



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 permitted without express written permission.

Table of Contents	1
ronald_black_GCFW.doc.....	2

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



**SANS GIAC Certification
Level 2 GCFW
Firewall and Perimeter Protection Curriculum**

**Practical Assignment
for
Capital SANS 2000**

**Ronald W. Black
February, 2001**

Structure of GCFW Practical Version 1.4

Assignment 1: Security Architecture

Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn \$200 million per year in online sales of fortune cookie sayings. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.

The candidate must consider and define access for:

- Customers (the companies that purchase bulk online fortunes);
- Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
- Partners (the international partners that translate and resell fortunes).

This architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

Assignment 2: Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for at least the following three components: Border Router, Primary Firewall and VPN. You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

By “security policy we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers, and partners. Keep in mind you are an E-Business with customers, suppliers and partners – you may not simply block everything.

For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:

1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
2. Any relevant information about the behavior of the service or protocol on the network.
3. The syntax of the ACL, Filter, rule, etc.
4. A description of each of the parts of the filter.
5. An explanation of how to apply the filter.
6. If the filter is order dependent, list any rules that should precede and/ or follow this filter, and why this order is important.
7. Explain how to test the ACL/filter/rule.

Assignment 3: Audit Your Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and Primary Firewall described in Assignment 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Border Router and Primary Firewall are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment, analyze the perimeter defense and make recommendation of improvements or alternate architectures.

Assignment 4: Design Under Fire

Select a network design from any previously posted GCFW Practical and paste the graphic into your submission. Design the following three attacks against the architecture.

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise and internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

© SANS Institute 2000 - 2002. All rights reserved. This document is for educational purposes only. It is not to be distributed, reproduced, or used in any manner without the written permission of SANS Institute.

Assignment 1 Submission: Security Architecture

This assignment requires the definition of a security architecture for GAIC Enterprises, a startup E Business. The architecture must specify filtering routers, firewalls, VPNs to Partners, secure remote access and internal firewalls. Defining a security architecture and security policy can be the sort of question about the chicken and the egg. Which comes first?

VISA has established core security requirement for their E Business partners. As a requirement for its core business, VISA has identified the following list of requirements for all e-business partners:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data accessible from the Internet.
4. Encrypt data sent across networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business "need to know."
7. Assign unique IDs to each person with computer access to data.
8. Track access to data by unique ID.
9. Don't use vendor-supplied defaults for system passwords and other security parameters.
10. Regularly test security systems and processes.

VISA's core requirements lend themselves to defense-in-depth, which is layered protection consisting of complementary countermeasures which provide both a robust infrastructure and the ability to contain and recover from incidents. Some aspects of a well designed defense-in-depth strategy will include the following:

1. Block attempts to map the site network
2. Detect attempts to probe the network or attacks against the infrastructure or connected computers.
3. Minimize information disclosure
4. Protect information during transmission and at rest.
5. Protect against malicious code.
6. Limit traffic into and out of the site to that which meets the "acceptable use" policy or criteria of the site.

Using this as the underlying security policy, a security architecture can begin to be designed. We also need to define some other fundamental principles for this architecture. We will keep the network as secure as possible with the available resources. Resources are always finite and there will always be some residual risk. The key is to know what those risks are and to manage those risks. Whenever possible we will err on the side of security. We will use web-browser based applications with SSL-based security to interact with our customers and partners rather than applications that require special software to be installed on workstations. Everything which could enter or leave our network is explicitly denied unless explicitly required and allowed. We will attempt to choose technologies and products to implement our business, security policies and security architectures that reduce the technical complexities for the people administering them. We will attempt to choose technologies that are scalable and offer multiple platform support. We will attempt to stay away from technologies (like MS Windows 9X) that don't have an adequate level of security features built in.

While the relative merits of various desktop operating system environments are hotly and religiously debated, we will use a single operating system environment for both workstations and servers. Choosing to use relatively inexpensive Intel based workstations, notebooks and servers as hardware platforms, we could still have a choice of several operating systems.

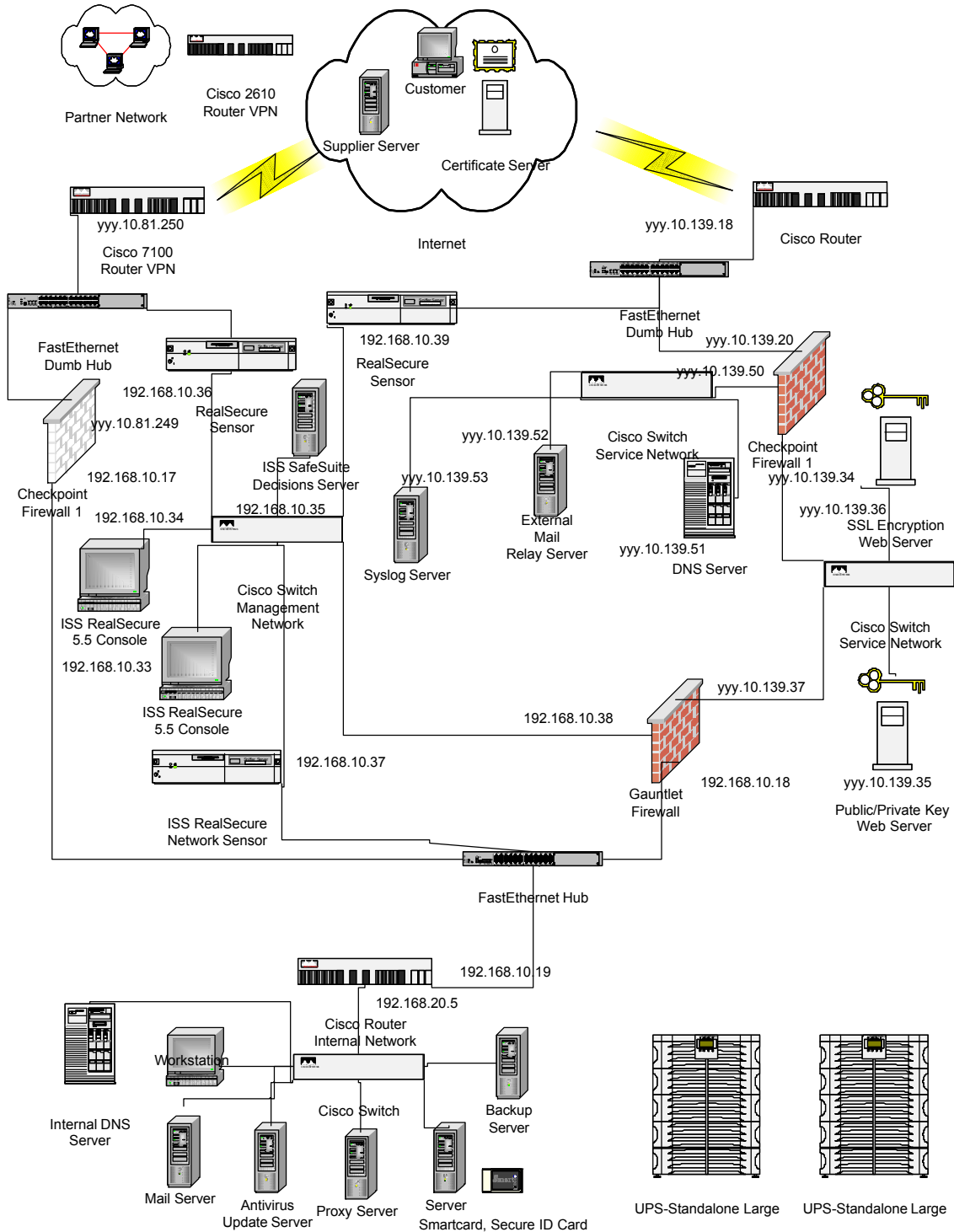
Windows NT/2000, Linux and several varieties of Unix are available with adequate security features. We will choose Windows NT/2000 and will follow configuration guidelines laid out in the SANS "Step by Step" series for Windows NT and the Navy Secure NT Configuration Guide. Windows NT/2000 lacks the scalability of several Unix offerings (and we may regret that later), but our end users are comfortable with that interface and MCSE administrators are more plentiful than their UNIX / Linux counterparts. Since we want to keep the environment as simple as possible we will select our web server, proxy server, mail, database, intrusion detection and firewall products based on the availability of Windows NT/2000 versions. The primary exception to this choice of a single operating system environment will be our routers, which will have the Cisco IOS. We will utilize fully switched 10/100 ethernet products from Cisco to build our internal network and minimize our susceptibility to "sniffers". We will build our e-Commerce web servers on an Oracle Application Server running SSL with 128 bit encryption. Customers will make SSL connections (server side encryption) to the web server for the exchange of sensitive private data. Suppliers will make PKI SSL based connections to a separate server. All queries and transactions to the database from un-trusted sources (customers and suppliers) will be routed to the internal Oracle Database through a Proxy Server using reverse proxy. This will "hide" our internal database from the outside.

Our GIAC Enterprise Security Architecture Diagram can be broken into several distinct areas of security considerations.

1. The internal network, which must be protected from outside threats.
2. A "trusted" Corporate Partner Network. We used "trusted" as a business term. We see that our network is only as secure as it's weakest link. The local network must be protected from intentional or unintentional security risks from "trusted" networks.
3. Service networks which must allow access to customers and suppliers as well as other Internet users.
4. The "un-trusted" Internet.

© SANS Institute 2000 - 2002

GIAC Enterprises Security Architecture Diagram



Running through VISA's requirements we find:

1. Install and maintain a working firewall to protect data accessible via the Internet.

- * Cisco 7100 series border routers running IOS 12.0 with ACLs implemented for the following:
 - * Ingress filtering
 - a. Deny packets with private IP addresses (RFC 1918)
 - b. Deny packets with localhost, broadcast, and multicast addresses
 - c. Deny packets without IP addresses
 - d. Deny packets appearing to come from your internal addresses
 - e. Permit everything else
 - * Egress filtering
 - a. Permit only packets from legal internal IP addresses to be sent out through the router
 - b. Establish a network to network IPSec VPN to Partner Network.
 - * Allow only ICMP traffic that is deemed necessary
 - * All other services as outlined in SANS Top Ten Blocking Recommendations
- * Checkpoint Firewall-1 Version 4.1 (also known as 2000) for NT/2000 is deployed on our two external firewall positions running on Dell 6500 servers. These two firewalls screen the two internet connections. One NAI Gauntlet Version 4.2 firewall screens the service networks from the internal network. Checkpoint Firewall-1 is a stateful firewall rather than a proxy firewall like NAI Gauntlet or Axent Raptor which also offer NT products. Checkpoint was chosen because of its Configuration interface and its compatibility with ISS RealSecure IDS rather than a preference to the stateful firewall technology. The NAI Gauntlet firewall is an existing asset. Personal firewalls such as Network ICE BlackICE Defender provides additional defense for all servers.

Intrusion detection systems, both network-based and host-based, have been implemented. The network IDS is comprised of 3 ISS RealSecure 5.5 network sensors for NT/2000 and single SNORT sensor (NT/2000). The host-based IDS is also RealSecure system sensor for NT/2000. RealSecure was chosen over Axent's Netprowler due to a preference for its interface. Windump and NAI's Sniffer Basic (Net Xray) provide basic packet capture and analysis capabilities.

Maintenance of all of these components includes monitoring of traffic, alerting where feasible, and reporting.

2. Keep security patches up-to-date.

All third party host, network, and application software has been inventoried, and versions of the same have been identified. Various security mailing lists are subscribed to by the company's system administrator / security manager, and are monitored for new vulnerabilities as they are identified.

Daily checks of the following sites are made to ensure GIAC Enterprises stays on top of all security advisories and patches:

<http://www.microsoft.com/technet/security/>
<http://www.cisco.com/warp/public/707/advisory.html>
<http://www.checkpoint.com>
<http://www.iss.net>
<http://www.cert.org>
<http://www.securityfocus.com>

As well as subscriptions to NTBugTraq (see <http://www.ntbugtraq.com>) and BugTraq (see <http://www.securityfocus.com>) mailing lists.

3. *Encrypt stored data accessible from the Internet.*

Corporate security policy states that no critical data will be stored on any server that is exposed to the Internet. A tiered architecture is the standard model for Internet web applications, with a firewall between the web/application servers and the database servers.

4. *Encrypt data sent across networks.*

- * Business-to-business communications are encrypted via Cisco's VPN component or through PKI certificate SSL.
- * Business-to-customer web traffic is encrypted using SSL.
- * Remote access traffic is encrypted by means of the Checkpoint VPN-1 Gateway and the Checkpoint VPN-1 SecureClient.

5. *Use and regularly update anti-virus software.*

Norton AntiVirus is deployed for workstations and servers. When new signatures become available, a process is initiated to pull the signature files down, and they are then distributed to servers and workstations throughout the organization. Norton AntiVirus is also implemented for remote users.

McAfee VirusScan is used in conjunction with Content Technology's MailSweeper to scan incoming emails and attachments for viruses as they enter the environment, before they are delivered to the user's mailbox.

6. *Restrict access to data by business "need to know".*

Corporate security policy states that access to data will be authorized on a "need to know" basis. Approval by the data owner is required for access authorization. Access to applications and data is based upon the user's role(s) within the organization. Access to sensitive data (payroll, sales, customer information, etc.) is audited, and the data owners review the audit reports for compliance.

Internet access is also restricted by policy, and is to be used for business purposes only.

Split DNS structure. External DNS server resolves queries for the few hosts in the screened network only. Internal DNS server resolves internal queries only. A version of Bind ported to NT/2000 will be used rather than the native Microsoft DNS service.

7. *Assign unique IDs to each person with computer access to data.*

Corporate security policy states that each employee is issued a unique ID with the level of access that his/her job requires, and that he/she is responsible for all activity while that ID is logged on to any system. Shared IDs are not acceptable and will not be issued. Third parties with access to extranet applications (vendors, partners, etc.) are issued unique IDs as well. These third parties are required to sign a legal access agreement before the IDs are issued.

Privileged system accounts, such as root, are not allowed direct login. The user must login with

his/her own account and switch user to the privileged account, based upon an access list of authorized users.

Password management guidelines are as follows:

- * Idle accounts expire after 30 days of inactivity
- * Account locks after 3 invalid password attempts
- * Password expiration interval of 30 days
- * Password history of 6 passwords

8. Track access to data by unique ID.

Tracking access to data by unique ID is accomplished by both application and system logs. System logs for servers residing in the screened network are consolidated on a protected log server. Server times are synchronized in order to facilitate the research of suspicious incidents.

9. Don't use vendor-supplied defaults for system passwords and other security parameters.

A standard baseline for securely configuring all devices and applications has been developed and is maintained and implemented by the responsible team. Default passwords are changed, and any unnecessary default accounts are either removed or disabled. Sample scripts and programs are removed. Default parameters are modified to reflect the organization's security policy. Windows NT/2000 is configured to comply with SANS and Navy Secure configuration guidelines. The Oracle database is tested by ISS Database Scanner for Oracle.

As previously stated, we're primarily using an NT environment and following the SANS guide. We've implemented the passfilt.dll from SP6a. After making a change to the NT registry to include the passfilt.dll, the following password policy is implemented:

- Passwords may not contain your user name or any part of your full name.
- Passwords must be at least eight characters long.
- Passwords must contain elements from three of the four following types of characters:

Character types	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized arabic numerals	0, 1, 2, ... 9
Non-alphanumeric characters (special characters)	!, %, ^

10. Regularly test security systems and processes.

This requirement is discussed in greater detail in Assignment 3. But the corporate Internal Audit team conducts periodic audits of applications and operating system security. Network-based audits are scheduled quarterly using tools such as nmapNT, ISS Internet Scanner, Axent's NetRecon, Foundstone's Superscan, Netcat, Fragrouter and Nessus. Database vulnerability scanning will be accomplished through ISS Database Scanner (for Oracle). CGI vulnerability scanners like Rain Forrest Puppy's Whisker and Rhino9's Grinder are used to test web applications. Enumeration tools like Legion, NAT and Dumpsec will be used. Axent's Enterprise Security Manager (ESM) will monitor security policy compliance on all servers. Password cracking programs such as L0phtCrack, Pwdump2, Pwdump, Revelation, Sid2user, User2sid and John the Ripper are run periodically to test compliance with password policies. Audits of our perimeter security and external web applications are also performed annually by contracted third parties to validate findings of our internal audits. All tests will be conducted with the following objectives.

Firewall Audit. This audit will verify whether the network has a functional firewall in place to protect data from the internet and any network that should not be able to reach resources on that network.

Security Status Audit. This Audit will verify if the current security status of information resources is maintained. This includes the OS and patch status for all systems, network or desktop, in the corporation.

Data Encryption Audit. This audit will verify whether or not all data accessible from the internet is encrypted. The only exception to this should be information of freely accessible public resources (i.e. external DNS, public website, etc.).

Encrypted Data Transfer Audit. This audit will verify that any data sent across networks is encrypted. This applies to any network where systems that exist on that network may not have a need to know for that information.

Anti-Virus Audit. This audit will ensure that anti-virus software is employed throughout the organization and that it is kept up to date. The status of these updates should be recorded.

Data Access Audit. This audit will verify that, for each resource available to users, only users with a business need to know have access to that resource.

User Identification Audit. This audit will verify that every user of corporate resources has a unique log on to access those resources. This will also verify that the users are following guidance in the security policy with regard to password security.

Data Manipulation Audit. The purpose of this audit is to ensure that data contained in corporate resources is tracked. As data is manipulated, it should be known which user did what.

Configuration Audit. This audit will verify that the corporation makes use of standard configurations. These configurations should be in keeping with the security policy and should improve the security of the systems from the installation defaults.

© SANS Institute

Assignment 2 Submission: Security Policy

Based on the security architecture that you defined in Assignment 1, provide a security policy for at least the following three components: Border Router, Primary Firewall and VPN. You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.

Defense In Depth

Defense in Depth is a layered approach to security, so that if one layer fails, another will be there to back us up. These layers may include leveraging border routers for defense, extra internal routers, multiple firewalls (possibly from different vendors) and host based protection. Since we know what services our network uses, it's a good idea as a part of Defense in Depth, to shutdown any services that aren't needed that may be running on internal hosts, and to securely configure and patch services that are needed. That way, even if traffic gets through, it won't be able to affect anything! "Personal" firewalls can be loaded on mission critical hosts. Anti-virus software should be loaded on all internal systems, and a strong password policy is essential. Another very important step is to setup some type of intrusion detection system to monitor anomalies, and verify that there isn't anything getting through that shouldn't be getting through. Monitoring helps protect beyond attacks we currently know, and collects evidence in the case of an attack. If these methods don't prevent an attack, they should at least slow the attacker down, and give you a means to document their actions, and track them down.

It is important to know what might be vulnerable. SANS lists the most commonly probed and attacked ports.

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
2. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
3. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
4. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 -- earlier ports plus 445(tcp and udp)
5. X Windows -- 6000/tcp through 6255/tcp
6. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
7. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
8. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
9. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
10. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
11. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

We will make it our policy to eliminate many but not all of these protocols. Some will still be required to conduct business.

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

Border Router Filtering with Cisco IOS

Before going into detail on the syntax of Cisco access-lists, it is necessary to discuss how Cisco routers are configured. Cisco routers can be configured one of several ways. First, they can be configured through a serial connection to the console port on the back of the router. This can be done directly, or by using a modem. While using a modem allows the convenience of remote access, it also opens another security hole in your network. A router can also be directly configured through a telnet client package. Simply run one of the telnet clients that comes with your operating system of choice, and connect to the router by its ip address. Cisco telnet does allow extra passwording, but unless correctly protected, the router's configuration can be made available to anyone on the Internet! Finally the newest versions of Cisco IOS support a web configuration client, however, for maximum security this should be disabled. For an article from Cisco on "hardening" your router's access security, see <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm>. For more documentation on Cisco router commands and configuration, try <http://www.cisco.com/pcgi-bin/ibld/all.pl?i=support&c=2&m=GUEST>. For further information on blocking the top ten ports on a Cisco router, please refer to <http://pasadena.net/cisco/secure.html> and http://www.sans.org/infosecFAQ/blocking_cisco.htm. A discussion of the importance to the community of egress filtering can be found at <http://www.sans.org/y2k/egress.htm>. Try <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm> for an entire Cisco IOS 12 command reference!).

We'll run through several of the IOS commands used and give a brief explanation.

```
service password-encryption
```

```
enable secret xxxxxxx
```

This configures the enable password to "xxxxxxx". Because "enable secret" is used, the password will be encrypted using the MD5 hash. This is more secure and preferred to the default password encryption.

```
service timestamps debug datetime
```

```
service timestamps log datetime
```

This configures the logs to be time stamped. By default they are not time stamped. Time stamps will be important for reconstruction during incident handling.

```
no service finger
```

```
no ip bootp server
```

```
no service tcp-small-servers
```

```
no service udp-small-servers
```

This set of commands disables access to several minor TCP and UDP services such as finger, bootp, echo, chargen, discard, and daytime. These services are not needed for operation and are disabled to ensure any security hole in them is blocked.

```
no ip source-route
```

This prevents the use of source routes. Source routing is not desired because we do not want traffic to have its path dictated by an unfriendly entity.

```
no cdp run
```

```
no ip http server
```

This disables the CDP protocol and prevents http configuration.

```
no ip domain-lookup
```

This disables the IP Domain Naming System-based host name-to-address translation.

```
no ip directed-broadcast
```

This ensures that all IP directed broadcasts are dropped. This helps to avoid DOS attacks.

```
Ip access-group 101 in
```

Applies the access list #101 to the interface.

```
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
```

```
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
```

```

access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip any 10.0.0.0 0.255.255.255 log
access-list 101 deny ip any 172.16.0.0 0.15.255.255 log
access-list 101 deny ip any 192.168.0.0 0.0.255.255 log

```

These lines deny traffic trying to use an RFC 1918 address.

```

access-list 101 deny ip <your internal network> <your netmask> log

```

This line denies spoofed internal addresses

```

crypto isakmp policy 1

```

Policy 1 identifies unique VPN

```

authentication pre-share
crypto isakmp key ipsec13 address xxx.xxx.xxx.xxx

```

Define our key and the external IP address of the router on the other end of our VPN

```

crypto ipsec transform-set tran13 esp-des esp-md5-hmac

```

Enable encapsulation and name this combination of protocols tran 13.

```

crypto map vpn13 10 ipsec-isakmp
set peer xxx.xxx.xxx.xxx
set transform-set tran13

```

Peer defines the external IP address of the remote router.

```

match address 113

```

These lines set up the IPSec VPN

Border Router & Partner VPN Configuration

Building configuration...

Current configuration:

```

!
version 12.0
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
no service udp-small-servers
no service tcp-small-servers
no service finger
no ip source route
!
hostname vpn3
!
logging buffered 50000 debugging
logging host inside 199.10.139.53
enable secret 5 $1$A0nL$3gkoXG1SI1BGMuKDArW6t/
enable password 7 105D1E1C1615171B58
!
username rblack password 7 0314521F075B204042
!
memory-size iomem 8
ip subnet-zero
no ip domain-lookup
!

```



```

cns event-service server
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key ipsec13 address yyy.133.5.116 255.255.255.255
!
crypto ipsec transform-set tran13 esp-des esp-md5-hmac
!
crypto map vpn13 10 ipsec-isakmp
 set peer yyy.133.5.116
 set transform-set tran13
 match address 113
!
interface Ethernet0/0
 ip address yyy.10.81.250 255.255.255.252
 ip access-group 112 in
 no ip directed-broadcast
 no ip redirects
 no ip unreachable
 no snmp
!
interface Ethernet0/1
 no ip address
 ip access-group 112 in
 no ip directed-broadcast
 no ip redirects
 no ip unreachable
 no snmp

interface Serial0/0
 description 1544kb serial link to ISP
 ip address yyy.10.81.5 255.255.255.252
 ip access-group 111 in
 no ip directed-broadcast
 no ip redirects
 no ip unreachable
 no snmp
 crypto map vpn13
 bandwidth 1536
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 199.10.139.64 255.255.255.0 199.10.81.249
no ip http server
!
access-list 113 permit ip yyy.10.81.249 0.0.0.0 yyy.133.5.0 0.0.0.255
access-list 113 permit ip yyy.10.139.0 0.0.0.255 yyy.133.5.0 0.0.0.255
!
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log

```

```

access-list 111 deny ip 172.16.0.0 0.31.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 224.0.0.0 0.255.255.255 any log
access-list 111 deny ip 248.0.0.0 0.255.255.255 any log
access-list 111 deny ip 192.0.2.0 0.0.0.255 any log
access-list 111 deny ip 169.254.0.0 0.0.255.255 any log
access-list 111 deny ip host 255.255.255.255 any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip host yyy.10.81.249 255.255.255.255 any log
access-list 111 deny ip host yyy.10.139.0 255.255.255.0 any log
access-list 111 permit icmp yyy.10.81.249 255.255.255.255 any echo-request
access-list 111 permit icmp yyy.10.139.0 255.255.255.255 any echo-request
access-list 111 deny icmp any any echo-request log
access-list 111 deny tcp any any eq 139 log
access-list 111 deny tcp any any telnet log
access-list 111 deny tcp any any range exec cmd log
access-list 111 permit ip any any
!
access-list 112 deny ip 10.0.0.0 0.255.255.255 any
access-list 112 deny ip 127.0.0.0 0.255.255.255 any
access-list 112 deny ip 172.16.0.0 0.31.255.255 any
access-list 112 deny ip 192.168.0.0 0.0.255.255 any
access-list 112 deny ip 224.0.0.0 0.255.255.255 any
access-list 112 deny ip 248.0.0.0 0.255.255.255 any
access-list 112 deny ip 192.0.2.0 0.0.0.255 any
access-list 112 deny ip 169.254.0.0 0.0.255.255 any
access-list 112 deny ip host 255.255.255.255 any
access-list 112 deny ip host 0.0.0.0 any
access-list 112 permit icmp yyy.10.81.249 255.255.255.255 any echo-request
access-list 112 permit icmp yyy.10.139.0 255.255.255.255 any echo-request
access-list 112 deny icmp any any echo-request log
access-list 112 permit ip any any

```

banner motd ^CC

```

-----<    GIAC Enterprises    >-----

```

THIS IS A GIAC ENTERPRISE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED USE. GIAC COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

-----< For Official Use Only >-----

^C

!

line con 0

login local

transport input none

line aux 0

line vty 0 4

login local

!

end

vpn3#

Border Router 2

Building configuration...

Current configuration:

!

version 12.0

service timestamps debug datetime

service timestamps log datetime

service password-encryption

!

no service udp-small-servers

no service tcp-small-servers

no service finger

no ip source route

!

hostname ecommerce

!

logging buffered 50000 debugging

logging host inside 199.10.139.53

enable secret 5 \$1\$A0nL\$3gkoXG1SI1BGMuKDArW6t/

enable password 7 105D1E1C1615171B58

!

username rblack password 7 0314521F075B204042

!

memory-size iomem 8

ip subnet-zero

no ip domain-lookup

!

cns event-service server

!

interface Ethernet0/0

ip address yyy.10.139.18 255.255.255.240

ip access-group 112 in

no ip directed-broadcast

```

no ip redirects
no ip unreachable
no snmp
!
interface Ethernet0/1
no ip address
ip access-group 112 in
no ip directed-broadcast
no ip redirects
no ip unreachable
no snmp

interface Serial0/0
description 1544kb serial link to ISP
ip address yyy.10.138.18 255.255.255.252
ip access-group 111 in
no ip directed-broadcast
no ip redirects
no ip unreachable
no snmp
bandwidth 1536
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 199.10.139.0 255.255.255.0 199.10.139.20
no ip http server
!
!
access-list 111 deny ip 10.0.0.0 0.255.255.255 any log
access-list 111 deny ip 127.0.0.0 0.255.255.255 any log
access-list 111 deny ip 172.16.0.0 0.31.255.255 any log
access-list 111 deny ip 192.168.0.0 0.0.255.255 any log
access-list 111 deny ip 224.0.0.0 0.255.255.255 any log
access-list 111 deny ip 248.0.0.0 0.255.255.255 any log
access-list 111 deny ip 192.0.2.0 0.0.0.255 any log
access-list 111 deny ip 169.254.0.0 0.0.255.255 any log
access-list 111 deny ip host 255.255.255.255 any log
access-list 111 deny ip host 0.0.0.0 any log
access-list 111 deny ip host yyy.10.139.0 255.255.255.0 any log
access-list 111 permit icmp yyy.10.139.0 255.255.255.255 any echo-request
access-list 111 deny icmp any any echo-request log
access-list 111 deny tcp any any eq 139 log
access-list 111 deny tcp any any telnet log
access-list 111 deny tcp any any range exec cmd log
access-list 111 permit ip any any
!
access-list 112 deny ip 10.0.0.0 0.255.255.255 any
access-list 112 deny ip 127.0.0.0 0.255.255.255 any
access-list 112 deny ip 172.16.0.0 0.31.255.255 any
access-list 112 deny ip 192.168.0.0 0.0.255.255 any

```

```

access-list 112 deny ip 224.0.0.0 0.255.255.255 any
access-list 112 deny ip 248.0.0.0 0.255.255.255 any
access-list 112 deny ip 192.0.2.0 0.0.0.255 any
access-list 112 deny ip 169.254.0.0 0.0.255.255 any
access-list 112 deny ip host 255.255.255.255 any
access-list 112 deny ip host 0.0.0.0 any
access-list 112 permit icmp yyy.10.139.0 255.255.255.255 any echo-request
access-list 112 deny icmp any any echo-request log
access-list 112 permit ip any any

```

```
banner motd ^CC
```

```
-----<    GIAC Enterprises    >-----
```

THIS IS A GIAC ENTERPRISE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED USE. GIAC COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

```
-----<    For Official Use Only    >-----
```

```
^C
```

```
!
```

```
line con 0
```

```
login local
```

```
transport input none
```

```
line aux 0
```

```
line vty 0 4
```

```
login local
```

```
!
```

```
end
```

```
ecommerce#
```

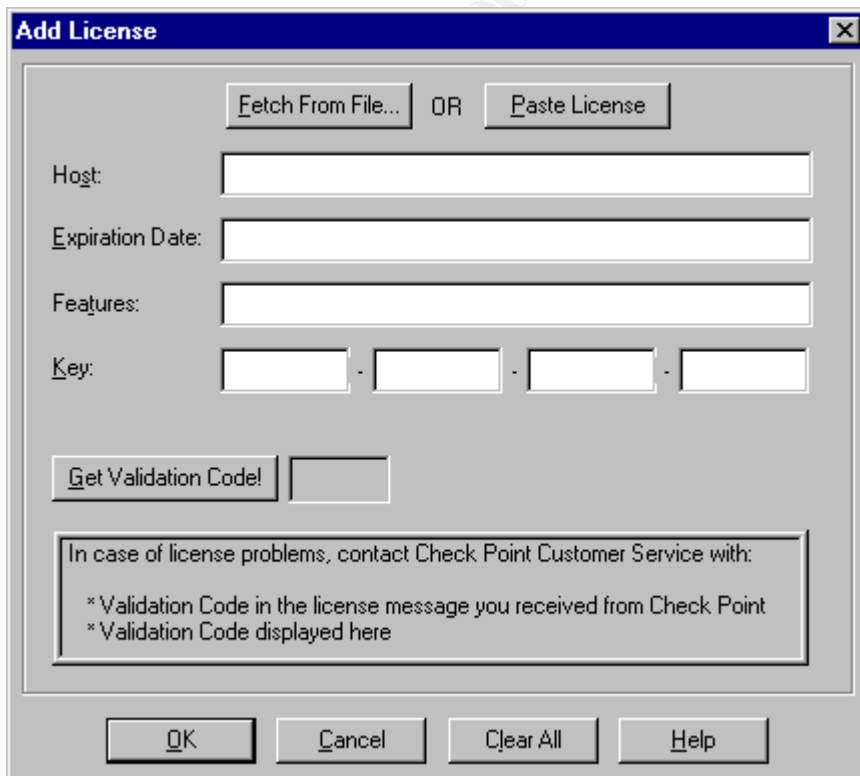
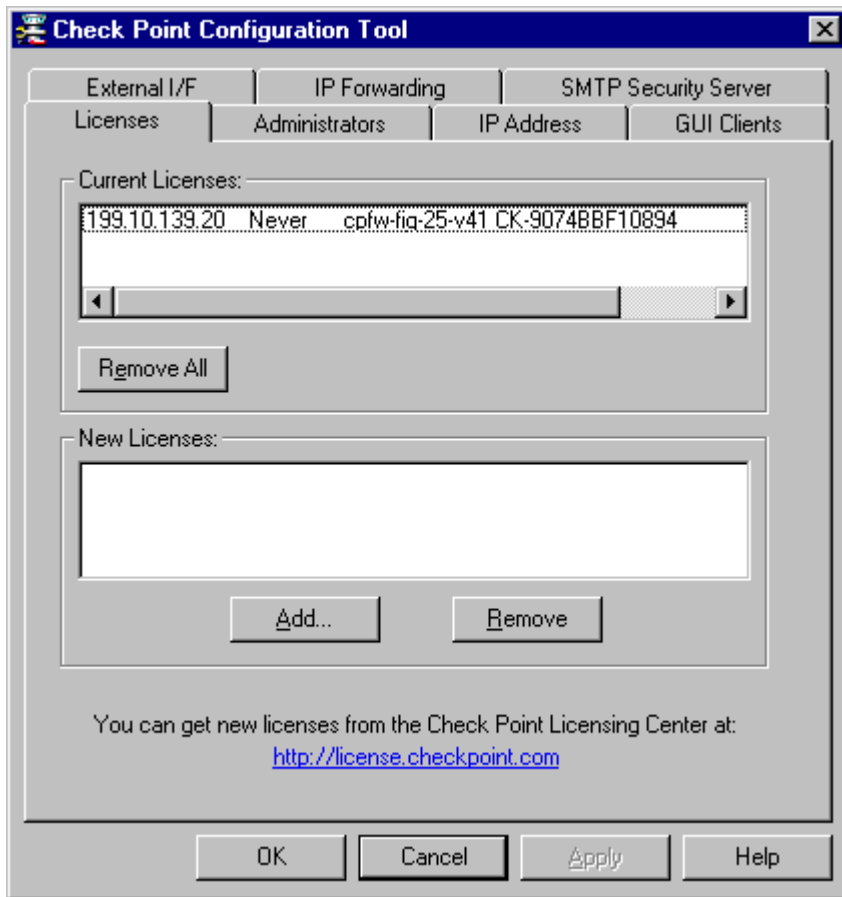
Internet / Service Network Firewall

As previously indicated, we've chosen to implement our Checkpoint Firewall-1 4.1 on a MS Windows NT 4.0 SP 6a platform. In addition to following the SANS Windows NT Security Step by Step guidelines, we've also referenced a whitepaper [Beginners Guide to Armoring NT 4.0](http://www.enteract.com/~lspitz/papers.html) by Lance Spitzer, at <http://www.enteract.com/~lspitz/papers.html>. For those who might choose Linux or Solaris platforms to implement a firewall, Lance also offers whitepapers on armoring those platforms. In fact Lance offers a series of whitepapers on Firewall-1. But for now we're concentrating on preparing the NT platform. We do not remove Server and Workstation from Services as Lance suggests, preferring to keep the AT command capabilities as Chris Brenton

prefers. The Server and Workstation services were retained to preserve the functionality these services provide. These two services were protected by blocking NBT, unbinding WINS, and by removing the ability for anyone to logon from the network. We've implemented static routes through the use of the ip route command. Some other things that we've done to our NT box includes the following

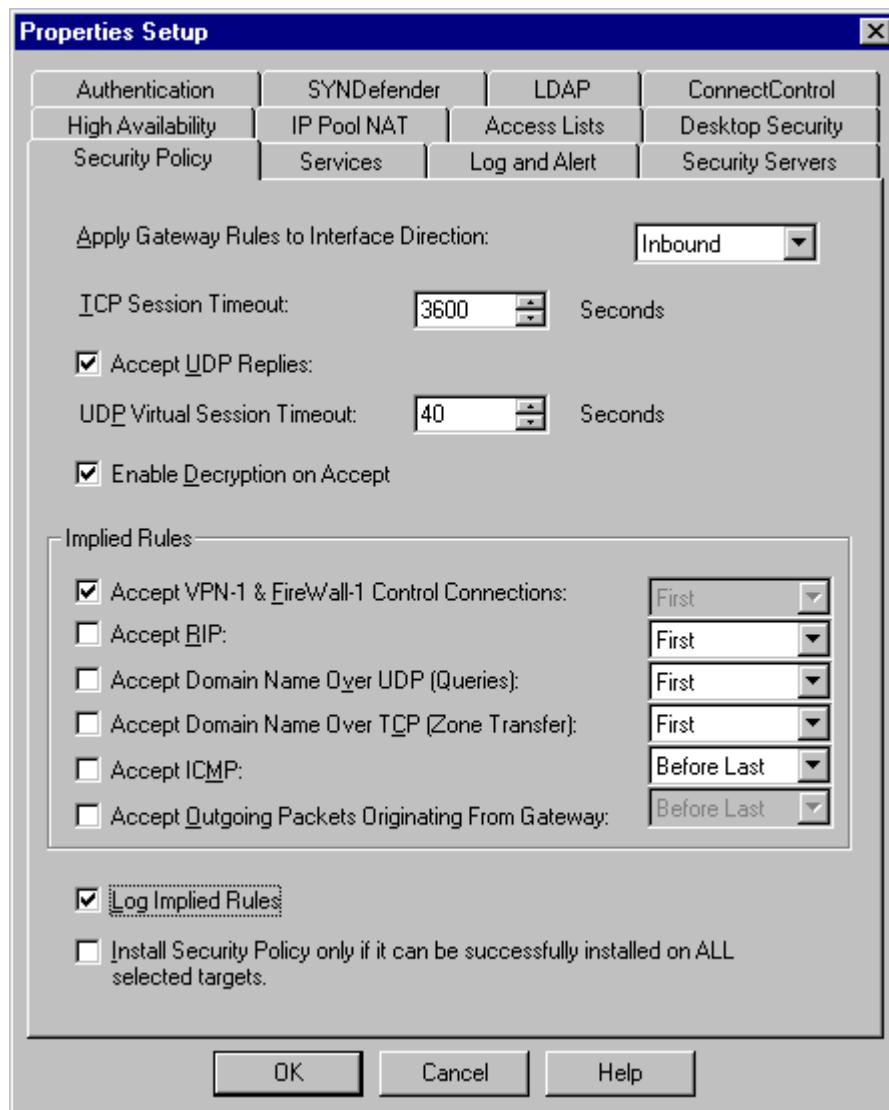
- 1) The C2 configuration tool from the resource kit was used to add a logon-warning message and to remove the OS2 and POSIX subsystems.
- 2) The passprop utility from the resource kit was used to force complex passwords and to allow the administrator account to be locked out if attacked.
- 3) The anonymous user's access to the registry was restricted:
HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous
- 4) Remote access to the registry was restricted:
HKLM\System\CurrentControlSet\Control\SecurePipeServers\WinReg
- 5) 8.3 naming was disabled using the registry key:
HKLM\System\CurrentControlSet\FileSystem\NtfsDisable8dot3NameCreation
- 6) Access to scheduler restricted:
HKLM\System\CurrentControlSet\Control\LSA\SubmitControl
- 7) Cached Logons were disabled:
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\CachedLogonsCount
- 8) LM authentication was disabled:
HKLM\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel
- 9) IP Source routing disabled:
HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\DisableIPSourceRouting
- 10) Base Objects were placed in protected mode:
HKLM\System\CurrentControlSet\Control\SessionManager\ProtectionMode
- 11) Administrative shares were removed:
HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\AutoShareServer
- 12) Null session access disabled:
HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessionAccess
- 13) Null session shares disabled:
HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares

Next we install Firewall-1 version 4.1 and apply the appropriate service packs. The current service pack is SP3. We restart the system and now we are ready to begin. We can find the latest information at <http://www.checkpoint.com/techsupport/index.html>. Using Configuration Manager, we define the interfaces, add our administrators and add the license key.

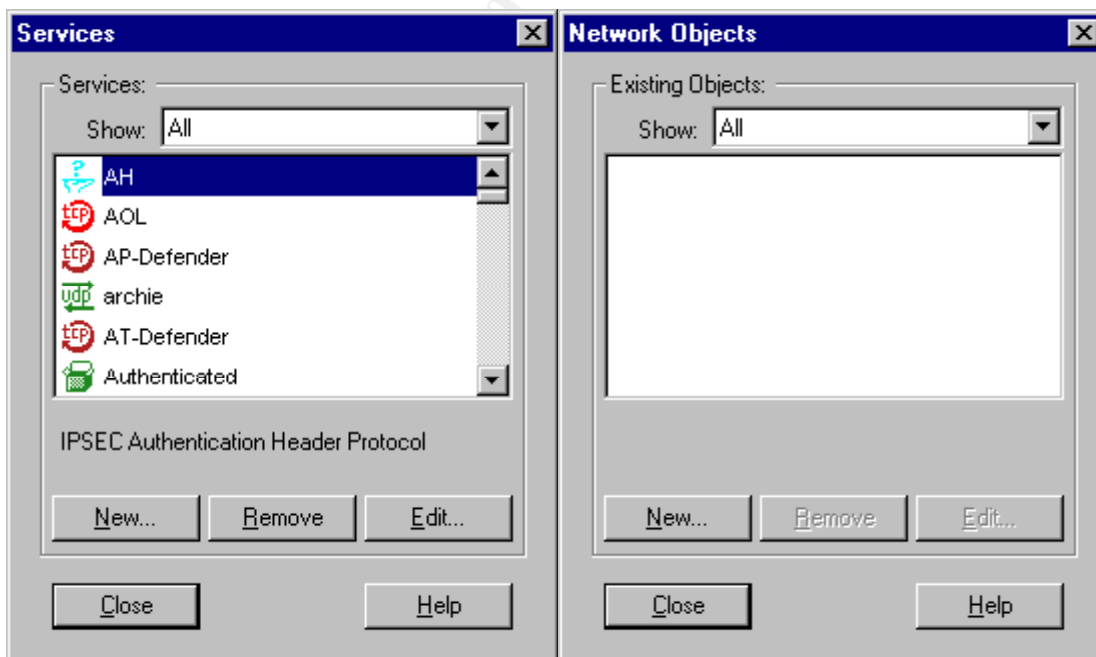
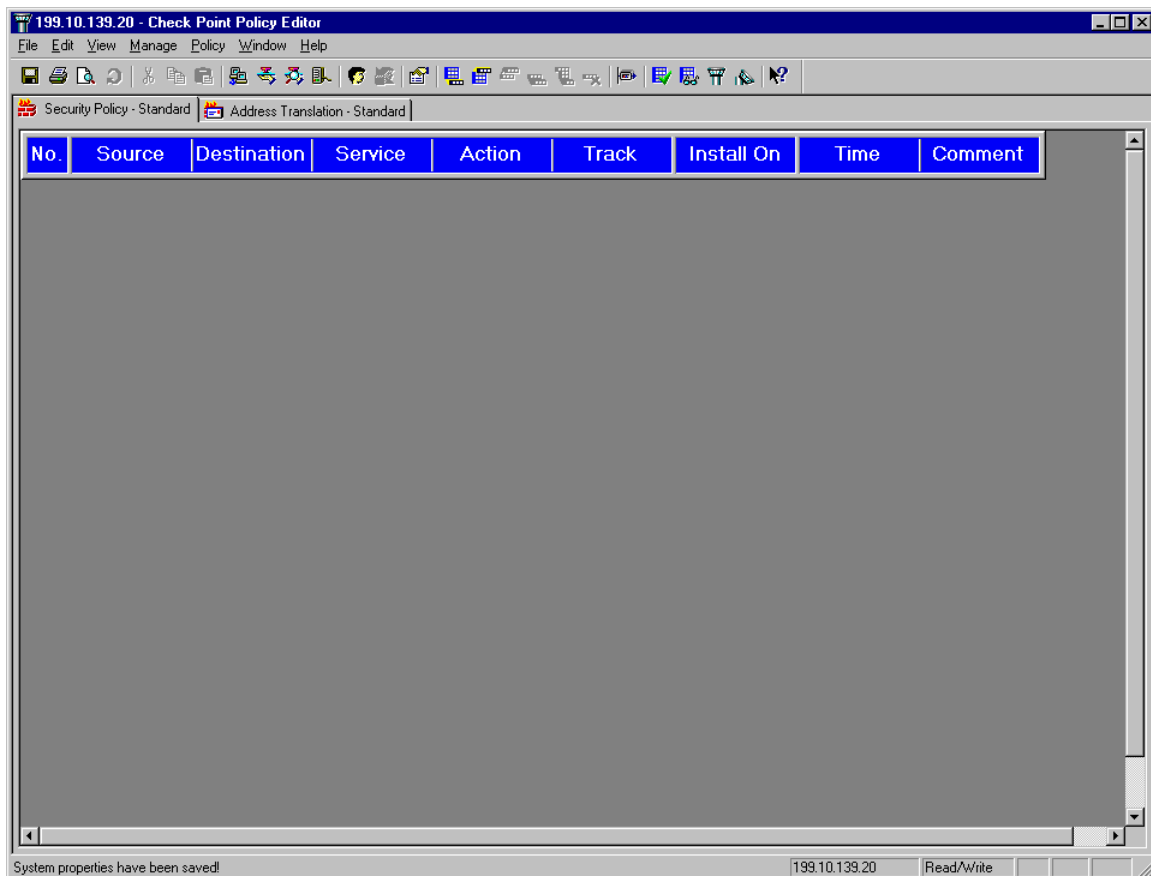


Now we are ready to set up the rulebase.

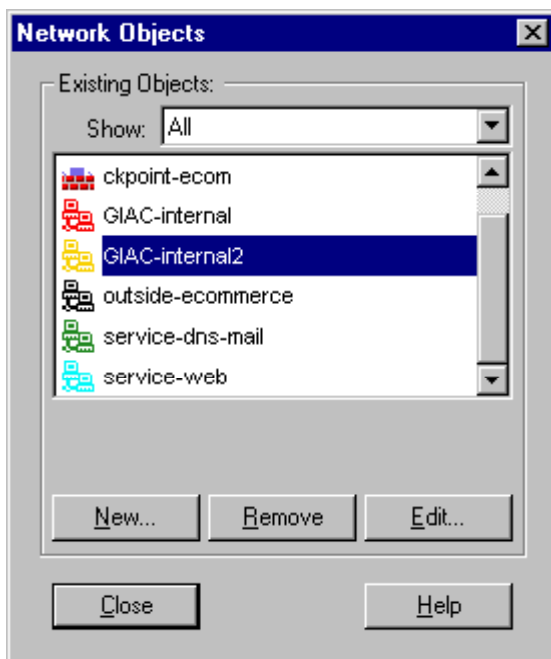
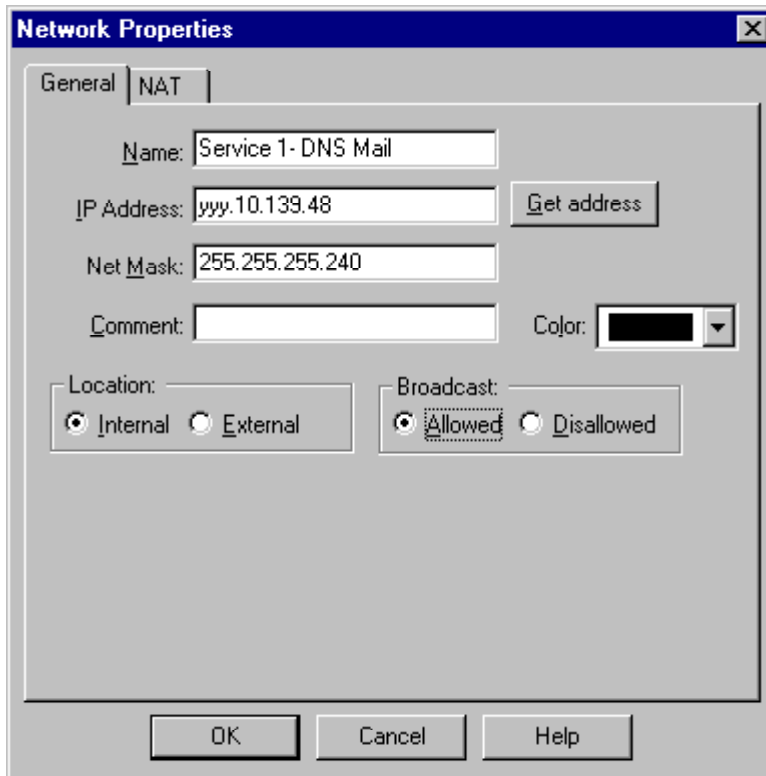
The first step in setting up a secure rulebase on the Checkpoint Firewall-1 4.1 firewall is to review the default properties page and turn off the default properties. If it's found that any of these properties are actually required, it is recommended to turn them back on in the firewall rulebase. For more details, please see an excellent whitepaper, Building Your Firewall Rulebase by Lance Spitzer, at <http://www.enteract.com/~lspitz/rules.html>.



As with any packet filtering device, rule order within the Firewall-1 policy is critical. When a packet is received, the firewall compares it against the rulebase and when it finds the first rule that matches, it applies that rule. Therefore it is important to keep the more specific rules first and the more general rules last. Rules are ordered by firewall-related rules first, screened network rules next, and finally internal rules. An exception to this ordering is the rule for both internal and external access to the webserver. Even though this is a general rule, because it will be accessed frequently, it appears towards the top after the firewall-related rules. Technical Incursion Countermeasures, at <http://www.ticm.com> also offers a great deal of information on Checkpoint and establishing your rulebase. See <http://www.ticm.com/info/insider/members/fwsecfaq/index.html>.



As you can see in the screenshots above, Services are populated while Network Objects and Security Policy is not. We'll begin by defining our network objects.



Now we finished populating our Network Objects, we can begin to define our Security Policy and rulebase. The next two screen shots show the resulting rulebase. Internal network users will not be using this internet connection to access external resources. The internal traffic is oriented to managing devices and allowing internal mail and database servers to exchange traffic with the external mail relay and the web servers respectively. The service networks themselves have restricted access to outgoing internet traffic.

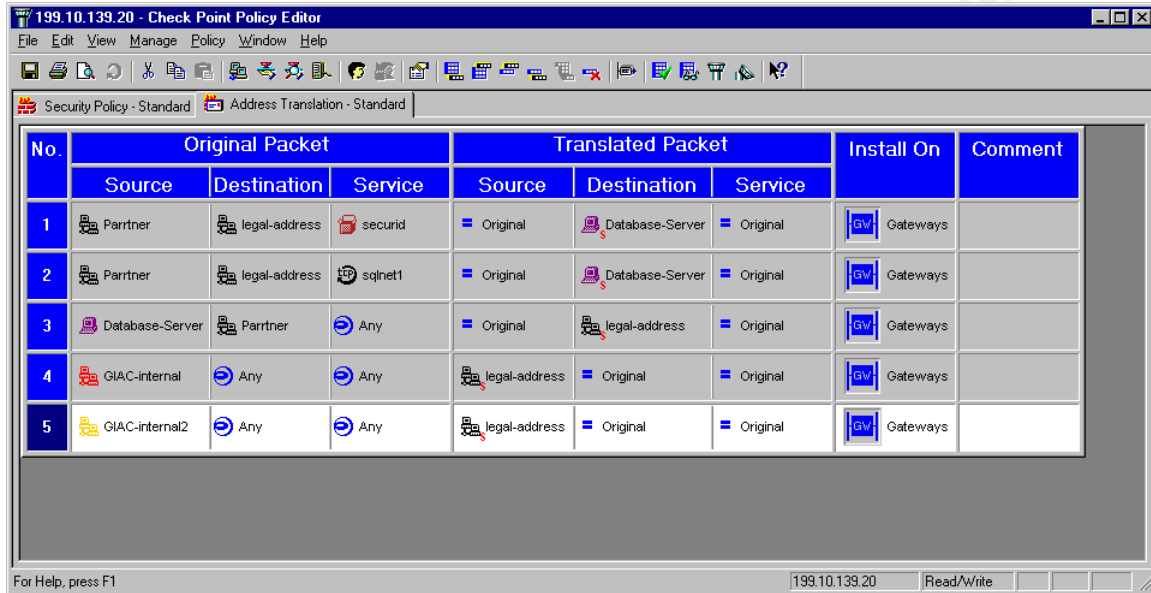
199.10.139.20 - Check Point Policy Editor							
File Edit View Manage Policy Window Help							
Security Policy - Standard Address Translation - Standard							
No.	Source	Destination	Service	Action	Track	Install On	Time
1	Firewall-Admin	ckpoint-ecom	FireWall1 time RealSecure	accept	Long	Gateways	Any
2	Any	service-dns-mail	smtp domain-udp	accept	Long	Gateways	Any
3	Any	service-web	https http Entrust-KeyMgmt ftp	accept	Long	Gateways	Any
4	e-commerce-border VPN-border-router	service-dns-mail	syslog	accept	Short	Gateways	Any
5	GIAC-internal GIAC-internal2 Gauntlet-FW-Internal	service-web	https sqlnet1 sqlnet2 echo ISS-Realsecure time	accept	Long	Gateways	Any
6	GIAC-internal GIAC-internal2 Gauntlet-FW-Internal	service-dns-mail	MSEExchange MSEExchange-RemoteAdmin MSEExchange-SiteConnector ISS-Realsecure echo time	accept	Long	Gateways	Any
7	service-dns-mail service-web	Any	echo ftp https http dns ISS-Realsecure MSEExchange smtp sqlnet2 Entrust-KeyMgmt	accept	Long	Gateways	Any

199.10.139.20 - Check Point Policy Editor							
File Edit View Manage Policy Window Help							
Security Policy - Standard Address Translation - Standard							
			MSEExchange smtp sqlnet2 Entrust-KeyMgmt				
8	Firewall-Admin	e-commerce-border	telnet	accept	Long	Gateways	Any
9	outside-e-commerce	GIAC-internal GIAC-internal2	Any	drop	Alert	Gateways	Any
10	Any	ckpoint-ecom	NBT ident	reject		Gateways	Any
11	Any	ckpoint-ecom	Any	drop	Long	Gateways	Any
12	Any	Any	Any	drop	Long	Gateways	Any

Our internal Gauntlet firewall and internal router ensure that our internal users direct their DNS queries to the internal DNS server. Nothing originating from the internet should reach our internal network directly. Only HTTP, HTTPS, and FTP should ever reach our web servers from the outside world. Only SMTP and UDP DNS Queries should reach that service network. All other traffic originating from the internet should

be dropped at the outside interface of the firewall.

Next we'll address our VPN Checkpoint Firewall-1 where we'll establish remote access VPN capabilities using Checkpoint's Secure Remote and Firewall-1's VPN capabilities. Our Partner VPN has already been established through the Cisco router. The traffic from our partner appears in unencrypted form before it gets to our firewall where it is inspected by our ISS RealSecure Network Sensor. We'll establish our Network Address Translation (NAT) capabilities on this Checkpoint Firewall-1.



The screenshot shows the 'Check Point Policy Editor' window for '199.10.139.20'. The 'Address Translation - Standard' tab is active, displaying a table with 5 rows of NAT rules. The table has columns for 'No.', 'Original Packet' (Source, Destination, Service), 'Translated Packet' (Source, Destination, Service), 'Install On', and 'Comment'. The rules are as follows:

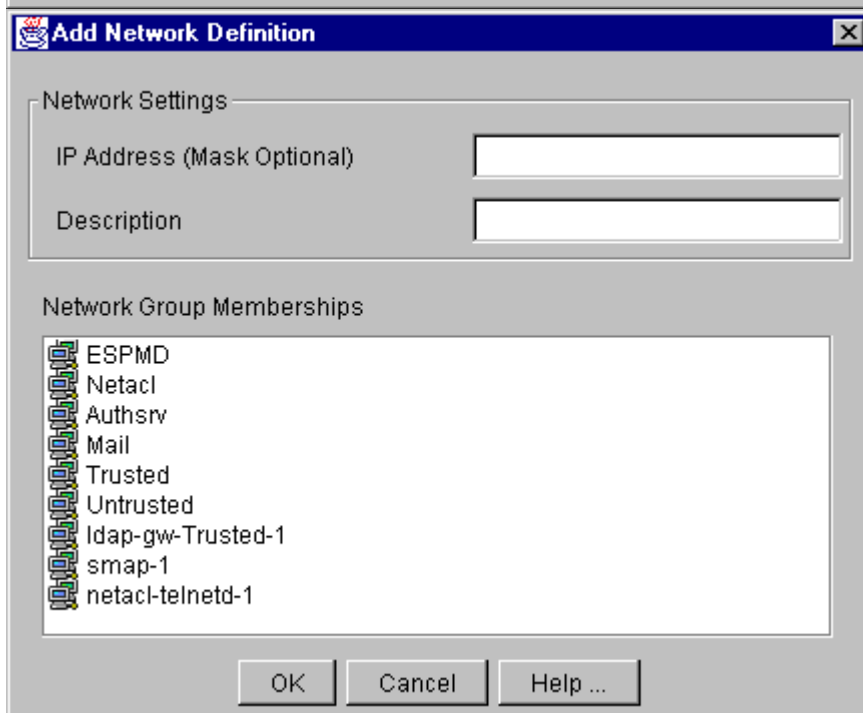
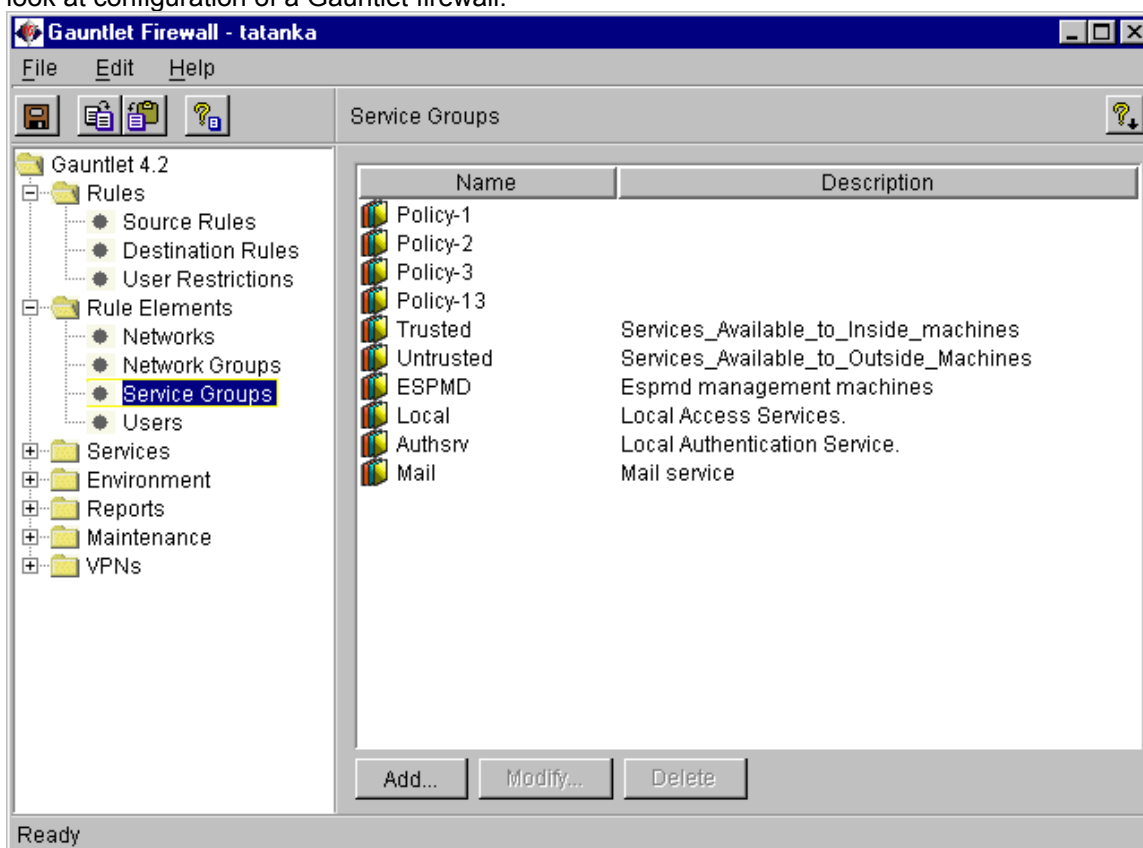
No.	Source	Destination	Service	Source	Destination	Service	Install On	Comment
1	Partner	legal-address	secuid	Original	Database-Server	Original	Gateways	
2	Partner	legal-address	sqlnet1	Original	Database-Server	Original	Gateways	
3	Database-Server	Partner	Any	Original	legal-address	Original	Gateways	
4	GIAC-internal	Any	Any	legal-address	Original	Original	Gateways	
5	GIAC-internal2	Any	Any	legal-address	Original	Original	Gateways	

We've added our address translation so our partners can access our database server and so our internal users can access the internet.

We will also have a screenshot to demonstrate how to set up a VPN on Checkpoint Firewall-1. Our GAIC Security Architecture currently doesn't employ this particular VPN setup and is included for demonstration purposes only. The screenshot on the next page represents a Firewall-1 to Firewall-1 VPN. Encryption domains are established on each end. The IPSEC encryption key is preshared just as with the Cisco VPN. With that we've finished with our discussion of Checkpoint.



Now we've finished with our Checkpoint Firewall-1 configuration and now we'll move on to a brief look at configuration of a Gauntlet firewall.



Add Network Group

Network Group Settings

Network Group Name:

Description:

Available List

☐ Networks

☒ Other Network Groups

Available Members

- ESPM
- Netac
- Authsv
- Mail
- Trusted
- Untrusted
- ldap-gw-Trusted-1
- smap-1
- netac-telnetd-1

Included Members

>>

<<

OK Cancel Help...

Add Service Group

Service Group Settings

Name:

Description:

Not Included in Group

- authsv
- netac-ftp
- netac-rlogind
- netac-telnetd
- smap
- smap
- pcxdpp
- tn-gw
- rlogin-gw
- ftp-gw
- nntp-gw
- info-gw
- http-gw

Included in Group

>>

<<

Authentication

☐ Enforce Authentication

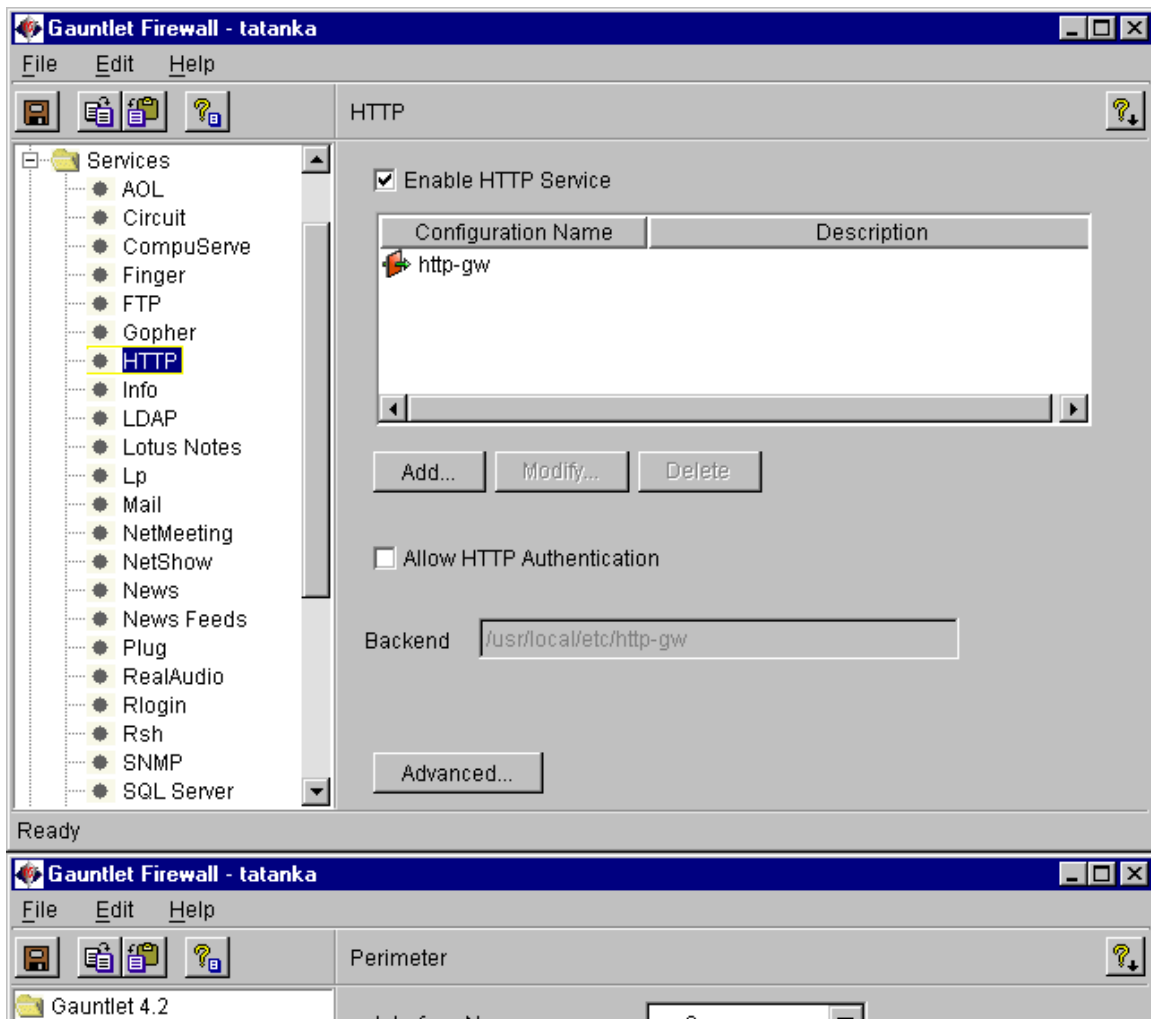
Authserver:

Port:

Allow Password Change?

☐ Permit ☒ Deny

OK Cancel Help...



Add Packet Screening Rule

Base Settings

Description:

Interface: exp2

Protocol Selection

☒ All
☐ Choose From List
☐ Enter Protocol Number

Protocol: exp2

Access Filter

☒ Deny Traffic ☐ Absorb Traffic ☐ Forward Traffic

Source

IP & Mask:

Port Range: To

Destination

IP & Mask:

Port Range: To

OK Cancel Help...

Our purpose here hasn't been to show the actual configuration of our Gauntlet or to provide a tutorial. It has simply been to provide a favor for the configuration of a Gauntlet firewall to contrast against the Checkpoint firewall configuration. However, that's not to say that these screenshot's wouldn't achieve a working firewall. They will. I am now down to the wire (this is due in 3 days) and I have already invested enough time. Now its time to move on to the next assignment.

Assignment 3 Submission: Audit Your Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and Primary Firewall described in Assignment 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Border Router and Primary Firewall are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment, analyze the perimeter defense and make recommendation of improvements or alternate architectures.

In preparing the assessment we want to look for guidance. Lance Spitzer provides some insight in his whitepaper, Auditing Your Firewall, at <http://www.enteract.com/~spitz/audit.html>.

Begin with a baseline. What do we expect our border routers, firewalls and other systems to do? This should be clearly defined and documented. All testing should be able to confirm or invalidate our expectations. Our goal is to clearly define that the GIAC security policy is or is not implemented in its various components.

- We expect that our customers can do business on our web sites.
- We expect to be able to exchange mail with our customers, suppliers and partners.
- We expect that only the network traffic necessary to accomplish those business goals will be able to gain entry into our internal and "service networks".
- We expect that external forces won't be able to map our internal and service networks.
- We do not expect that our employee's will be able to access unauthorized resources like Internet Relay Chat (IRC), Realplayer or Napster.
- We expect to be able to manage our network assets.
- We expect that our partner and our web servers will be able to access our internal database server.
- We do not expect to receive mail directly to our internal mail server.
- We do not expect our internal users to be able to query our external dns server.
- We expect that even if we are compromised by a Trojan or Worm that it will not be able to be contacted by a hacker.
- We expect that our traffic to our partner will be encrypted by an IPSec VPN from their router to ours.
- We expect that our external routers will be able to log to a server on our service network.
- We do not expect to be susceptible to known system vulnerabilities.
- We do not expect our firewall to accept traffic to the firewall from anything except our firewall administrators.
- We expect to "see" our audit tests on our IDS capabilities.
- We expect our logs to reflect our probes.

We want to define what services are available on each system. What can be "seen" from the local network, from the internet, from our partners network and from other components of our network. We will baseline all systems in accordance with SANS Incident Handling Step by Step guide and course material.

The technical approach will to use various commercial and open source software tools to probe our network resources. First we will use various tools to document what is actually available on each system that we are trying to reach. We will test production systems rather than lab "equivalents". After all, we all make mistakes. What we think is an equivalent may not be. We will use resources we know are available to hackers to make our architecture as secure as possible. We realize that we may inadvertently subject our own resources to what amounts to a denial of service attack in performing some tests but we will minimize the impact on our customers, partners and suppliers by conducting those tests during the least utilized periods of the day, week, and year. We want to ensure that we are operating at a known and acceptable level of risk.

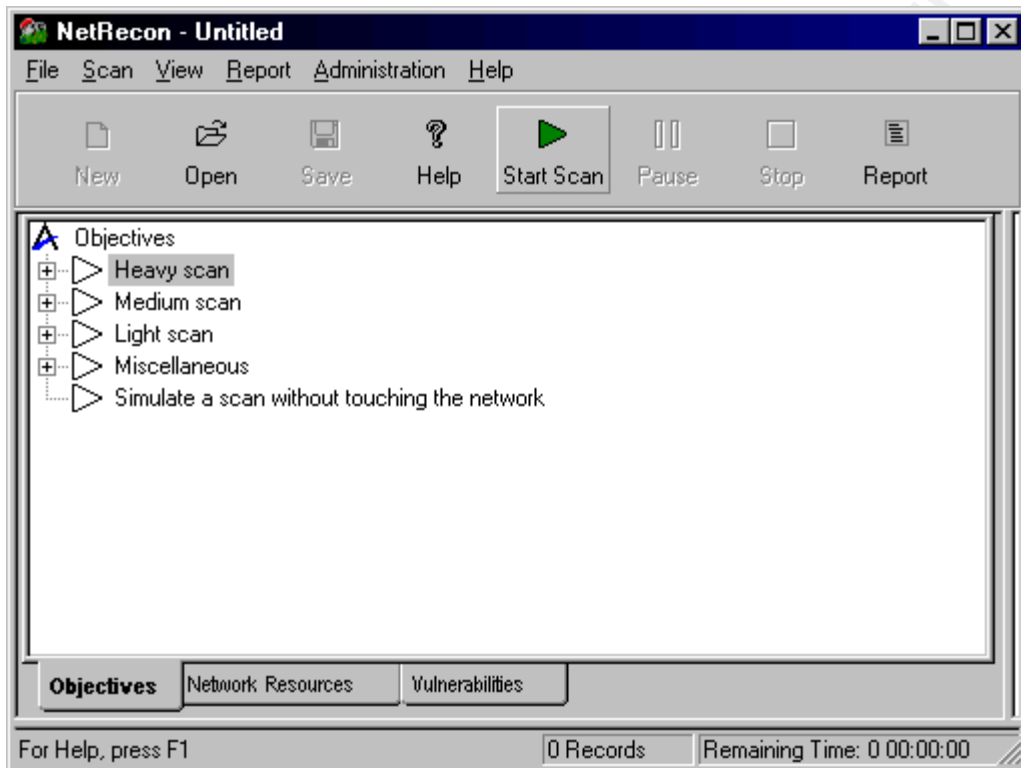
There are a number administrative and technical considerations that must be taken into considerations in executing the Audit:

1. Legal considerations: Many of the techniques and tools used in performing the tasks can be illegal if they are not specifically authorized by management. To avoid legal entanglements, written authorization of all tools and techniques is required.
2. Technical considerations: During the period of the assessment, there is the potential that servers, hosts, routers and other networking infrastructure can be irreparably compromised. It is important that all servers and hosts that are going to be targeted be properly backed up and a Disaster Recovery Plan be in place prior to the implementation of the assessment. Another technical consideration is that of false positives: Some tools may result in false positives and therefore the information gathered may not be that useful - it is therefore important to use multiple tools when preparing the information for use in the implementation phase; There is also a risk of an actual attack during the assessment: If an actual attack occurs during the assessment, a vulnerability exposed by you may be used by the attacker.
3. Shifts: Typically there are peak periods. We will conduct our tests during off peak periods.
4. Level of Effort: For each network (internal, external, and service) audit, levels of effort could be divided into a Recon phase (1 day), Enumeration phase (2 days), a Vulnerability Mapping & Penetration phase (2 days), and a Report Generation phase (3 days).

The effectiveness of a perimeter protection is only as strong as the weakest point. Every component (hosts, users, servers, services, etc.) present potential points of entry into a Network. However, our audit is specifically geared to establish that the firewall and border routers actually implement the security policies and rules they are supposed to. To do this, it will be necessary to set up a machine on the outside of the perimeter which will target the internal and service networks with variously formed packets. We will test the firewalls and the firewall rulebases. We will use tools such as nmapNT, Symantec (Axent) NetRecon, Superscan, Netcat, and Fragrouter to test the router and firewall rulebases. We'll monitor the scans with ISS RealSecure Network Sensor, NAI Sniffer Basic (former Net-Xray) and Windump. Enumeration tools like Red Button, Legion, NAT and Dumpsec will be used to test the firewall systems. Password cracking programs such as L0phtCrack, Pwdump2, Pwdump, Revelation, Sid2user, User2sid and John the Ripper will be used to test compliance with password policies on all firewalls.

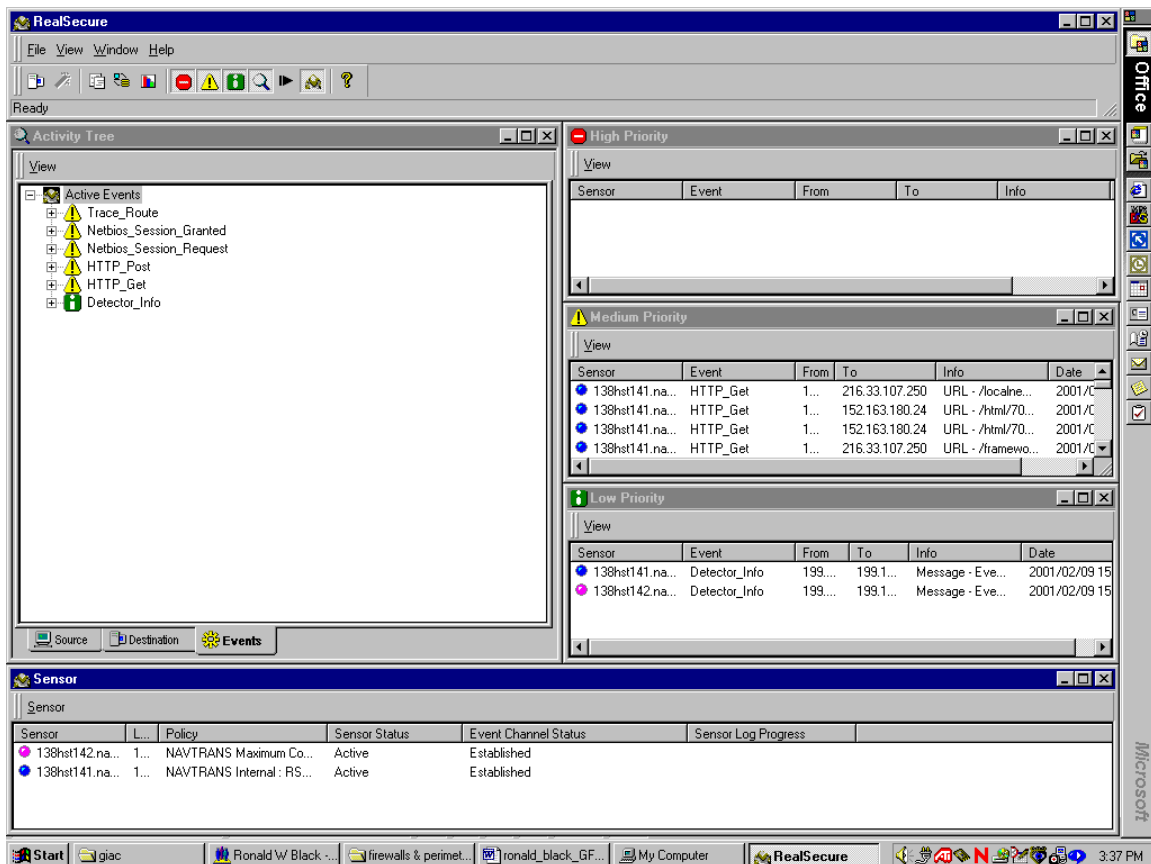
Now we want to implement our audit. Since the GIAC Enterprises Security Architecture firewalls, VPNs and border routers are conceptual creations, it will be impossible to produce "live"

screenshots. Screenshots are for demonstration purposes only and do not reflect actual configuration testing. We will begin by scanning our firewalls with 3 tools: NetRecon, NmapNT and Superscan. We will monitor the effects of the scans with 3 more tools: ISS RealSecure Intrusion Detection System, NAI's Sniffer Basic and Windump. We could also utilize or add SNORT IDS or Windows 2000 Network Monitor to help evaluate the effectiveness of the scans. We'll use multiple tools in this phase in order to have comparative data. We'll scan the specific devices and we'll scan the network addresses beyond the device to determine the effectiveness of our rulebases. Where necessary, we'll inject a passive hub to facilitate monitoring.



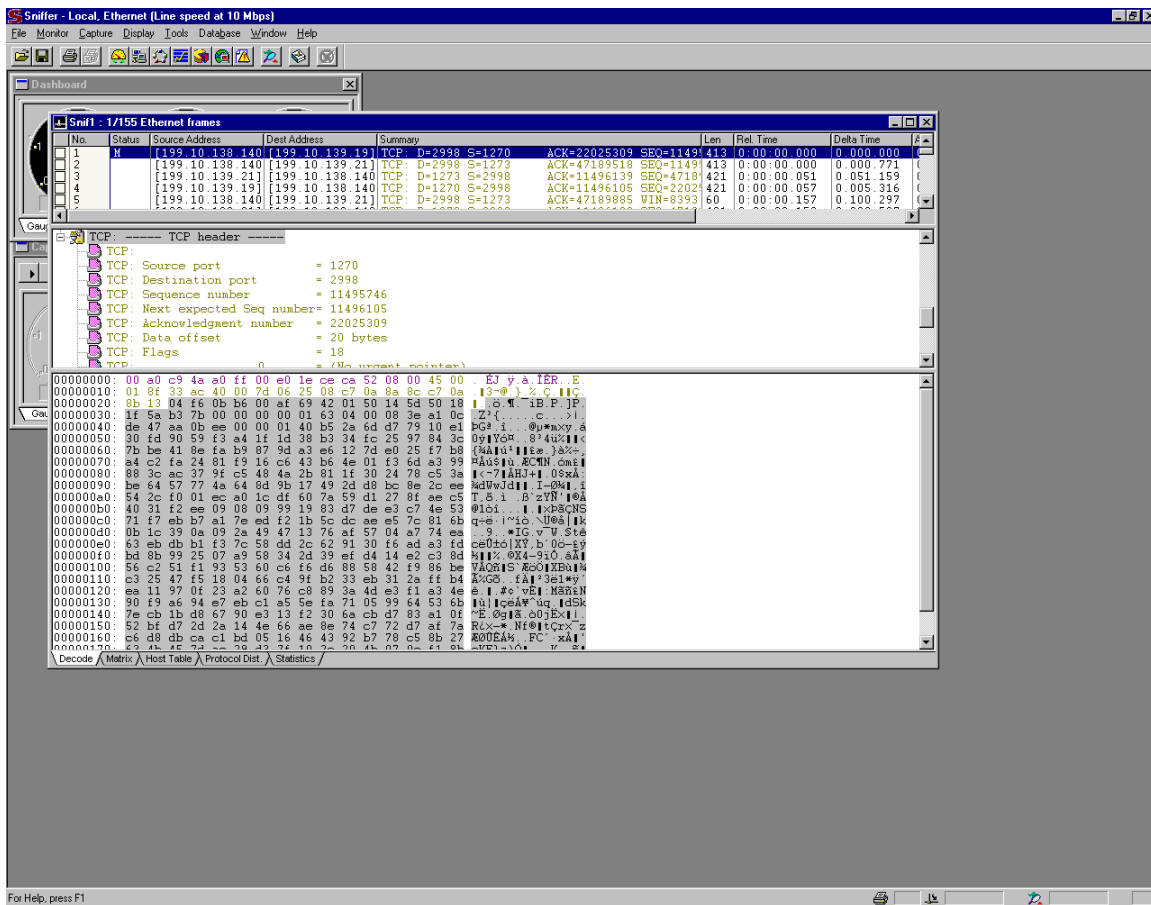
NetRecon is a commercial vulnerability scanner. Information concerning exactly what tests are performed by NetRecon can be found at http://www2.axent.com/swat/index.cfm?Doc=2000_04_25. We are running with Security Update 11 which adds a number of checks to the list above. Unlike ISS Internet Scanner which provides a number of scanning policy options, NetRecon functions on a "one size fits all" mentality. However it requires no particular skill or understanding to be able to use. Just press Start Scan and define the resource to be scanned. NetRecon will do the rest. NetRecon provides a report generation capability and contains information about what each vulnerability is and how to "fix" the vulnerability.

Our security architecture included ISS RealSecure Network Sensors and console. We'll use this commercial IDS capability to help us monitor the results of our audit. Our external sensors will help us monitor the effectiveness of our router configurations. Our internal Sensor will help us monitor the traffic getting past one of our Checkpoint Firewall-1s and our Gauntlet that screens our service networks from our internal network. The screenshot below gives a sample of the console interface.



We'll use our other commercial product, NAI Sniffer Basic, to monitor traffic on our service networks and our internal networks when we are testing to see what traffic passes beyond our firewall. Sniffer Basic provides a number of features which simplify the analysis of traffic if you don't have the understanding of TCP/IP that Windump requires.

© SANS Institute



The other tools that will be useful in determining the functionality of our design will be nmapNT, Superscan and WinDump. All of these tools are readily available. They are freeware and are very versatile in their use. NmapNT can be obtained at <http://www.eeye.com/html/databases/software/nmapnt.html>. Windump can be obtained at <http://netgroup-serv.polito.it/windump/>. Superscan can be obtained at <http://members.home.com/rkeir/software.html>. Other tools such as Fscan can be found at <http://www.foundstone.com/rdlabs/tools.php>. We can find netcat for NT at <http://www.l0pht.com/users/l0pht/nc11nt.zip>. The MAN page for nmap can be found at http://www.insecure.com/nmap/nmap_manpage.html. This manpage provides details on how to perform various scans with nmap

One nmapNT script to be used is

```
nmapnt -v -sS -sR -P0 -O -p1-65000 -oN nmap.out <system IP>
```

```
-v      = verbose mode
-sS     = syn scan
-sR     = RPC scan
-P0     = do not try to ping
-O      = try to identify remote host OS
-p1-65000 = scan ports 1-65000
-oN nmap.out = send out put to file nmap.out
<system IP> = IP addresses of systems to be scanned
```

```

MS-DOS Command Prompt
nmap U. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
  * -sS TCP SYN stealth port scan (best all-around TCP scan)
  * -sU UDP port scan
  -sP ping scan (Find any reachable machines)
  * -sF, -sX, -sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
  * -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
  * -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid!Sneaky!Polite!Normal!Aggressive!Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
  * -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES

D:\security\tool box\Nmapnt>_

```

Windump is a sniffer utility that we will use to capture network traffic. This will allow us to confirm that the packets that should have gotten through did and it should also let us see any packets that should not have gotten through but did. The syntax for this utility is

```
windump -v -n >dump.out
```

```

-v      = verbose mode
-n      = do not resolve domain names
>       = send output to human readable file dump.out

```

Below we've shown the results of an nmapNT scan of a Windows NT Checkpoint Firewall-1. This is not the firewall previously described in section 2 but is similar. This is an internal interface on that firewall. Note the operating system guess – Cisco IOS 11.2.

```

MS-DOS Command Prompt
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org ( www.insecure.org/nmap/ )

We skillfully deduced that your address is 0.0.0.0
Initiating SYN half-open stealth scan against (199.10.139.34)
Adding TCP port 23 (state open).
Adding TCP port 79 (state open).
The SYN scan took 66 seconds to scan 65000 ports.
For OSscan assuming that port 23 is open and port 1 is closed and neither are fi
rewalled
Interesting ports on (199.10.139.34):
(The 64998 ports scanned but not shown below are in state: closed)
Port      State      Service
23/tcp    open       telnet
79/tcp    open       finger

TCP Sequence Prediction: Class=random positive increments
                        Difficulty=1820 (Medium)

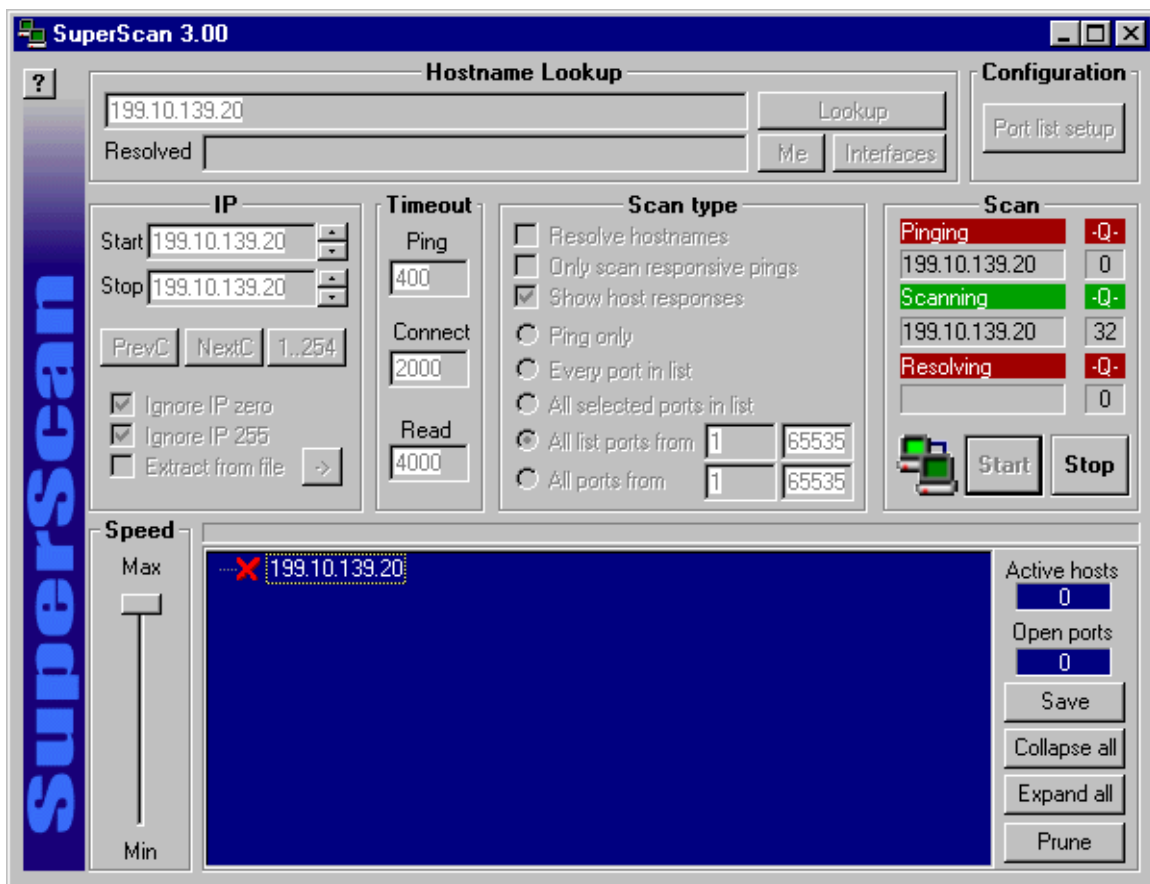
Sequence numbers: 19EA44D4 19EAA83C 19EB1C97 19EB91EA 19EC082A 19EC7C9A
Remote operating system guess: Cisco Router/Switch with IOS 11.2

Nmap run completed -- 1 IP address (1 host up) scanned in 76 seconds

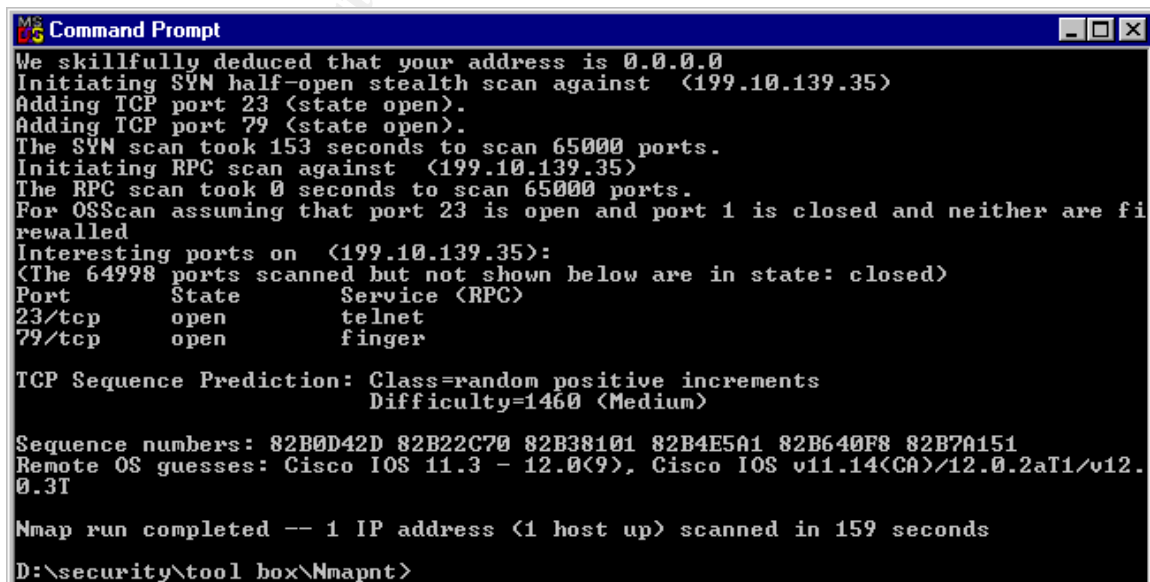
D:\security\tool box\Nmapnt>_

```

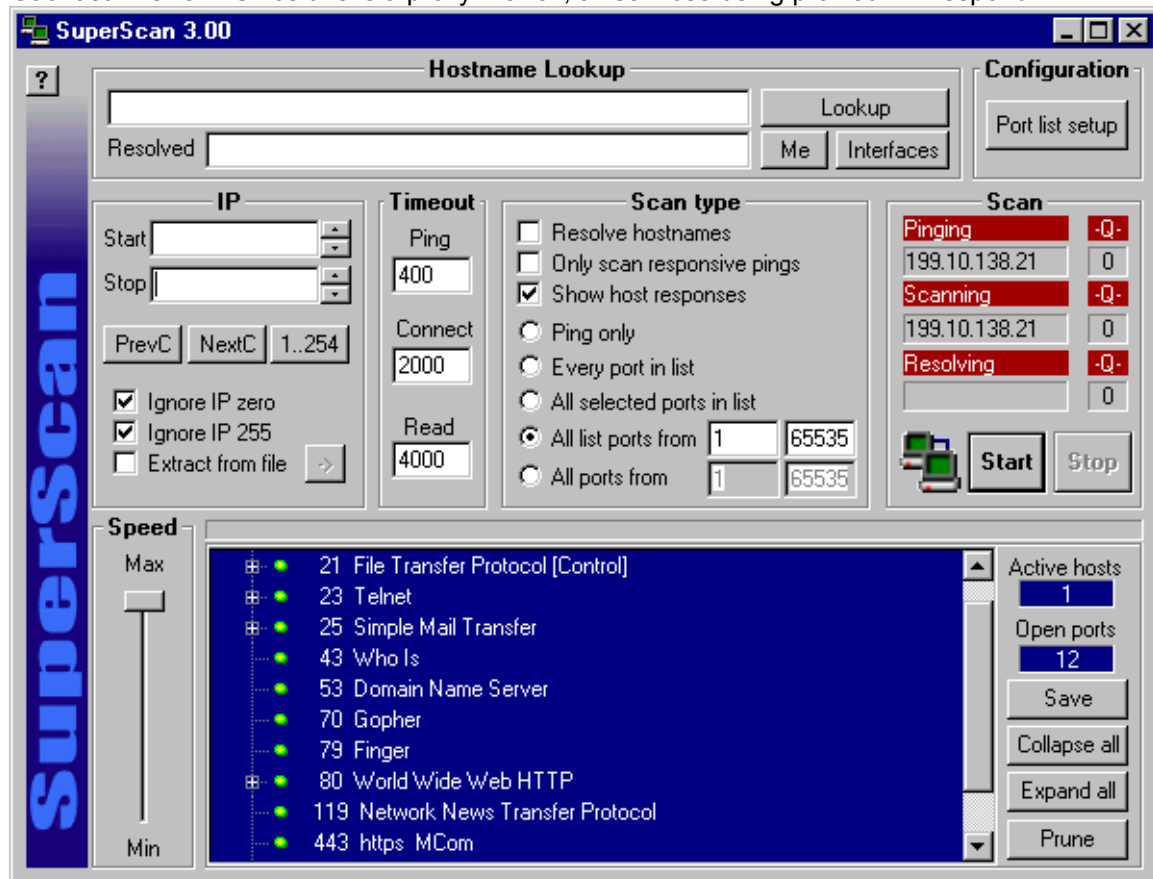
Here we've shown the same Firewall using Superscan but we are scanning the external interface. The external interface dropped all packets.



Here we've shown a nmapNT scan of a Cisco router running IOS 12.0 without the no finger command.

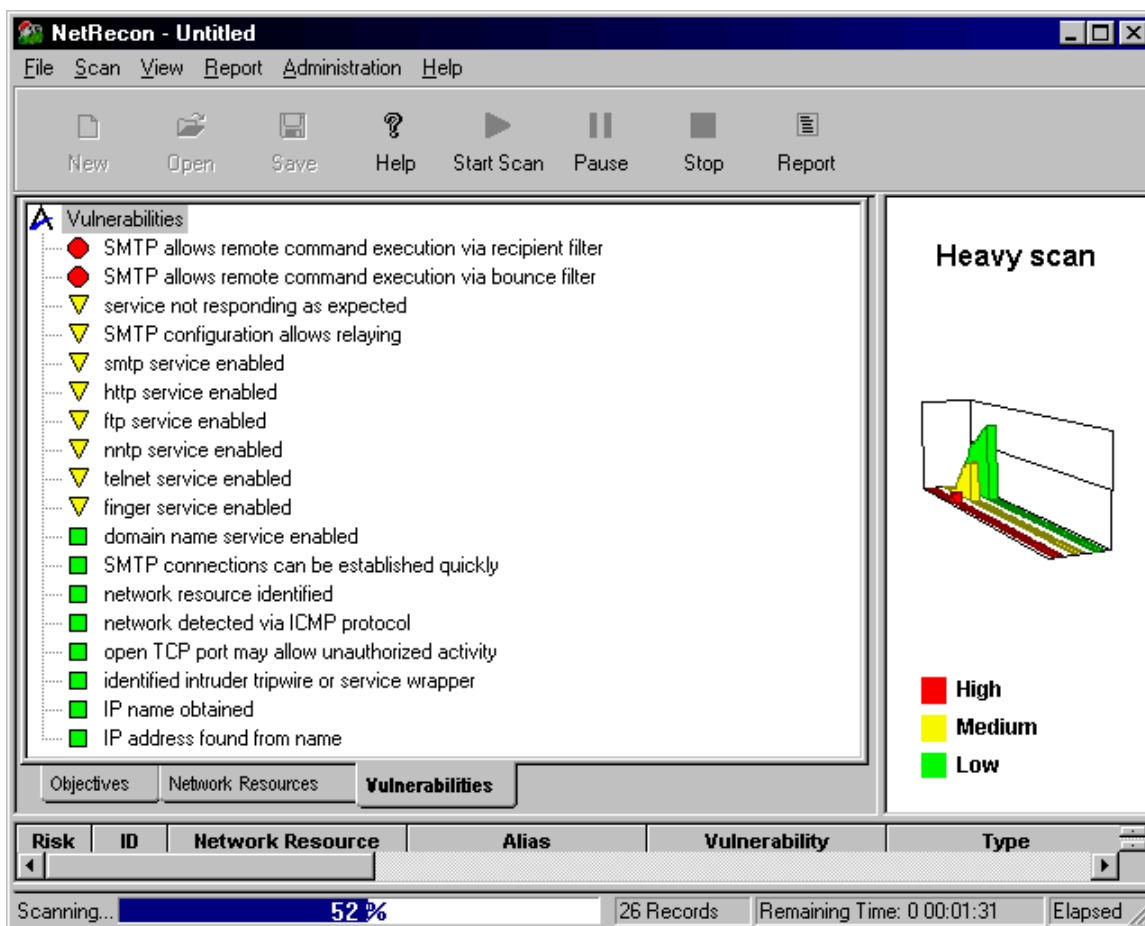


Here we've used Superscan to scan the external interface (service Network interface) of our Gauntlet Firewall. Since this is a proxy firewall, all services being proxied will respond.



The next screen shot is a NetRecon scan of the external interface (service Network interface) of our same Gauntlet Firewall.

© SANS Institute



We must understand how the firewalls and routers will react to being scanned in order to understand our results when we scan resources beyond the firewall. Otherwise we initially see something that didn't occur. That's also why we'll employ sniffers on the networks behind the routers and networks in order to capture and analyze the traffic which actually makes it beyond these devices. We can try to confuse and trick our firewalls with fragmented packets using netcat and Anzen's Fragrouter found at <http://www.anzen.com/research/nidsbench/>. Information on how to use fragrouter can be found at <http://www.anzen.com/research/nidsbench/fragrouter.html>. We can find netcat for NT at <http://www.i0pht.com/users/i0pht/nc11nt.zip>.

nc -v -z -w2 xxx.xxx.xxx.xxx produces a netcat UDP port scan

We can also use nmapNT's spoofing options to test our routers ability to block spoofed RFC 1918 addresses and our own legal addresses from the internet.

Referring to our network architecture diagram in Assignment one, we will want to make scans from the internet to our internal network through our "VPN" internet connection, from the internet to our DNS-Mail service network, from the internet to our Web service network, and from the internet to our internal network through our ecommerce connection. We'll want to scan our internal network from both service networks and we'll want to scan our service networks from our internal. Having completed these scans we can now move on to specific attempts to enumerate our firewall OS and password cracking. We'll try to establish a null session with our NT firewalls.

net use \\xxx.xxx.xxx.xxx\IPC\$ "" /u:"

We'll also use Reb Button to attempt to establish a null session and enumerate the box. This should fail because of our registry entry denying null sessions as well as the firewall's rule to drop all packets destined for the firewall except from the group called firewall admin. We'll also

use Checkpoints Policy Editor from various unauthorized addresses on our Firewall-1 firewalls and we'll use Gauntlet's GUI to attempt to hack the box. We'll perform this testing from our service networks, internal network, as well as from the internet.

After completing the testing we'll compile the results and make specific recommendations to improve the design. One of the weaknesses in the current design is the use of unencrypted telnet to manage the routers. Cisco offers Encrypted Kerberized Telnet based on the 56-bit Data Encryption Standard (DES) with a 64-bit Cipher Feedback. However, you must order the kerberos image in order to take advantage of this capability.

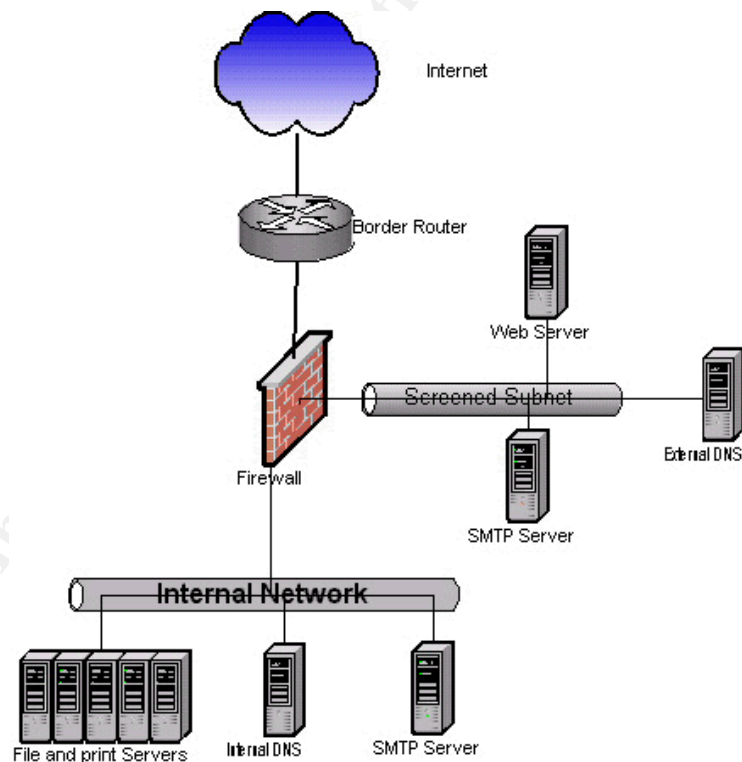
© SANS Institute 2000 - 2002, Author retains full rights.

Assignment 4 Submission: Design Under Fire

Select a network design from any previously posted GCFW Practical and paste the graphic into your submission. Design the following three attacks against the architecture.

- i. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
- ii. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
- iii. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

A Linux firewall with ipchains



An attack against the firewall itself.

The design reflected here was described as a Cisco 3600 series border router and a Mandrake 7.1 Linux machine running ipchains. The practical offered no particular information on what, if anything, was done to armor the Linux operating system before establishing an ipchains firewall. Searching www.rootshell.com identified a potential vulnerability in ipchains (Fragment Overlap

vulnerability) and www.linuxsecurity.com/advisories/mandrake.html offered a number of potential vulnerabilities to attack. The ipchains vulnerability allows traffic beyond the firewall, allowing attacks on the systems protected by the firewall.

Fragment Overlap vulnerability. There is a vulnerability in the linux firewall implementation in kernels 2.2.0 and above (IPChains). The vulnerability allows for an attacker to possibly send data to a blocked port. When a fragment is sent to a non-filtered port on a firewall with the IP_MF bit set and an offset of 0 with a full tcp header inside, it's possible to overlap the tcp port information. It is done by sending another fragment with an offset of 0, the IP_MF bit set and a length of 4 with the destination port number information. What happens is the following: when fragment A is sent to the firewall, it's passed onto the target host assuming it's going to the allowed port in the tcp header included in the fragment. The second fragment is sent along it's way as well, only to overlap the port information in the first while inside the reassembly chain. To finish off the attack, a fragment is sent with a normal offset (relative to the initial fragment) and an unset IP_MF bit. There are two conditions which need to be met to make this vulnerability exploitable: the linux kernel doing the firewalling needs to be configured so that defragmentation does not occur before passing through the filters and the firewall must allow non-first fragments to pass through. The first two fragments sent may need to be reversed depending on the defragmentation implementation of the target host operating system. We can attempt to make use netcat and fragrouter to craft the packets required to exploit this vulnerability.

So to begin our attack in earnest, the first thing that we will have to do is map the environment. We will use netcat and nmapnt because both include features that allow use to control the rate at which this network is scanned. After all, we don't want to call attention to ourselves as we attack this network. Once we've established what services are available on each system discovered, we can plot our attack. We can employ a couple of enumeration techniques. We'll try finger if its identified as a listening service.

```
finger -l @xxx.xxx.xxx.xxx
```

If finger isn't available we'll use netcat and telnet to feed raw data to listening ports. The netcat readme and Hobbit's original text provides guidance.

Now we can concentrate on attacking the firewall operating system services and the services of the other systems discovered. Based on services discovered we'll look for tools (script kiddie stuff) that will help us in our attacks. We can also try linuxconfig (port 98) to gain access.

A denial of service attack

Now we will subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that we've chosen. Since we have specifically been told to use 50 compromised cable modems/DSL system, we can be assured that we're looking at using DDoS tools that are designed for MS Windows 9x/ME/NT/2000 systems. While we might find Linux boxes on these network connections, it is less likely that we will find Unix systems. If given the source code we could port the UNIX DDoS tools to Linux but we're not going to work that hard. Besides, cracking the default install of any MS Windows version is relatively easy. Tools previously mentioned are readily available. Although we can choose from a number of DDoS tools (Trinoo, Tribe Flood Network (TFN), Stracheldraht, Trinity, Shaft, Freak88, Trank, Dest, FAPI, Mstream and TFN2K) many are Unix based. Only Trinoo for Windows or WinTrinoo will run on Windows 95, 98 and NT and is known to support enough zombies. Stracheldraht has an NT version but that isn't broad enough a platform selection to make finding zombie systems easy. Mstream is a Linux DDoS but we aren't looking to go in that direction.

Gary C. Kessler has posted an excellent paper on DDoS at

<http://garykessler.net/library/ddos.html> and also at www.sans.org under the GSEC practical where DDOS is explained. Information of all types of DDOS tools, Trojans and Worms ports, operating systems, and files can be found at <http://www.simovits.com/sve/myhetsyarkiv/1999/myheter9902.html>. We've chosen WinTrinoo and the client and daemon programs implement a DDOS network which can initiate a SYN flood attack. See <http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt> and <http://packetstorm.securify.com/distributed/razor.wintrinoo.txt> for more details. If we find enough Windows NT systems we'll also use Stacheldraht NT which performs ICMP floods, SYN floods, UDP floods and SMURF attacks (like TRN). See <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt> for more details. We'll scan ISPs like the @Home Network and cable companies for systems which have already picked up SubSeven and Qaz Trojans to ease our burden of compromising 50 computers. We will however, specifically hack a system to establish Master for our attack. We will use a previously discovered SubSeven compromised system to serve as the base system for the Hack of our master DDOS platform, thereby keeping our identity secret if discovered in the process. For our attack we'll use a combination of a SYN flood to the target network web server. We'll also attempt to exploit the new icmp-pmtu vulnerability below from our Stacheldraht NT boxes if we have them. Since the Web server is the core of the e-business, it becomes the logical target for a denial of service attack.

Date Reported: 1/15/01
Vulnerability: icmp-pmtu-dos
Platforms Affected: Linux
BSD
Risk Factor: Medium
Attack Type: Network Based
Brief Description: ICMP PMTU denial of service
X-Force URL: <http://xforce.iss.net/static/5975.php>

Defensive measures which should be taken to protect against a DDOS would include maintaining patches for system security vulnerabilities, egress filtering at the border routers for RFC 1918 and other "bad" addresses, blocking known Trojan ports, blocking unnecessary services like IRC (6665-6669), using tcpwrappers or "personal" firewalls on all systems, using a network based Intrusion Detection System (IDS), monitoring all logs, and insisting that ISP also performs egress filtering, etc. There are also tools available to detect the DDOS zombies like Robin Keir's DDOSping, Zombie Zapper by Bindview's Razor Team, and find_ddos by the National Infrastructure Protection Center.

Compromise an internal system through the perimeter

The Red Hat Linux DNS server is undoubtedly running a version of BIND. The four recently announced vulnerabilities in BIND would seem to be a "must try" to compromise a Perimeter system since the practical states that BIND 8.2.2-p5 is running. Another "must try" would seem to be using Trojans and Worms attached to email since internal mail system is MS-Exchange 5.5 SP3. We'll look at vulnerabilities associated with sendmail 8.11.0. And last but not least we'll look at vulnerabilities associated with an Apache 1.3.11 Web server.

Date Reported: 1/29/01
Vulnerability: bind-inverse-query-disclosure
Platforms Affected: Bind (4.x, 8.2.x)
Risk Factor: Medium
Attack Type: Network Based
Brief Description: BIND 4.x and 8.2.x exposes environment variables

X-Force URL: <http://xforce.iss.net/static/6018.php>

Date Reported: 1/29/01
Vulnerability: bind-tsig-bo
Platforms Affected: BIND 8.2.x
Risk Factor: Unauthorized Access Attempt
Attack Type: Network/Host Based
Brief Description: BIND 8.2.x transaction signature (TSIG) buffer overflow
X-Force URL: <http://xforce.iss.net/static/6015.php>

Date Reported: 1/10/01
Vulnerability: linux-apache-symlink
Platforms Affected: Apache
Risk Factor: Medium
Attack Type: Host Based
Brief Description: Linux Apache symbolic link
X-Force URL: <http://xforce.iss.net/static/5926.php>

We'll attempt to compromise the external DNS server through the new Bind 8.2.x TSIG buffer overflow vulnerability and gain root. We can also use helot.c (bitchx/ircd) DNS overflow script. If successful we'll introduce sniffers, crack and other hacker tools such as the Linux Rootkit (LRK) and Knark into the compromised DNS server. If we are able to crack the password file of the DNS server, we will use the root password and root equivalent accounts and passwords against the firewall since many administrators use the same accounts and passwords on all systems. We can use Crack and John the Ripper to crack passwords. We can also try the qib and rules exploit scripts to attempt to gain access.

We'll attempt to compromise the sendmail server. We'll try the following enumeration:

```
telnet xxx.xxx.xxx.xxx 25 * use telnet to connect to smtpd
vrfy root * confirms names of valid users
expn adm * reveals actual delivery addresses of aliases
mailing lists
```

These commands may be turned off in our target or may require authentication if it is properly configured. If they work we can use the information in a brute force password attack. We can still find some valid account information on the web site. We can attempt to exploit buffer overflow vulnerabilities in sendmail such as the sendmail pipe vulnerability. We can attempt to create or modify a users ~/.forward file. We can add all sorts of good stuff to this forward file like a string that will create a shell on the target system with the privileges of the victim user. By sending email to the victim user account, the file creating the shell will be written to the victims home directory (if it is writable).

```
cp /bin/sh /home/victim/gotya , chmod 755 /home/victim/gotya
```

When executed the file will create a shell.

We'll attempt to compromise the web server. We will use scripts like Phfscan.c and Cgiscan.c to help us identify vulnerabilities as well as scanners like Sitedscan and Whisker.

In the end, we'll opt to try one of the most sure fire means of compromise. We'll use email to send a worm into our target network from a compromised system. We'll send it to everyone in the company. At least one of ten employees are likely to open suspect email even though it may be against company policy. Like our most recent email worm, we'll use Worm Generator or simply modify the code of other VBS attacks to deliver netcat or some Trojan to internal systems. Netcat will be scripted to contact a compromised system, thereby introducing a portal inside the target network.

References

Hacking Exposed: Network Security Secrets & Solutions Second Edition, Joel Scambray, Stuart McClure, and George Kurtz, Osborne/McGraw-Hill, 2001.

Checkpoint Firewall-1 Administration Guide, Marcus Goncalves and Steven Brown, McGraw-Hill, 2000.

Building Internet Firewalls Second Edition, Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, O'Reilly, 2000

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