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 36 40 00 3F 06 A5  .....E..(h6@.?..
0x0020: 88 10 16 04 9B 10 16 09 4B 07 DA 05 D0 62 85 3F  ........K....b.?
0x0030: D7 1D 96 59 DF 50 10 44 70 15 D7 00 00           ...Y.P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.649286 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2871 IpLen:20 DgmLen:166 DF
***AP*** Seq: 0x1D9659DF  Ack: 0x62853FD7  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 A6 0B 37 40 00 80 06 C1  .....E....7@....
0x0020: 09 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 59  ....K..........Y
0x0030: DF 62 85 3F D7 50 18 16 D0 AF D7 00 00 55 73 65  .b.?.P.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 41 63 63 65 70 74 3A 20  ndows)..Accept:
0x0070: 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70  */*..Content-typ
0x0080: 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  e: application/x
0x0090: 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63  -www-form-urlenc
0x00A0: 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65  oded..Content-le
0x00B0: 6E 67 74 68 3A 20 30 0D 0A 0D 0A                 ngth: 0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
04/04-10:43:29.649757 10.0.4.155:2010 -> 10.0.9.75:1488
TCP TTL:63 TOS:0x0 ID:26679 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x62853FD7  Ack: 0x1D965A5D  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 37 40 00 3F 06 A5  .....E..Lh7@.?..
0x0020: 63 10 16 04 9B 10 16 09 4B 07 DA 05 D0 62 85 3F  c.......K....b.?
0x0030: D7 1D 96 5A 5D 50 18 44 70 79 54 00 00 48 54 54  ...Z]P.DpyT..HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.649759 10.0.4.155:2010 -> 10.0.9.75:1488
TCP TTL:63 TOS:0x0 ID:26680 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x62853FFB  Ack: 0x1D965A5D  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 38 40 00 3F 06 A5  .....E..(h8@.?..
0x0020: 86 10 16 04 9B 10 16 09 4B 07 DA 05 D0 62 85 3F  ........K....b.?
0x0030: FB 1D 96 5A 5D 50 11 44 70 15 34 00 00           ...Z]P.Dp.4..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.650308 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2872 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D965A5D  Ack: 0x62853FFC  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 38 40 00 80 06 C1  .....E..(.8@....
0x0020: 86 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 5A  ....K..........Z
0x0030: 5D 62 85 3F FC 50 10 16 AC 42 F8 00 00 55 73 65  ]b.?.P...B...Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.650585 10.0.9.75:1488 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2873 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D965A5D  Ack: 0x62853FFC  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 39 40 00 80 06 C1  .....E..(.9@....
0x0020: 85 10 16 09 4B 10 16 04 9B 05 D0 07 DA 1D 96 5A  ....K..........Z
0x0030: 5D 62 85 3F FC 50 11 16 AC 42 F7 00 00 55 73 65  ]b.?.P...B...Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.650861 10.0.4.155:2010 -> 10.0.9.75:1488
TCP TTL:63 TOS:0x0 ID:26681 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62853FFC  Ack: 0x1D965A5E  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 39 40 00 3F 06 A5  .....E..(h9@.?..
0x0020: 85 10 16 04 9B 10 16 09 4B 07 DA 05 D0 62 85 3F  ........K....b.?
0x0030: FC 1D 96 5A 5E 50 10 44 70 15 33 00 00           ...Z^P.Dp.3..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.651499 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2874 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D979773  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 3A 40 00 80 06 C1  .....E..0.:@....
0x0020: 7C 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 97  |...K...........
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0030: 73 00 00 00 00 70 02 16 D0 7B 88 00 00 02 04 05  s....p...{......
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.651778 10.0.4.155:2010 -> 10.0.9.75:1489
TCP TTL:63 TOS:0x0 ID:26682 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x6285ED77  Ack: 0x1D979774  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 3A 40 00 3F 06 A5  .....E..,h:@.?..
0x0020: 80 10 16 04 9B 10 16 09 4B 07 DA 05 D1 62 85 ED  ........K....b..
0x0030: 77 1D 97 97 74 60 12 44 70 12 E1 00 00 02 04 05  w...t`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.652145 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2875 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D979774  Ack: 0x6285ED78  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 3B 40 00 80 06 C1  .....E..(.;@....
0x0020: 83 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 97  ....K...........
0x0030: 74 62 85 ED 78 50 10 16 D0 58 3E 00 00 02 04 05  tb..xP...X>.....
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.652425 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2876 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D979774  Ack: 0x6285ED78  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 3C 40 00 80 06 C1  .....E..9.<@....
0x0020: 71 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 97  q...K...........
0x0030: 74 62 85 ED 78 50 18 16 D0 64 4B 00 00 50 4F 53  tb..xP...dK..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.717481 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2877 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D946580  Ack: 0x62839F05  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 3D 40 00 80 06 C1  .....E..(.=@....
0x0020: 81 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 65  ....K..........e
0x0030: 80 62 83 9F 05 50 10 16 AC D8 D1 00 00 50 4F 53  .b...P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.717899 10.0.4.155:2010 -> 10.0.9.75:1486
TCP TTL:63 TOS:0x0 ID:26683 IpLen:20 DgmLen:318 DF
***AP*** Seq: 0x62839F05  Ack: 0x1D946580  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 01 3E 68 3B 40 00 3F 06 A4  .....E..>h;@.?..
0x0020: 6D 10 16 04 9B 10 16 09 4B 07 DA 05 CE 62 83 9F  m.......K....b..
0x0030: 05 1D 94 65 80 50 18 44 70 21 15 00 00 7F E1 86  ...e.P.Dp!......
0x0040: CF D8 D3 E8 6D D0 F3 21 12 B6 5F E7 E4 6B 38 96  ....m..!.._..k8.
0x0050: 70 E5 1B D4 8A 15 7C 6D B0 FB E4 58 D7 5F 35 2E  p.....|m...X._5.
0x0060: 6C 36 0A 9F 92 79 DD 74 C1 0E 71 24 CB B7 18 AF  l6...y.t..q$....
0x0070: 22 C8 43 47 61 3E EC F0 87 BF 61 3F 25 E3 D9 2C  ".CGa>....a?%..,
0x0080: AF BC D4 CC D4 69 F4 6F 69 FB 46 4C D3 B3 5F 52  .....i.oi.FL.._R
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0090: 12 F7 02 6E B5 C0 03 56 F0 CC 57 B9 83 CD C2 23  ...n...V..W....#
0x00A0: EA A9 E1 9D F4 3E F1 28 40 CB 19 93 DB C1 73 7D  .....>.(@.....s}
0x00B0: D3 D2 AA E6 43 5C 15 98 10 D9 0C 5C 5E 13 A9 0B  ....C\.....\^...
0x00C0: C6 B7 5E 99 2A 40 EF AC 04 D1 52 22 CB B3 20 56  ..^.*@....R".. V
0x00D0: 17 32 64 39 39 A8 53 7F 8D A4 98 48 48 E0 8C 15  .2d99.S....HH...
0x00E0: 25 65 2E 41 3E FD BC 2F D9 FB 96 86 85 0A 4C FA  %e.A>../......L.
0x00F0: 49 F3 04 0C 26 E8 65 5A 98 50 4D 82 D9 D7 2E 6C  I...&.eZ.PM....l
0x0100: 4B 5B 4E D0 FC 9A 88 61 0F 97 DE 23 25 AA 82 AA  K[N....a...#%...
0x0110: 7F D6 D4 9D F4 7C 67 09 38 44 07 8A 0C B9 4E A7  .....|g.8D....N.
0x0120: 02 24 96 85 ED 19 2E 6E 5F 6B 71 33 53 F5 04 8E  .$.....n_kq3S...
0x0130: 63 A9 28 61 CC 8A 60 B5 6E 8E 03 4E E4 E5 79 21  c.(a..`.n..N..y!
0x0140: 39 2D 4A 71 6F 25 01 E6 67 CF 66 A0 50 A9 60 7F  9-Jqo%..g.f.P.`.
0x0150: 0C E5 E9                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.748619 10.0.4.155:2010 -> 10.0.9.75:1489
TCP TTL:63 TOS:0x0 ID:26684 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6285ED78  Ack: 0x1D979785  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 3C 40 00 3F 06 A5  .....E..(h<@.?..
0x0020: 82 10 16 04 9B 10 16 09 4B 07 DA 05 D1 62 85 ED  ........K....b..
0x0030: 78 1D 97 97 85 50 10 44 70 2A 8D 00 00           x....P.Dp*...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.749544 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2878 IpLen:20 DgmLen:513 DF
***AP*** Seq: 0x1D979785  Ack: 0x6285ED78  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 02 01 0B 3E 40 00 80 06 BF  .....E....>@....
0x0020: A7 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 97  ....K...........
0x0030: 85 62 85 ED 78 50 18 16 D0 1A E1 00 00 55 73 65  .b..xP.......Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket:
0x00C0: 25 45 32 25 44 36 57 25 46 44 25 31 30 25 41 35  %E2%D6W%FD%10%A5
0x00D0: 25 44 45 69 25 38 39 7A 25 44 31 25 30 37 54 25  %DEi%89z%D1%07T%
0x00E0: 30 41 69 25 42 33 54 4F 25 38 35 25 30 42 33 25  0Ai%B3TO%85%0B3%
0x00F0: 45 31 7E 25 41 41 25 46 30 25 38 43 25 44 45 34  E1~%AA%F0%8C%DE4
0x0100: 25 32 30 4F 56 25 43 33 25 46 45 53 25 46 36 68  %20OV%C3%FES%F6h
0x0110: 25 45 32 79 39 56 0D 0A 43 6F 6E 74 65 6E 74 2D  %E2y9V..Content-
0x0120: 6C 65 6E 67 74 68 3A 20 32 33 31 0D 0A 0D 0A 4B  length: 231....K
0x0130: CB 02 2A 60 73 68 28 5F 31 00 6E A5 54 20 87 26  ..*`sh(_1.n.T .&
0x0140: 53 B3 1C D7 32 00 99 14 8A D8 96 E6 37 A6 ED D4  S...2.......7...
0x0150: A9 54 F6 DF D9 04 BC C8 A9 91 B2 0C BB 92 A6 7A  .T.............z
0x0160: CF 42 C5 CE EA 0E 57 92 5D 21 11 B0 5F 61 E6 99  .B....W.]!.._a..
0x0170: B7 19 14 5F C0 98 CF BC 10 4E B9 02 06 A0 EB 0D  ..._.....N......
0x0180: 2A FA 4E 15 E1 86 8D 58 60 CB 08 C6 41 42 C4 32  *.N....X`...AB.2
0x0190: E3 5B 62 59 B8 88 27 BF A8 90 4B 9F 2B 57 9B 6D  .[bY..'...K.+W.m
0x01A0: 57 7C 9A DF 11 AD 5F D6 88 82 5B 4C CF 02 6B 47  W|...._...[L..kG
0x01B0: 63 07 5B 61 6A 82 A1 8B DF 56 F4 07 81 DF 90 FB  c.[aj....V......
0x01C0: FD 14 51 26 1C 2E 30 68 69 0B 1F 12 A2 27 FE 87  ..Q&..0hi....'..
0x01D0: 04 8F 9E 81 B9 E4 44 B6 85 C2 48 54 A3 90 2B F1  ......D...HT..+.
0x01E0: E0 45 20 60 98 38 02 F0 D9 84 F1 C2 5C D6 56 31  .E `.8......\.V1
0x01F0: BA 8D 6C 89 92 1D EB 7E 01 9C 7E C3 19 30 12 FC  ..l....~..~..0..
0x0200: 80 F7 44 2A BE E3 53 09 14 28 E0 14 0F 31 9D D8  ..D*..S..(...1..
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0210: BA 8A 91 4E 8F 30                                ...N.0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.750444 10.0.4.155:2010 -> 10.0.9.75:1489
TCP TTL:63 TOS:0x0 ID:26685 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x6285ED78  Ack: 0x1D97995E  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 3D 40 00 3F 06 A5  .....E..Lh=@.?..
0x0020: 5D 10 16 04 9B 10 16 09 4B 07 DA 05 D1 62 85 ED  ].......K....b..
0x0030: 78 1D 97 99 5E 50 18 44 70 8C AF 00 00 48 54 54  x...^P.Dp....HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.753450 10.0.4.155:2010 -> 10.0.9.75:1489
TCP TTL:63 TOS:0x0 ID:26686 IpLen:20 DgmLen:1288 DF
***AP**F Seq: 0x6285ED9C  Ack: 0x1D97995E  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 05 08 68 3E 40 00 3F 06 A0  .....E...h>@.?..
0x0020: A0 10 16 04 9B 10 16 09 4B 07 DA 05 D1 62 85 ED  ........K....b..
0x0030: 9C 1D 97 99 5E 50 19 44 70 D4 DF 00 00 53 D0 05  ....^P.Dp....S..
0x0040: 2E 6F 6D 25 7F 25 84 AF EB 12 25 BB 00 FE 55 85  .om%.%....%...U.
0x0050: 76 49 49 C5 A9 93 B6 F4 6E 97 B3 D7 BA B0 F5 A1  vII.....n.......
0x0060: 2F DC C2 50 BE 10 0F 2E BD 61 7B 54 81 2B 18 A4  /..P.....a{T.+..
0x0070: A7 04 B8 E8 61 93 4C 4F D1 09 1B B7 B1 F9 4A 04  ....a.LO......J.
0x0080: 48 02 C4 B7 33 48 13 CF 78 55 E6 97 CE 99 1C B4  H...3H..xU......
0x0090: 04 FB E8 E2 26 C2 BA 89 4F D4 F7 71 66 B6 86 43  ....&...O..qf..C
0x00A0: 75 63 B2 CC CA 7B E1 C3 35 16 A1 D8 D8 25 5E 3A  uc...{..5....%^:
0x00B0: D1 F6 46 F0 E3 54 6B 43 EA 60 0B 76 C5 0D E6 F8  ..F..TkC.`.v....
0x00C0: AB E8 EF 2D 29 CE 45 7D 94 DD 97 99 B3 5D A4 05  ...-).E}.....]..
0x00D0: D0 FA 2F 62 47 BA 56 14 35 C2 19 94 0B 2A 15 F7  ../bG.V.5....*..
0x00E0: 3D C1 3F 60 90 89 8E 59 BD AE B3 6E AA 2A C5 F1  =.?`...Y...n.*..
0x00F0: A4 66 D9 73 B6 99 1A A7 AA 91 AB 6E B4 2F 2A AF  .f.s.......n./*.
0x0100: 62 A1 32 ED A2 72 FE 77 56 06 32 66 53 31 6E A8  b.2..r.wV.2fS1n.
0x0110: 33 42 01 7E 2C 88 F8 2D 1F D4 DA FA 70 8F B4 B2  3B.~,..-....p...
0x0120: 10 63 60 F9 94 90 9C EF 85 A2 FC CF 08 60 C0 97  .c`..........`..
0x0130: 37 80 38 EC 85 D1 25 A5 19 1B A9 13 81 EC 20 E5  7.8...%....... .
0x0140: D6 1C 48 67 95 2B 99 1A DF 76 E3 F2 7C 4B 12 76  ..Hg.+...v..|K.v
0x0150: EB 52 D2 BA 5C A3 35 FC F9 8F A4 CD 46 5E 23 1F  .R..\.5.....F^#.
0x0160: 17 47 C7 30 42 C8 FB E8 DD 55 BB A2 FB E2 38 70  .G.0B....U....8p
0x0170: CB E8 B7 16 C4 F1 88 9B 2B 81 17 FD B2 7D A7 EB  ........+....}..
0x0180: 70 C4 61 ED 2F 1B 2B 78 FD FD 6B 80 19 58 45 28  p.a./.+x..k..XE(
0x0190: 4C 27 3A 17 BA 30 6D 90 62 FD C1 50 11 A0 1F 08  L':..0m.b..P....
0x01A0: 7D 33 AC A3 41 84 1A 5E 5E 1E BE 57 A5 57 4C 12  }3..A..^^..W.WL.
0x01B0: 00 B6 8D 9D 94 FD 47 A8 B0 07 A6 90 40 0B 4D A3  ......G.....@.M.
0x01C0: 31 C5 2A E7 55 77 BC 91 BC FD 96 B8 4B EF 49 CF  1.*.Uw......K.I.
0x01D0: 46 90 A2 D5 57 4C F9 8E 21 25 96 5D D0 A9 B4 A8  F...WL..!%.]....
0x01E0: AB 7D 2E BE 8A FE 15 31 61 9F 98 42 C4 B7 52 AB  .}.....1a..B..R.
0x01F0: 19 DD BB 05 27 CD 0A E5 B0 2A 70 00 42 97 ED 32  ....'....*p.B..2
0x0200: A2 23 4C A2 8E 42 13 73 88 46 07 32 FD CA 7D 50  .#L..B.s.F.2..}P
0x0210: 69 88 36 12 4E 60 D5 31 4D 34 B4 E0 71 93 09 78  i.6.N`.1M4..q..x
0x0220: 51 B2 09 5F F9 9C F7 83 A6 3C A3 07 EC 3D DC E5  Q.._.....<...=..
0x0230: 09 DC 15 DC 50 0C 46 E7 DE 56 3E 5F F4 96 12 B9  ....P.F..V>_....
0x0240: E1 2E AB B8 81 1E C4 68 5F 33 E0 C2 42 44 DD 0D  .......h_3..BD..
0x0250: DD 88 2A 0D BC 85 BF 5C B2 75 BD FC 54 71 74 43  ..*....\.u..TqtC
0x0260: 3E BB 08 98 4E 81 BD C6 CC 16 52 18 8F 4B 6E 71  >...N.....R..Knq
0x0270: 04 24 4C BE 46 A8 66 47 80 C7 EE 22 A2 A3 20 5F  .$L.F.fG...".. _
0x0280: 5D 4C A9 EA 40 A8 FB 29 01 C4 E3 C2 87 67 BA 41  ]L..@..).....g.A
0x0290: D2 50 AD E1 13 28 BC D5 51 27 51 9D DD 97 A5 DD  .P...(..Q'Q.....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x02A0: 78 53 55 8A ED 97 0B FC 6E EC FC 37 98 51 88 EF  xSU.....n..7.Q..
0x02B0: 2F 6C A2 17 B1 03 34 D8 AA 42 0F 53 3C 47 CF DE  /l....4..B.S<G..
0x02C0: CD 74 EE 28 86 C8 8E 12 7C ED E3 2A 23 FD 91 36  .t.(....|..*#..6
0x02D0: 4B 4C A6 C8 83 E8 BE 3A 36 F2 6E 81 6E 48 1D DD  KL.....:6.n.nH..
0x02E0: DE 17 E9 40 9A 37 43 9E 8A 27 FE 51 83 94 BF 29  ...@.7C..'.Q...)
0x02F0: 4A 3E EC CD 63 BA 9B CE 51 5F 9D B7 C0 9F 2D E5  J>..c...Q_....-.
0x0300: 18 F7 41 B8 A9 54 79 EA C2 B6 E2 39 64 F0 86 29  ..A..Ty....9d..)
0x0310: C2 C9 12 D4 7A F6 FA 98 C8 15 57 77 81 76 FF 69  ....z.....Ww.v.i
0x0320: 41 85 9E DF D5 0C E6 9B 3B 74 1E F5 D3 BC 2D D2  A.......;t....-.
0x0330: 8D B9 24 6A 7C F4 3B 35 D0 10 90 78 A4 8D E0 4F  ..$j|.;5...x...O
0x0340: B1 79 14 88 9A 90 58 F7 A5 ED EF 92 95 0B 69 7F  .y....X.......i.
0x0350: 97 28 F3 65 39 DB 8A 0A D1 9B E6 5C D9 3E 90 03  .(.e9......\.>..
0x0360: 66 93 03 DC E9 05 8C 42 73 4C BB 2C 92 4E E5 79  f.......BsL.,.N.y
0x0370: E8 67 6A 94 05 61 ED 02 36 EE E3 A0 03 CA 2B 72  .gj..a..6.....+r
0x0380: 56 D6 80 95 B3 30 62 BF 01 06 10 56 6A A8 57 FF  V....0b....Vj.W.
0x0390: 03 E0 66 71 3C 5B AC 0B F0 68 41 91 2D 01 E7 61  ..fq<[...hA.-..a
0x03A0: 59 9D 3D 96 76 40 18 7B 01 E6 07 55 B5 31 CC 43  Y.=.v@.{...U.1.C
0x03B0: 10 ED 18 D9 D8 77 17 8D D4 6D B6 A9 D3 C3 98 02  .....w...m......
0x03C0: 36 DC DA 39 1A C7 3F 5D 6F DA 85 49 8E 57 D1 78  6..9..?]o..I.W.x
0x03D0: 36 87 08 6C 4A 9F 16 FF 06 04 95 6A DB 2A D0 6E  6..lJ......j.*.n
0x03E0: 3C 1E DE 71 16 7D 87 4D 5D F8 E0 52 63 23 6E 41  <..q.}.M]..Rc#nA
0x03F0: 3E 43 15 D1 D3 CE 3D 1B 97 8D A4 22 C8 3E C4 EE  >C....=....".>..
0x0400: 35 C7 0D 7B 74 76 A5 65 8B E8 14 13 9E BC AB 78  5..{tv.e.......x
0x0410: 1A 22 3F 88 92 E6 D0 2E 69 66 EE EB 97 C4 CF 48  ."?.....if.....H
0x0420: 2E 68 F4 A0 10 92 BD 4F F8 2E 68 51 35 0C FD 43  .h.....O..hQ5..C
0x0430: E7 87 9E A2 B5 BB 56 C4 70 73 C2 23 91 4C 54 A2  ......V.ps.#.LT.
0x0440: E1 CD 17 72 ED 35 4E 34 3C 77 A7 CD 7F 3E 24 73  ...r.5N4<w...>$s
0x0450: FC 56 EE FD F8 B6 F4 98 4F 3F 29 46 2E 15 14 B9  .V......O?)F....
0x0460: 96 D1 5A AC CC A9 90 0F A3 50 EC 72 81 41 A7 E8  ..Z......P.r.A..
0x0470: 01 85 27 1E 33 22 A2 07 5E 3E B4 D9 4F 32 37 9E  ..'.3"..^>..O27.
0x0480: BA E1 28 DA 9F 4D 64 FB DC 1F 19 2B 47 4C CD 81  ..(..Md....+GL..
0x0490: 9F 9D D4 13 3B C6 AE CD C0 B1 83 ED 9E 38 7A 70  ....;........8zp
0x04A0: 6D AC E5 29 1E 8D 8E 79 F1 AA 77 00 C4 B2 41 C7  m..)...y..w...A.
0x04B0: B5 EE FB 6F D7 F3 37 5D 28 6F 75 AA 75 EF C1 5F  ...o..7](ou.u.._
0x04C0: 24 44 96 02 89 1A 2E A8 63 40 E2 E2 DE DC A9 60  $D......c@.....`
0x04D0: 9D 38 F6 EE D6 11 BB 9E CB 26 85 1E 84 9B 66 9E  .8.......&....f.
0x04E0: 3A 93 1E A1 0E 4A D6 A2 F4 8A 8C 00 D4 90 6C 91  :....J........l.
0x04F0: 51 CB 4A BA 91 30 AB 38 A8 3E 7E FE F0 1F B5 8F  Q.J..0.8.>~.....
0x0500: ED 93 4F F1 EE 79 58 13 02 1D D2 24 73 C6 EE 12  ..O..yX....$s...
0x0510: 4B CE 2F 4E 84 E2 C0 C3 67 DD 69 4C E9           K./N....g.iL.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.754942 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2879 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D97995E  Ack: 0x6285F27D  Win: 0x11CC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 3F 40 00 80 06 C1  .....E..(.?@....
0x0020: 7F 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 99  ....K...........
0x0030: 5E 62 85 F2 7D 50 10 11 CC 56 53 00 00 50 4F 53  ^b..}P...VS..POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.755979 10.0.9.75:1489 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2880 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D97995E  Ack: 0x6285F27D  Win: 0x11CC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 40 40 00 80 06 C1  .....E..(.@@....
0x0020: 7E 10 16 09 4B 10 16 04 9B 05 D1 07 DA 1D 97 99  ~...K...........
0x0030: 5E 62 85 F2 7D 50 11 11 CC 56 52 00 00 50 4F 53  ^b..}P...VR..POS
0x0040: 54 20 2F                                         T /
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.756297 10.0.4.155:2010 -> 10.0.9.75:1489
TCP TTL:63 TOS:0x0 ID:26687 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x6285F27D  Ack: 0x1D97995F  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 3F 40 00 3F 06 A5  .....E..(h?@.?..
0x0020: 7F 10 16 04 9B 10 16 09 4B 07 DA 05 D1 62 85 F2  ........K....b..
0x0030: 7D 1D 97 99 5F 50 10 44 6F 23 AF 00 00           }..._P.Do#...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.803756 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2881 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D98C07F  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 41 40 00 80 06 C1  .....E..0.A@....
0x0020: 75 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C0  u...K...........
0x0030: 7F 00 00 00 00 70 02 16 D0 52 7A 00 00 02 04 05  .....p...Rz.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.804080 10.0.4.155:2010 -> 10.0.9.75:1490
TCP TTL:63 TOS:0x0 ID:26688 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x628818C5  Ack: 0x1D98C080  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 40 40 00 3F 06 A5  .....E..,h@@.?..
0x0020: 7A 10 16 04 9B 10 16 09 4B 07 DA 05 D2 62 88 18  z.......K....b..
0x0030: C5 1D 98 C0 80 60 12 44 70 BE 82 00 00 02 04 05  .....`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.804511 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2882 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D98C080  Ack: 0x628818C6  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 42 40 00 80 06 C1  .....E..(.B@....
0x0020: 7C 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C0  |...K...........
0x0030: 80 62 88 18 C6 50 10 16 D0 03 E0 00 00 02 04 05  .b...P..........
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.804800 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2883 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0x1D98C080  Ack: 0x628818C6  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 3D 0B 43 40 00 80 06 C1  .....E..=.C@....
0x0020: 66 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C0  f...K...........
0x0030: 80 62 88 18 C6 50 18 16 D0 2E 1A 00 00 50 4F 53  .b...P.......POS
0x0040: 54 20 2F 74 69 6D 65 20 48 54 54 50 2F 31 2E 30  T /time HTTP/1.0
0x0050: 0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.898619 10.0.4.155:2010 -> 10.0.9.75:1490
TCP TTL:63 TOS:0x0 ID:26689 IpLen:20 DgmLen:40 DF
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***A**** Seq: 0x628818C6  Ack: 0x1D98C095  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 41 40 00 3F 06 A5  .....E..(hA@.?..
0x0020: 7D 10 16 04 9B 10 16 09 4B 07 DA 05 D2 62 88 18  }.......K....b..
0x0030: C6 1D 98 C0 95 50 10 44 70 D6 2A 00 00           .....P.Dp.*..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.899178 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2884 IpLen:20 DgmLen:166 DF
***AP*** Seq: 0x1D98C095  Ack: 0x628818C6  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 A6 0B 44 40 00 80 06 C0  .....E....D@....
0x0020: FC 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C0  ....K...........
0x0030: 95 62 88 18 C6 50 18 16 D0 70 2B 00 00 55 73 65  .b...P...p+..Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 41 63 63 65 70 74 3A 20  ndows)..Accept:
0x0070: 2A 2F 2A 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70  */*..Content-typ
0x0080: 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78  e: application/x
0x0090: 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63  -www-form-urlenc
0x00A0: 6F 64 65 64 0D 0A 43 6F 6E 74 65 6E 74 2D 6C 65  oded..Content-le
0x00B0: 6E 67 74 68 3A 20 30 0D 0A 0D 0A                 ngth: 0....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.899617 10.0.4.155:2010 -> 10.0.9.75:1490
TCP TTL:63 TOS:0x0 ID:26690 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x628818C6  Ack: 0x1D98C113  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 42 40 00 3F 06 A5  .....E..LhB@.?..
0x0020: 58 10 16 04 9B 10 16 09 4B 07 DA 05 D2 62 88 18  X.......K....b..
0x0030: C6 1D 98 C1 13 50 18 44 70 39 A8 00 00 48 54 54  .....P.Dp9...HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.899671 10.0.4.155:2010 -> 10.0.9.75:1490
TCP TTL:63 TOS:0x0 ID:26691 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x628818EA  Ack: 0x1D98C113  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 43 40 00 3F 06 A5  .....E..(hC@.?..
0x0020: 7B 10 16 04 9B 10 16 09 4B 07 DA 05 D2 62 88 18  {.......K....b..
0x0030: EA 1D 98 C1 13 50 11 44 70 D5 87 00 00           .....P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.900132 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2885 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D98C113  Ack: 0x628818EB  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 45 40 00 80 06 C1  .....E..(.E@....
0x0020: 79 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C1  y...K...........
0x0030: 13 62 88 18 EB 50 10 16 AC 03 4C 00 00 55 73 65  .b...P....L..Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.900365 10.0.9.75:1490 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2886 IpLen:20 DgmLen:40 DF
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***A***F Seq: 0x1D98C113  Ack: 0x628818EB  Win: 0x16AC  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 46 40 00 80 06 C1  .....E..(.F@....
0x0020: 78 10 16 09 4B 10 16 04 9B 05 D2 07 DA 1D 98 C1  x...K...........
0x0030: 13 62 88 18 EB 50 11 16 AC 03 4B 00 00 55 73 65  .b...P....K..Use
0x0040: 72 2D 41                                         r-A

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.900652 10.0.4.155:2010 -> 10.0.9.75:1490
TCP TTL:63 TOS:0x0 ID:26692 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x628818EB  Ack: 0x1D98C114  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 44 40 00 3F 06 A5  .....E..(hD@.?..
0x0020: 7A 10 16 04 9B 10 16 09 4B 07 DA 05 D2 62 88 18  z.......K....b..
0x0030: EB 1D 98 C1 14 50 10 44 70 D5 86 00 00           .....P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.901242 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2887 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1D99B498  Ack: 0x0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 30 0B 47 40 00 80 06 C1  .....E..0.G@....
0x0020: 6F 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B4  o...K...........
0x0030: 98 00 00 00 00 70 02 16 D0 5E 5F 00 00 02 04 05  .....p...^_.....
0x0040: B4 01 01 04 02                                   .....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.901853 10.0.4.155:2010 -> 10.0.9.75:1491
TCP TTL:63 TOS:0x0 ID:26693 IpLen:20 DgmLen:44 DF
***A**S* Seq: 0x62890A2E  Ack: 0x1D99B499  Win: 0x4470  TcpLen: 24
TCP Options (1) => MSS: 1460
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 2C 68 45 40 00 3F 06 A5  .....E..,hE@.?..
0x0020: 75 10 16 04 9B 10 16 09 4B 07 DA 05 D3 62 89 0A  u.......K....b..
0x0030: 2E 1D 99 B4 99 60 12 44 70 D8 FD 00 00 02 04 05  .....`.Dp.......
0x0040: B4                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.902230 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2888 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D99B499  Ack: 0x62890A2F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 48 40 00 80 06 C1  .....E..(.H@....
0x0020: 76 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B4  v...K...........
0x0030: 99 62 89 0A 2F 50 10 16 D0 1E 5B 00 00 02 04 05  .b../P....[.....
0x0040: B4 01 01                                         ...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.902554 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2889 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x1D99B499  Ack: 0x62890A2F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 39 0B 49 40 00 80 06 C1  .....E..9.I@....
0x0020: 64 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B4  d...K...........
0x0030: 99 62 89 0A 2F 50 18 16 D0 2A 68 00 00 50 4F 53  .b../P...*h..POS
0x0040: 54 20 2F 20 48 54 54 50 2F 31 2E 30 0D 0A        T / HTTP/1.0..
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.917703 10.0.9.75:1486 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2890 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D946580  Ack: 0x6283A01B  Win: 0x1596  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 4A 40 00 80 06 C1  .....E..(.J@....
0x0020: 74 10 16 09 4B 10 16 04 9B 05 CE 07 DA 1D 94 65  t...K..........e
0x0030: 80 62 83 A0 1B 50 10 15 96 D8 D1 00 00 50 4F 53  .b...P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.998613 10.0.4.155:2010 -> 10.0.9.75:1491
TCP TTL:63 TOS:0x0 ID:26694 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62890A2F  Ack: 0x1D99B4AA  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 46 40 00 3F 06 A5  .....E..(hF@.?..
0x0020: 78 10 16 04 9B 10 16 09 4B 07 DA 05 D3 62 89 0A  x.......K....b..
0x0030: 2F 1D 99 B4 AA 50 10 44 70 F0 A9 00 00           /....P.Dp....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:29.999890 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2891 IpLen:20 DgmLen:699 DF
***AP*** Seq: 0x1D99B4AA  Ack: 0x62890A2F  Win: 0x16D0  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 02 BB 0B 4B 40 00 80 06 BE  .....E....K@....
0x0020: E0 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B4  ....K...........
0x0030: AA 62 89 0A 2F 50 18 16 D0 1A 54 00 00 55 73 65  .b../P....T..Use
0x0040: 72 2D 41 67 65 6E 74 3A 20 4E 46 52 20 43 6F 6E  r-Agent: NFR Con
0x0050: 73 6F 6C 65 2F 31 20 28 32 2E 31 29 20 28 57 69  sole/1 (2.1) (Wi
0x0060: 6E 64 6F 77 73 29 0D 0A 43 6F 6E 74 65 6E 74 2D  ndows)..Content-
0x0070: 74 79 70 65 3A 20 6E 66 72 5F 64 65 73 0D 0A 43  type: nfr_des..C
0x0080: 6F 6E 74 65 6E 74 2D 43 6F 64 69 6E 67 3A 20 61  ontent-Coding: a
0x0090: 70 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 6E 66 72  pplication/x-nfr
0x00A0: 5F 73 74 72 65 61 6D 0D 0A 55 73 65 72 6E 61 6D  _stream..Usernam
0x00B0: 65 3A 20 6E 66 72 0D 0A 54 69 63 6B 65 74 3A 20  e: nfr..Ticket:
0x00C0: 49 7D 25 44 30 25 39 35 25 46 35 25 43 42 25 44  I}%D0%95%F5%CB%D
0x00D0: 37 25 32 42 25 45 38 25 43 43 43 25 30 43 25 39  7%2B%E8%CCC%0C%9
0x00E0: 45 4F 25 44 31 25 38 36 30 25 41 46 25 41 46 25  EO%D1%860%AF%AF%
0x00F0: 39 32 66 34 25 43 33 43 25 41 46 25 43 31 25 46  92f4%C3C%AF%C1%F
0x0100: 35 25 39 34 4F 43 25 38 32 25 46 44 3C 25 45 30  5%94OC%82%FD<%E0
0x0110: 25 46 32 6D 31 7F 25 33 42 25 33 41 0D 0A 43 6F  %F2m1.%3B%3A..Co
0x0120: 6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 34 31  ntent-length: 41
0x0130: 31 0D 0A 0D 0A 1A 2F E8 53 4A 74 B8 FB 02 2D 62  1...../.SJt...-b
0x0140: 18 DC FE CA B4 C0 79 8E 41 10 65 45 D5 D9 D3 98  ......y.A.eE....
0x0150: CF EC C6 CB 2B 39 4A EF 2A 78 70 84 1B 29 5A F1  ....+9J.*xp..)Z.
0x0160: 8E A4 C7 02 9D DF AA 49 53 F2 DA 75 60 8E CF E9  .......IS..u`...
0x0170: CD F9 21 C2 66 23 5A BA B1 0E 11 CF 1E 6F AA DE  ..!.f#Z......o..
0x0180: 96 8F 30 4F F5 89 09 19 7F C7 B8 2F D8 CB D0 66  ..0O......./...f
0x0190: DD B8 D9 73 7D 8E 63 A6 5A 62 46 15 06 B0 2B B3  ...s}.c.ZbF...+.
0x01A0: DE 70 8C 07 AE 3A 21 75 1E 93 25 D5 45 B1 6A 76  .p...:!u..%.E.jv
0x01B0: 03 80 2E 0B BF B6 F7 E7 76 BA 39 5E 97 74 F0 9A  ........v.9^.t..
0x01C0: 19 78 10 B0 67 56 B0 C0 98 EF B3 30 BC 1F AA F2  .x..gV.....0....
0x01D0: 7D B8 62 25 28 72 CF 08 38 FA EF 16 A9 95 EF 25  }.b%(r..8......%
0x01E0: D9 BD ED FB A8 22 B7 B0 22 40 27 B4 32 F6 8B C3  .....".."@'.2...
0x01F0: 36 C7 74 1B 15 C8 0F A4 A9 9C AC 90 56 F4 98 FD  6.t.........V...
0x0200: 05 A0 85 6E 62 7F 04 F4 63 4E 45 C0 A5 7F 3B DD  ...nb...cNE...;.
0x0210: 18 BC 1D A6 C4 01 38 76 86 23 2B 56 05 56 B4 9E  ......8v.#+V.V..
0x0220: D1 85 DA BF 14 86 24 5B 4B 9C 16 B7 6A A1 E4 07  ......$[K...j...
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0230: A4 79 30 22 D4 AC DF 92 04 F8 A0 8F 98 EB C3 81  .y0"............
0x0240: 1A 3D CB 03 B3 23 C1 5F 12 E1 F3 C2 CD 6D 51 03  .=...#._.....mQ.
0x0250: A4 08 69 B3 FA BB BD C2 87 13 D5 50 A0 59 36 55  ..i........P.Y6U
0x0260: 6C BD DC DE 79 F3 D6 B4 BC 2D 7A 5A 47 5C BD 53  l...y....-zZG\.S
0x0270: F3 DC AF EF 3B 2F E5 B0 24 C1 01 5E 83 39 BB 3F  ....;/..$..^.9.?
0x0280: A8 FA D3 84 E5 50 F8 90 74 CF 9B 11 6F 50 CF F5  .....P..t...oP..
0x0290: EC 96 AA 74 09 DE 2F 49 25 BA B2 C4 29 34 F3 46  ...t../I%...)4.F
0x02A0: CA 19 15 19 EC 69 1B 96 E8 19 C2 5E 0D 4F EE 18  .....i.....^.O..
0x02B0: DF EE D5 8E 00 0B D9 54 B1 4E DE BF 52 93 68 92  .......T.N..R.h.
0x02C0: 85 7D 8E DB 95 11 47 FD 27 09 AD A1 33 2F 62 E2  .}....G.'...3/b.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:30.000696 10.0.4.155:2010 -> 10.0.9.75:1491
TCP TTL:63 TOS:0x0 ID:26695 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x62890A2F  Ack: 0x1D99B73D  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 4C 68 47 40 00 3F 06 A5  .....E..LhG@.?..
0x0020: 53 10 16 04 9B 10 16 09 4B 07 DA 05 D3 62 89 0A  S.......K....b..
0x0030: 2F 1D 99 B7 3D 50 18 44 70 52 12 00 00 48 54 54  /...=P.DpR...HTT
0x0040: 50 2F 31 2E 30 20 32 30 30 20 4F 4B 0D 0A 54 69  P/1.0 200 OK..Ti
0x0050: 6D 65 3A 20 39 38 36 34 30 30 32 36 32 0D 0A 0D  me: 986400262...
0x0060: 0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:30.004856 10.0.4.155:2010 -> 10.0.9.75:1491
TCP TTL:63 TOS:0x0 ID:26696 IpLen:20 DgmLen:202 DF
***AP**F Seq: 0x62890A53  Ack: 0x1D99B73D  Win: 0x4470  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 CA 68 48 40 00 3F 06 A4  .....E...hH@.?..
0x0020: D4 10 16 04 9B 10 16 09 4B 07 DA 05 D3 62 89 0A  ........K....b..
0x0030: 53 1D 99 B7 3D 50 19 44 70 6C 79 00 00 02 34 EF  S...=P.Dply...4.
0x0040: 57 45 6A F5 AC 3E 82 60 2F 8A AE AF 42 18 6A 05  WEj..>.`/...B.j.
0x0050: 1D 4B 68 BF 28 28 99 68 65 CF 8B 6B BB 05 11 8E  .Kh.((.he..k....
0x0060: 6D E4 AC 6E B0 B3 75 36 15 FB 59 7B 07 B1 7F C3  m..n..u6..Y{....
0x0070: 05 18 9A 74 EB 5C C5 2B 56 6A 2D A7 81 86 32 32  ...t.\.+Vj-...22
0x0080: 18 07 C8 EE 41 B8 4D 00 1F BE 1E 50 F2 46 5E 42  ....A.M....P.F^B
0x0090: 91 A8 DF 07 F3 62 FC 51 EF 2A 69 40 EF 4B 75 AB  .....b.Q.*i@.Ku.
0x00A0: FC 57 38 5B 1F BC 53 29 E2 26 76 24 71 F5 77 DB  .W8[..S).&v$q.w.
0x00B0: 26 FB 8E 64 7B DA FA 9F 8B C3 7F FB B4 16 1B E6  &..d{...........
0x00C0: C6 C2 D0 A8 09 0C E4 D3 F4 C7 52 AC 60 E0 BB E7  ..........R.`...
0x00D0: 7C 08 36 9D 65 54 11 97 2F DB 9E 7B E5 22 86     |.6.eT../..{.".

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:30.005388 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2892 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1D99B73D  Ack: 0x62890AF6  Win: 0x160A  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 4C 40 00 80 06 C1  .....E..(.L@....
0x0020: 72 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B7  r...K...........
0x0030: 3D 62 89 0A F6 50 10 16 0A 1B B6 00 00 50 4F 53  =b...P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:30.005801 10.0.9.75:1491 -> 10.0.4.155:2010
TCP TTL:128 TOS:0x0 ID:2893 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1D99B73D  Ack: 0x62890AF6  Win: 0x160A  TcpLen: 20
0x0000: 50 00 00 0C 07 AC 03 00 50 8B 52 4E 91 AA AA 03  P.......P.RN....
0x0010: 00 00 00 08 00 45 00 00 28 0B 4D 40 00 80 06 C1  .....E..(.M@....
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0x0020: 71 10 16 09 4B 10 16 04 9B 05 D3 07 DA 1D 99 B7  q...K...........
0x0030: 3D 62 89 0A F6 50 11 16 0A 1B B5 00 00 50 4F 53  =b...P.......POS
0x0040: 54 20 2F                                         T /

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

04/04-10:43:30.006125 10.0.4.155:2010 -> 10.0.9.75:1491
TCP TTL:63 TOS:0x0 ID:26697 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x62890AF6  Ack: 0x1D99B73E  Win: 0x446F  TcpLen: 20
0x0000: 50 00 50 8B 52 4E 91 00 10 F6 4A 98 1C AA AA 03  P.P.RN....J.....
0x0010: 00 00 00 08 00 45 00 00 28 68 49 40 00 3F 06 A5  .....E..(hI@.?..
0x0020: 75 10 16 04 9B 10 16 09 4B 07 DA 05 D3 62 89 0A  u.......K....b..
0x0030: F6 1D 99 B7 3E 50 10 44 6F ED 4F 00 00           ....>P.Do.O..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The preceding packets were all required simply to log on to the NFR NID 200 sensor using the remote workstation Administration Interface. The packet stream stops when the management client sends a FIN/ACK, which the sensor acknowledges. The user now has completed the logon sequence, and has the GUI displayed on his screen. In summary, the system issues a Kerberos ticket for each user who logs in and creates a unique, secure communications channel between the user and the sensor system.

Checklist Item 6 – Test Isolation of Management Network

This test was designed to verify that the network on which the management workstation resides is physically isolated from the rest of the organization's internal network. The management workstation could have a single, point-to-point network connection from it to the management interface on the NID 200 sensor, or it could be on a small LAN that is physically isolated from the rest of the organization's internal network. In conducting the audit, we discovered that the latter case was true.

There were two parts of this audit checklist item: Physical inspection of the network cables in the isolated management LAN, and using scanning software to verify the results of our physical inspection. We inspected all of the physical cabling of the systems in the isolated management LAN and found no physical connections from the half dozen systems connected to a common hub. We then used a scanning tool to confirm that we did not miss any hidden cables. The following table shows the results of a ping sweep scan using a network management tool called SolarWinds. It enumerates all of the active TCP/IP-based systems on the network to which the NFR management station is connected.

Ping Sweep Results

IP Address	Response Time	DNS Lookup
172.16.10.10	0 ms	
172.16.10.20	0 ms	
172.16.10.65	0 ms	SolarWinds System
172.16.10.70	0 ms	NFR MGMT Server
172.16.10.75	0 ms	
172.16.10.100	0 ms	CORPSERVER

Exported from PingSweep Version 4.0.409 on 4/1/2002 10:26:20 AM
SolarWinds.Net

In the output of this tool, we can see that it found a total of six different systems: 172.16.10.65 is the host from which the SolarWinds tool was run. 172.16.10.70 is the NFR AI remote management workstation that manages the NID 200 sensor. 172.16.10.75 is the management interface on the NID 200 sensor itself. The three remaining systems are other administrative systems that are unrelated to the management of the intrusion detection system. The DNS Lookup names have been sanitized.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A concern that we had in conducting this test was the possibility that we missed a network connection to another network, and one of these systems was forwarding IP packets, in effect acting as a router. To eliminate this possibility, we ran another tool in the SolarWinds suite called NetSonar, which takes router IP addressess as input and attempts to use the routing tables on those systems to discover routes to other networks. We entered the IP addresses of all of the systems we found using the ping sweep and let the tool interrogate them for routing capability. As shown below, the results were negative:

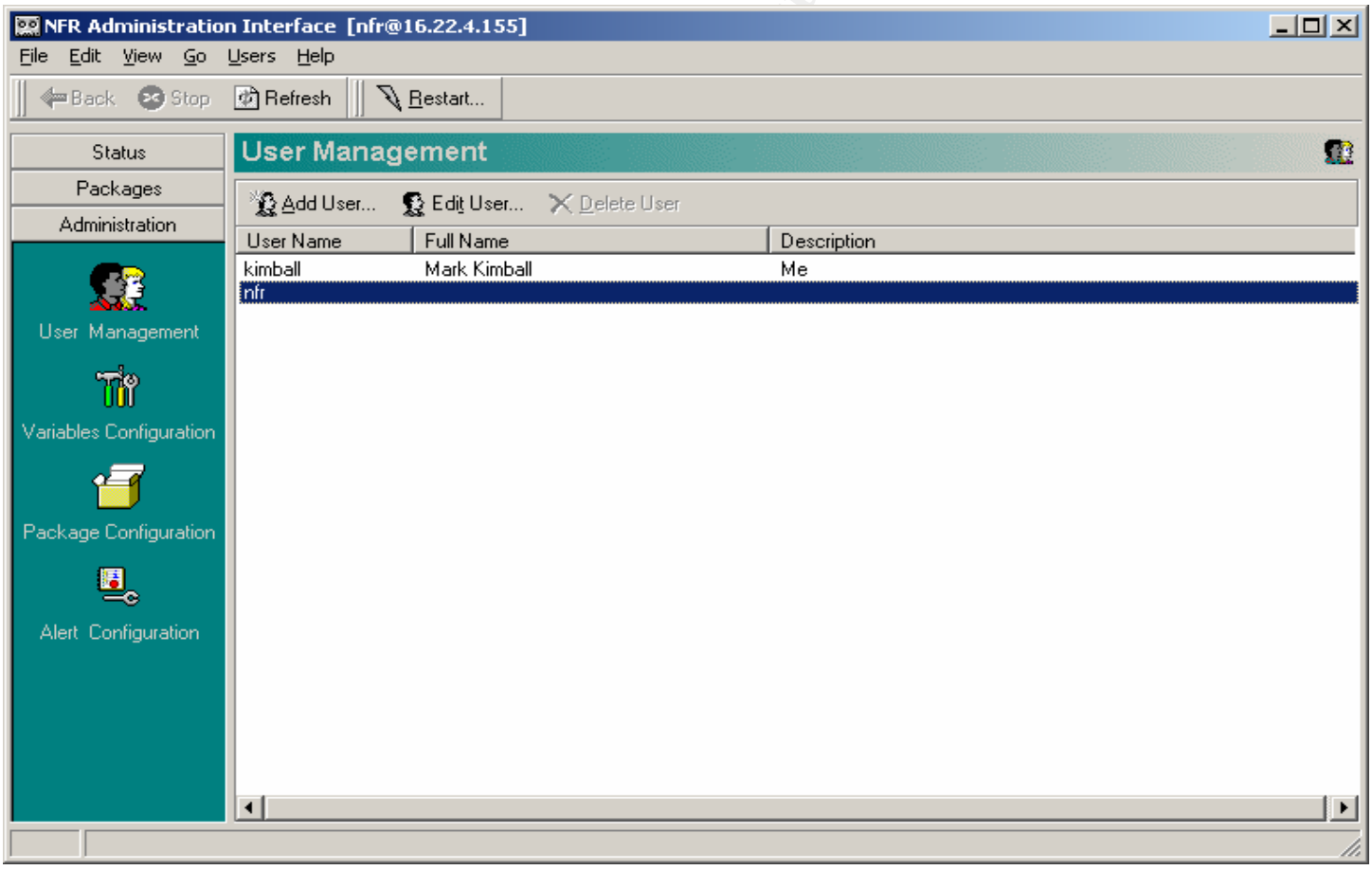
```
# Routers exported from New.SDB
#
# Network Sonar   Version 3.1.471
# Discovery Engine Version 3.2.4
# 4/1/2002 11:19:13 AM

SysName,"Agent IP Address",DNS,"Response Time",Vendor,"System
Description",Community,Location,Contact,"Last Boot Time",Interfaces,"Discovery Status"
```

author retains full rights.

Checklist Item 7 – Unnecessary User Accounts

This test was designed to verify that there are no unnecessary or extra user accounts on the system. Superfluous user accounts represent an added security risk because there are more avenues through which an attacker can gain access to the system. More user accounts means more potentially weak passwords, accounts left logged in on unattended workstations, and so on.



Checklist Item 8 – Sensor Management Interface Open Ports

This test was designed to establish which ports, if any, are open on the NID 200 sensor's management interface. We used the Nmap port-scanning tool to carry out this test.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Nmap port-scanning program was running on a Red Hat 7.0 Linux-based system. The version of Nmap we used was 2.53. The following is the output of the Nmap command as described below.

Nmap was run with a number of different command line options. We used the TCP stealth scan at a normal scan rate. As you can see from the output, nmap only saw a single port, tcp port 2010, open on the NID 200 sensor's management interface. This is a very secure system. There are no extraneous ports open on the system that could be attacked. The only port that is open is tcp port 2010. This port is used by the Administration interface on the management workstation to communicate with the sensor. In addition, Nmap was unable to positively identify the host operating system using its fingerprinting function. The TCP Sequence Prediction is difficult. This is all good news for the IDS administrator.

Nmap (V. nmap) scan initiated 2.53 as: nmap -v -sS -R -O -P0 -oN gsna.txt 10.0.4.155

Interesting ports on nfr.lab.mycorp.net (10.0.4.155):

(The 1522 ports scanned but not shown below are in state: closed)

Port State Service

2010/tcp open search

TCP Sequence Prediction: Class=random positive increments

Difficulty=24944 (Worthy challenge)

Sequence numbers: 4EEA38CA 4EEAFF8C 4EEC69C5 4EED9E7C 4EEE22B2 4EEFA5C7

No OS matches for host (If you know what OS is running on it, see http://www.insecure.org/cgi-bin/nmap-submit.cgi).

TCP/IP fingerprint:

TSeq(Class=RI%gcd=1%SI=103D3)

TSeq(Class=RI%gcd=1%SI=9F72)

TSeq(Class=RI%gcd=1%SI=6170)

T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)

T2(Resp=N)

T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=M)

T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)

T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)

T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)

PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DAT=E)

Nmap run completed at Wed Apr 3 16:16:44 2002 -- 1 IP address (1 host up) scanned in 14 seconds

Checklist Item 9 – Sensor Monitor Interface Detectability

This test was designed to verify that the NID 200 sensor's monitor interface is completely undetectable by potential attackers. To reiterate the design of the system, remember that it is impossible to assign an IP address to the sensor monitor interface. In fact, the sensor monitor interface has no TCP/IP capability associated with it. It simply listens passively to all network traffic, examining each packet as it receives it. To confirm that there is in fact no TCP/IP capability associated with the monitor interface, we used a MAC address-scanning tool that is part of the SolarWinds suite. The tool produced the following results:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MAC Addresses

Subnet 172.16.0.0\255.255.0.0

IP Address	MAC Address	DNS	Network Card Manufacturer
172.16.10.10	0000.F875.2C3C		DIGITAL EQUIPMENT CORPORATION
172.16.10.20	0000.F875.2C3C		DIGITAL EQUIPMENT CORPORATION
172.16.10.65	0050.8BD8.BEFD		COMPAQ COMPUTER CORPORATION
172.16.10.70	0008.C7AF.C3E0		COMPAQ COMPUTER CORPORATION
172.16.10.75	0020.ED11.0F5B		GIGA-BYTE TECHNOLOGY CO., LTD.
172.16.10.100	0000.F806.C736	CORPSERVER	DIGITAL EQUIPMENT CORPORATION

Exported from MAC Address Discovery Version 1.1.95 on 4/1/2002 10:51:39 AM
SolarWinds.Net

As we can see, the tool enumerates all of the systems in subnet 172.16.0.0/255.255.0.0. The same six systems we found in a ping sweep in an earlier test also show up here, along with the MAC addresses of their interfaces. The monitor interface for the NID 200 is on a different network, so it would not appear in this list anyway. We then scanned the external, public Internet-facing network where the monitor interface terminates. The results of this scan do not reveal the NID 200's monitor interface MAC address. The only evidence that the monitor interface is there is the presence of a link light LED on the device to which it is attached:

MAC Addresses

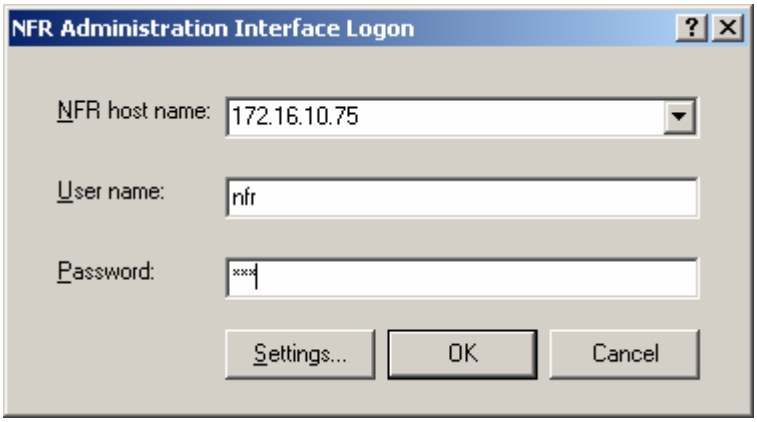
Subnet 192.168.4.0\255.255.255.0

IP Address	MAC Address	Network Card Manufacturer
192.168.4.1	0002.A5FB.9F5F	Compaq Computer Corporation
192.168.4.2	0000.F878.3246	DIGITAL EQUIPMENT CORPORATION
192.168.4.4	0800.2BC3.C5E3	DIGITAL EQUIPMENT CORPORATION
192.168.4.5	0050.8BD8.BFD8	COMPAQ COMPUTER CORPORATION
192.168.4.6	0050.8BD8.BEFD	COMPAQ COMPUTER CORPORATION
192.168.4.7	0000.D1EE.AD41	ADAPTEC INCORPORATED
192.168.4.10	0050.8B66.2628	COMPAQ COMPUTER CORPORATION
192.168.4.20	0207.0113.F46B	RACAL-DATACOM
192.168.4.21	0207.0113.E500	RACAL-DATACOM
192.168.4.22	0207.0113.F7E3	RACAL-DATACOM
192.168.4.23	0207.0113.F805	RACAL-DATACOM
192.168.4.45	0003.6B75.B6BF	Cisco Systems, Inc.
192.168.4.46	0080.C75D.4DE2	XIRCOM
192.168.4.51	0040.EA02.1904	PLAIN TREE SYSTEMS INC
192.168.4.52	0000.1D1A.773D	CABLETRON SYSTEMS, INC.
192.168.4.53	0000.1D1D.7D13	CABLETRON SYSTEMS, INC.
192.168.4.54	0000.1D18.DB73	CABLETRON SYSTEMS, INC.
192.168.4.55	0800.2BA3.902B	DIGITAL EQUIPMENT CORPORATION
192.168.4.56	0000.F8C7.0200	DIGITAL EQUIPMENT CORPORATION
192.168.4.57	0800.2BA6.B140	DIGITAL EQUIPMENT CORPORATION
192.168.4.58	0800.2BA1.C30C	DIGITAL EQUIPMENT CORPORATION
192.168.4.59	0800.2BB3.0B80	DIGITAL EQUIPMENT CORPORATION
192.168.4.60	0010.F64A.9870	CISCO SYSTEMS, INC.
192.168.4.61	0050.3E6B.B88C	CISCO SYSTEMS, INC.
192.168.4.62	0000.0C07.AC04	CISCO SYSTEMS, INC.

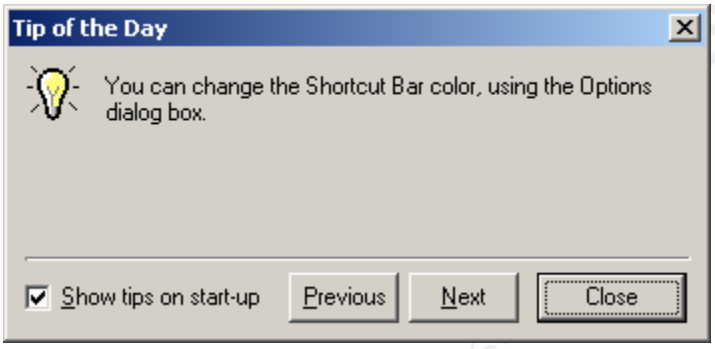
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Checklist Item 10 – Forced Administrator Password Change After Install

This checklist item was designed to check whether the NFR Security NID 200 intrusion detection sensor forces the system administrator to change the default system password after the system is installed and the administrator logs in for the first time. The default password for the nfr account is "nfr". The system does **not** require a password change from the default password when one first logs in:



In the NFR Administration Interface logon box, we can see what the user sees when first logging in to the sensor after installation of the AI on the management workstation. The Password field shows three asterisks, which represent the default nfr account password of nfr. Clicking OK brings us to the main management screen. No password change is required.



Is the System Securable? (Evaluate the System)

In our opinion, the NFR Security NID 200 is quite securable. Unlike many multi-user, general-purpose computing systems that serve a wide range of users and an even wider range of functions, the NID 200 is dedicated to a single task: Network intrusion detection. You can configure the NID 200 to allow the least amount of access by the fewest users. The system is extremely well bounded to performing just those tasks that its users need to get the job of intrusion detection done. The greatest number of vulnerabilities seems to be those that involve the human element.

For example, when the system administrator first installs the system, the system does not force him or her to select a new, hard-to-guess/hard-to-break password. Furthermore, the system allows the administrator to create accounts that have short (4 characters or less) passwords and to change that password to something as short as one character. This places the responsibility of creating stringent passwords on the administrator and users. This is not a good idea. Many other computer security products enforce difficult to guess passwords and force the user to select a new one periodically. In addition, it is easy to design a network where the management station resides in a physically isolated area.

Is the System Auditable? (Evaluate the Audit)

For the most part, the NFR NID 200 is auditable. The checklist items we developed were mostly objective and easily verifiable. The primary weakness of the system is its non-enforcement of hard-to-guess, hard-to-break passwords. Using

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the user administration function, we can tell how many characters a particular password is, but we cannot tell if those characters are all the same, for example, fffffffff (ten f's). The only way to tell if a password is difficult to crack would be to interview the system administrator or users and ask them if they use a combination of upper and lower case characters, numbers, and non-alphanumeric characters when they create their passwords. Even then, this is very subjective: We are relying on the human elements to tell us what they do, even if there is a formal corporate policy in place. Of course there is often a huge discrepancy between what people say they do, and what they actually do in practice. What we need is a tool like l0phtcrack that we run against the password database to see if the passwords in it are easy to guess or crack. Because the NID 200 is a bounded appliance, with no general-purpose user interface with which to interact with the underlying operating system, this is quite unlikely to work.

Besides the weakness of the audit process regarding the authentication system, there seems to be no way to verify whether we can verify if the system drops packets while it is under heavy load, such as during a denial-of-service attack, or that the monitor interface will fail to respond to any stimulus it receives.

Assignment Four – Follow Up

Executive Summary

On April 1, 2002, Acme Consulting Services conducted an audit of ReallyBig Corporation's NFR Security NID 200 intrusion detection system. The NFR Security NID 200 serves as the corporation's early warning system to defend against network-based attacks. This audit was the result of a request by ReallyBig Corporation's CIO and the Director of Security Services. Acme Consulting Services would like to thank the members of ReallyBig Corporation's IT Services department for their cooperation during the audit. We could not have achieved the desired results without your help.

Briefly, we consider the assessment of the NID 200 system to be an unqualified success. The number and type of problems we uncovered are mostly process-related, and relatively minor. We believe that they can be easily corrected with minimum effort and expense. The weaknesses in the administration of the system that we found can be easily corrected. The creation of standard written policies which, if followed carefully can eliminate most of the risk associated with the operation of the system. We feel that our recommendations can help ReallyBig Corporation secure its computing environment from future threats. We look forward to working with ReallyBig Corporation in the future. The sections below address the following topics:

1. Audit Findings describes what we found during the audit.
2. Background/Risk contains items that are not in compliance and the risk that is associated with each item.
3. Audit recommendations outlines what ReallyBig Corporation needs to do to correct the problems identified in the Audit Findings section.
4. Costs addresses the costs involved in either eliminating or mitigating the risk associated with each item that was not in compliance.
5. Compensating Controls describes strategies to mitigate the risk involved with items that may be too expensive or impractical to eliminate as risks.

Audit Findings

This section contains details of our findings during the audit. Our methodology for the audit was as follows: The scope of the audit was confined to the NFR Security NID 200 sensor system, including

1. The role the sensor plays in the ReallyBig Corporation network
2. The way it communicates with the remote management station
3. The way in which the users or system administrator interact with and manage the system.

The NFR Security NID 200 intrusion detection system is situated just outside of ReallyBig Corporation's corporate firewall. The NID 200 has two network interfaces: One facing the public Internet, and one facing the internal network. There are several areas of concern regarding the design of the intrusion detection system's configuration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

First, we verified that the NID 200 has no TCP/IP stack or address bound to its public facing, or monitor interface. We confirmed this by running a network discovery using the SolarWinds Network discovery tool. All of the systems running TCP/IP that the tool found were accounted for and did not include the NID 200. Furthermore, we wanted to confirm that the NFR NID 200 system's monitor interface could not be given an IP address manually. Based on our investigation, there is no way to assign an IP address to the NID 200's monitor interface. See checklist item number two for more details. Finally, we needed to confirm that the sensor's monitor interface was completely undetectable by any kind of device, which it is. See checklist item number nine for details of this test. In summary, the NFR Security NID 200 is designed to be completely undetectable out of the box, and the monitor interface cannot be intentionally or accidentally misconfigured to allow network visibility. If there is no network visibility, there is very little chance that an intruder could detect the system, break in, and disable it, thereby rendering the ReallyBig Corporation's internal network prone to other attacks.

Second, we examined the way in which the sensor communicates with the remote management workstation. What we found was that the Administration Interface (AI) application on the management station creates a secure communications channel between the sensor and itself for all communications. This was confirmed by capturing encrypted traffic sent between the sensor and the management station. Details of that communication, including passwords and commands, could not be recovered from the traffic stream. See checklist item number five for details. Finally, we ran a network discovery using the SolarWinds discovery tool to confirm that the network on which the management station resides was physically isolated from the rest of ReallyBig Corporation's internal network. This is important because the management interface on the sensor must be connected to the same physical network as the management workstation. If the network on which the management workstation resides is not physically isolated from the rest of the internal network, this represents a potential security risk to the organization. This is perhaps the greatest risk for the system. If a user inside the company's network were to gain access to the system, he could selectively disable one or two attack signatures. This kind of subtle degradation of service might go unnoticed by the system administrator and could allow certain malicious exploits against the company's perimeter to proceed unnoticed.

Third, we examined the way in which the system is administered in ReallyBig Corporation and how the users interact with the system. This area contains the most risk for your organization. While the system allows the creation of long, complex, hard-to-break passwords, it also allows for short, simple, easy-to-guess passwords as well. These findings are described in greater detail in the following section, Background/Risk.

Background/Risk

The majority of the risk we found centered on user account creation and the passwords for those accounts. By default the NFR Security NID 200 comes with a single administrator user account (nfr) with a password of nfr. During our audit, we discovered that the system administrator had not changed the default nfr administrator account password from its factory default setting. This is a serious security risk for your organization. If a malicious user inside the company knew the default password for this type of system, he could effectively disable it, rendering your company's network susceptible to outsider attacks.

Studies have shown that the threat of insider attack/mischief is greater than that of attacks from outside. If the NFR NID 200 has a weakness, it is that it allows the system administrator to create passwords for the default admin account (nfr) or other user accounts that are incredibly weak. If the user logs in to the AI and selects the **Change Password…** feature from the Edit menu, he can set a password that is as short as a single character. It is a well-known best practice in the industry that passwords that contain both upper and lower case characters, numbers, and non-alphanumeric characters are harder to guess or break.

Because the authentication system is so weak, this leads to yet another vulnerability. There is the possibility that an inside user could degrade the attack recognition configuration by selectively disabling the NID 200's package alerts. There is no built-in logging or configuration change notification system, like Tripwire, that would notify the system administrator of changes performed without their knowledge.

Audit Recommendations

Our recommendations are targeted almost exclusively on the areas of user account creation and management. While the NFR Security NID 200 is basically a secure intrusion detection appliance out-of-the-box, it needs to be correctly

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

configured and managed to ensure that it cannot be compromised. First, the default administrator password for the nfr account should be changed immediately to something that is neither easy-to-guess, nor easy-to-break. We recommend at least an eight-character password, consisting of both upper and lower case characters, numbers, and non-alphanumeric characters. This policy should be followed for all user accounts on the system.

ReallyBig Corporation needs a written policy in place that outlines the procedure for creating new user accounts on the system, and the creation of passwords for those accounts. The number of accounts on the system should be kept to an absolute minimum, so as to reduce the risk of exposure of the system to insider attack. Also, the system administrator should follow the policy of least privilege; that is, users of the system should be limited by policy to only those privileges that they require for their job. For example, not all users on the system need to be able to configure it. The Permissions tab on user account management/creation allows the system administrator to selectively allow certain types of operations (Configure, Query, View Alerts, Diagnostics) that the user can perform. If a particular user only needs to view alerts or look at diagnostics, there is no need to give them the privilege to configure the system, create accounts, or change passwords.

Finally, there appears to be no way to create a baseline of currently enabled packages, or attack/alert signatures. The system administrator can and should print out the system Variables configuration. However, there is no print capability for the items in the signature database.

Costs

The costs associated with correcting the deficiencies outlined above should not be great. To reiterate, the root causes of the weaknesses in the system are mainly human resource, or personnel issues. System administration and users of the intrusion detection system must be instructed to create and use passwords that are complex and hard to guess or break. The primary cost would be the creation of a written policy, and the dissemination of that policy to all system administration personnel.

Compensating Control

If the cost of creating and distributing written policies and procedures for training system administration personnel is too high to reduce the risk associated with the creation and use of weak passwords, there isn't much that one can do except change to an entirely different product that enforces the use of strong passwords.

Regarding the possibility that an insider who has access to the system could modify the system's attack recognition and alerting capability, the system administrator needs to find a way to make a copy of the current configuration which acts as a baseline, and which can be compared to the running system configuration on a regular basis. The system does not have this functionality built in. The only suggestion might be to perform a screen capture of each of the appropriate screens that show whether package signatures are enabled or disabled.

References

[1] https://support.nfr.com/nid-200/, "NFR NID 200 Getting Started Guide". 2001.

[2] https://support.nfr.com/nid-200/, "NFR NID 200 User's Guide". 2001.

[3] http://www.nss.co.uk/ Intrusion Detection Group Test. The NSS Group, 2001.

[4] "CobiT 3rd Edition Audit Guidelines". Information Systems Audit and Control Foundation (ISACAF). 2000.

[5] Proctor, Paul. "The Practical Intrusion Detection Handbook". Prentice Hall Publishing. 2001.

[6] Northcutt, Stephen. "Network Intrusion Detection An Analyst's Handbook". New Riders Publishing. 2001.

[7] Ranum, Marcus. "Intrusion Detection and Network Forensics". Slide show presentation. 2000.

[8] SANS Institute. "Track 3 – Intrusion Detection In-Depth. http://www.sans.org.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.