Global Information Assurance Certification Paper

GIAC Firewall and Perimeter Protection Curriculum

Practical Assignment for SANS Security DC 2000
Submitted By: *Danovan Golding*

Assignment 1: Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.

Currently, Most attacks rely on falsifying, or ”spoofing” the source address of IP datagrams. To help prevent your network from being use for Denial of Service(DoS) attacks, minimally you will need to implement anti-spoofing Access Control List(ACL) at your border router on the inbound interface. This ACL is also known as Ingress filter. The source routing should be turned off so that attackers cannot use the routing ability of TCP. In order to choose the path a packet will take and return on a network. For example, if a host on your network is able to spoof the address and then use source routing to a network that might use remote procedure calls(RPC) on a trusted host relationship, then they will be able to gain access to a remote machine without using passwords.

The Standard Access List filter will be used on a Cisco router running IOS. The access list uses a top down implementation trying to match a packet to a list of criteria. This is like a first fit implementation rather than best fit. You can only apply 1 access list in any given direction(serial) interface. Cannot define a standard and extended on a single interface. The syntax for a Standard Access List is:

```
access-list number action source wild-card any.
access-list   20   permit 192.168.1.0 0.0.0.255
```

The list number must have a value between 1 and 99 to specify a Standard Access List. The action could be permitted or denied. The “source” is the source IP address to compare. A “wild-card” determines what parts of an IP address are compared and which are not. The keyword “any” can be use in place of the address wildcard pair 0.0.0.0 255.255.255.255.

The access list needs to be created from the Cisco config prompt. The following is the anti-spoof access list:

```
access-list 20 deny     0.0.0.0         0.255.255.255
access-list 20 deny     10.0.0.0        0.255.255.255
access-list 20 deny     127.0.0.0       0.255.255.255
access-list 20 deny     192.168.0.0     0.0.255.255
access-list 20 deny     172.16.0.0      0.15.255.255
access-list 20 deny <your internal network> <your netmask>
```

Once the access list is applied on the interface in the following matter:

ip access-group 20 in

In order to block the source route you need to add a single command:

no ip source-route

Finally, you must exit the Cisco configuration prompt and write the new configuration file to memory. I prefer to test the new changes by implementing Nmap. Nmap is a port scanning utility by Fyodor. You can download Nmap at www.insecure.org and try to run a scan from outside your network coming in.

Assignment 2: Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

Ftp and telnet both are ways for logging on to remote servers to either download and upload files, or to establish a console. The majority of ftp applications and telnet should be restricted since they transfer passwords in clear text. E.g., (tcpdump can retrieve the password(or data)). NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a local area network. The protocol was created by IBM and adopted by Microsoft. An example of the use of this program is if an attacker can send NetBIOS name service a NetBIOS Name Conflict message even when receiving. The machine is not in the process of registering its NetBIOS name. That places the name in conflict and it can no longer be use. As a result, Microsoft only pay's attention to NetBIOS Name Conflict messages while in the registration phase, which leaves a machine vulnerable. This is part of the insecure design of NetBIOS(you can read more at www.securityfocus.com). Secure Shell is the replacement for rsh, rlogin, rcp, telnet, rexec, rcp and ftp. It encrypts all traffic and provides various levels of authentication. Eventhough, ssh encrypts data it provides a mean for a unprivileged user to gain access to a machine. In the occasion that a user gains access. They can do some recognizant to find vulnerability and will try to exploit the server. For those reasons the login services should be restricted.

***Check Point FireWall-1 will be employed to block the login services. The reason I am using a firewall to block these ports. Due to the fact that the Border router and firewall should work together. The access list on the Border router are cpu intensive and it may have an impact on the speed the packets are routed. The policy editor is where the access control policy is define. The rulebase format is similar to a Cisco ACL. They are process in first-fit as opposed to best-fit order and it reads from left to right:

Source
Destination
Service(port)
Action(accept, deny, reject, authenticate)
Track(long, short, alert)

The source is the inbound or traffic coming from the Border router. Destination passes the packets to the screen network. The service is login services or ports that use tcp which we will block . The action is what happens to the packet and the track will log the results. There are two fields that are irrelevant. They are install on and time. Creating a

group for the login service rulebase would make things clean. The group would need to have 21, 22, 23, 139, 512 and 514 for tcp ports. The source and destination is any. The action would be drop and the track could be long. Be careful on the order of the filter for netbios. It will be essential to include the rulebase to drop all internal netbios source with no logging. Unless you prefer a bunch of log files to filter through. Also, don't forget to allow your internal users login access to the internal machines. You may attempt telneting or ftping from a remote location to test the filter. The best alternative will be to test with the Nmap utility.

Assignment 3: RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

RPC stands for Remote Procedure Calls. RPC is a mechanism that allows a program to run on one machine and to execute commands on a remote system. NFS is a flexible method of sharing filesystems over heterogeneous environments. The portmap daemon converts RPC program numbers into Internet port numbers. Another type of portmapper is rpcbind. Many RPC services run as root, and a successful buffer overflow or an input validation attack that leads to direct root access. NFS relies on RPC services and can be easily confused into allowing attackers to mount a remote file system. The majority of NFS vulnerabilities relates to misconfiguration that exports the file systems to the public. Access to portmapper is the first step in scanning a system for the RPC services enabled, such as rpc.mountd, NFS, rpc.statd, rpc.csmd, rpc.ttybd, etc. If the intruder finds the appropriate service enabled they will run an exploit against the port where the service is running. IN the case that the portmapper is blocked an attacker may be able to manually scan for the RPC services. The best countermeasure for RPC and NFS is to disable all unnecessary services. A host base protection like TCP Wrappers can be implemented as well, but we will discuss blocking the ports using Check Point Firewall-1.

The syntax and description of Firewall-1 was explained in the second question. An additional group needs to be created for RPC and NFS. The ports will have 111, 2049 and 4045 for tcp and udp. The rulebase will be source is "any", destination is "any", services will be the newly created group, action is "drop" and the track is "long". After implementing the rule can be tested by using Nmap or rpcinfo. Rpcinfo is the equivalent of finger to find RPC applications listening on remote hosts.

Assignment 4: NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

Netbios was explained in details in the second assignment. It is important to reiterated that Microsoft uses netbios to communicate with other Microsoft machines with port 135. The clients remotely connect to the machine. They query the end-point mapper to find out where the service is. Hackers can scan the machine on this port to find out such things that the Exchange Server is running on this machine. This port is often hit in order to scan for services E.g.,(using the "epdump" utility); this port may also be attacked directly. There are a few denial-of-service attacks that can be directed at this port. You will see packets for port 137 any time someone is attempting to resolve your name (on Windows),

which may also result in unknown machines sending these packets to your site. If someone is using your IP address as part of a decoy scan, then the victim will send NetBIOS packets at you in order to resolve your name. Incoming connections to port 139 are trying to reach NetBIOS/SMB, the protocols used for Windows "File and Print Sharing" as well as SAMBA. The public will be sharing their hard disks on this port since it is the common vulnerability on the Internet. Firewall-1 will be used to block the ports 135(tcp and udp), 137(udp), 138(udp), 139(tcp) and 445(tcp and udp). After creating the group you can build a rulebase with source and destination is any. The service is the new group, action will be dropped and the track is long. Following installation of the new rule you can check if it works with the Nmap utility outside of the firewall. Another tool to use is NetBios Auditing Tool(NAT), based on code written by Andrew Tridgell.

Assignment 5: X Windows -- 6000/tcp through 6255/tcp

The X windows system allows many programs to share a single graphical display. The major problem with X windows is the security model is all or nothing. If the administrator runs "xhost +" command then it allows unauthenticated access to the server by any local or remote user. Many PC-based x servers default to the "xhosts +" unknown to the users. X clients can capture the keystrokes of the console user, kill windows, capture windows for display, and even remap the keyboard. One of the best programs to identify an X server with "xhost +" enabled is xscan. Xscan will scan an entire subnet looking for an open X server and log all keystrokes to a log file. But, if "xhost –" is enabled on the target system , an attacker may be able to capture the console screen of the user's session via xwd utility if the attacker has shell access and the target system is using standard xhost authentication.

Firewall-1 will be used to block the X Windows services. The services for X Windows must be created using the tcp ports 6000 to 6255. Now you will build a new rule by using "any" for source and destination. The services will be the recent generated X window with action being dropped and track being long. After installing the rule, run xscan and Nmap to verify it works.

Assignment 6: Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)

Domain Name System(DNS) gives out information to the internet and retrieves information about others. DNS is a distributed database use to resolve IP addresses to IP names and IP names to IP addresses. LDAP stands for Lightweight Directory Access Protocol or Active Directory(AD) for Microsoft users. LDAP is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. What DNS is to the internet LDAP is to an organization. Attackers can use the DNS zone transfer to get valuable information on a network. Once they have the data they can actually map out the entire network. Attackers can also perform DoS attacks by convincing the victim server to cache bogus address information . When a

DNS server performs a lookup, they are redirected to the site the attackers want them to go. LDAP is designed to contain a unified, logical representation of all the objects relevant to the corporate technology infrastructure which attackers can use for recognizant. Using a tool from NT Resource Kit called ldp, which connects to an AD server and browses contents of the directory.

You will need to create four rules for this filter. First rule will allow DNS queries to the DNS server. The source will be "any" and the destination will be DNS-server. The services is udp 53 and the action is "accept". The track is short because the expectation of queries. The second rule allows zone transfers to and from the secondaries to the master DNS. The source are the IPs of the secondaries DNS servers. The destination will go to the internal DNS server. The service is tcp 53 and the action is "accept". The track for this will be "short". The third rule will deny any other DNS request. The source and destination will be "any". The service is 53 for tcp and udp. The action is "drop" and the log is "short". The last rule is to drop any LDAP packets. The source and destination is "any". The service is 389 for tcp and udp. The action is "drop" and the track is "long". After installing the rule, you can run a zone transfer with nslookup and change your server to another machine behind the firewall. Use the ldp command to check for LDAP service.

Assignment 7: Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

SMTP stands for Simple Mail Transfer Protocol and it is a TCP/IP protocol use for sending and receiving e-mail. POP stands for Post Office Protocol and it is a client/server protocol in which e-mail is received and held for you by your internet server. POP downloads all your e-mail from the server to your local machine. IMAP stands for Internet Message Access Protocol and it lets you view your e-mail at the server as though it was on your client machine. POP can be thought of as a "store-and-forward" service. IMAP can be thought of as a remote file server. SMTP, POP and IMAP do not typically include provisions for reliable authentication as part of the core protocol, allowing email messages to be easily forged. Nor do these protocols require the use of encryption which could ensure the privacy of email messages. A misconfigured e-mail server could be compromised or use as a spamming machine.

Check Point FireWall-1 filters will be installed. Two rulebases will be created to implement a successful filter. The first rulebase will allow all mail request to the mail server. The source is any and the destination is the mail server. The service will be tcp 25(smtp) and the action is accept. The track is going to be long. The second rulebase will drop all mail services including IMAP and POP. The source and destination is any. Create a group for tcp 25(smtp), tcp 109 and 110 (pop), and tcp 143(imap). Put the newly created group in service and the action is drop. The track is going to be long. I have a problem with these two rulebase, because it leaves no means for users to retrieve their e-mail especially if login services will be blocked. This means another rule should be created before the dropping of all mail traffic to allow IMAP and POP to retrieve messages. After installing the rules try to telnet to a server's port 25 from outside the

firewall. A telnet attempt to the mail server will be successful but may fail in any other machine. Also, try telnet to ports 109, 110 and 143 from outside the firewall. This should result in an unsuccessful attempt. Don't forget to use Nmap the reliable port tester.

Assignment 8: Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)

The Hypertext Transfer Protocol (HTTP) is the set of rules for transferring files E.g.,(text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocol, HTTP is an application protocol. HTTP has multiple vulnerabilities that allow attackers to execute any command locally as the web server users. This often results in downloading of the "/etc/passswd" files. Common Gateway Interface(CGI) is another open point for attackers. The basic problem arises frequently from not validating input scripts. Without input validation it is possible for attackers to submit a character, along with a local command, as a parameter and have the web server execute it locally. The Secure Sockets Layer(SSL) protocol provides a relatively secure means to encrypt data passed over a public network like the Internet. SSL was created by Netscape to use the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. SSL is use by other web servers like Apache and Microsoft. The SSL protocol is vulnerable to hyperlink spoofing, an attack on the SSL server authentication. In earlier versions it was discovered that a flaw in the design will allow some circumstances for an intruder who is able to capture the traffic of an SSL-encrypted session, and subsequently interrogate the server involved in the session, to recover the session key used in that session, and then recover the encrypted data from that session.

Check Point FireWall-1 filters will limit the web traffic. My understanding is that the network will only allowed web access to the organization external Web servers, which will result in two rules. The first rule will allow internal users web access to external web servers. The source is going to be internal and the destination is the pre-defined external web servers. The service ports are 80 and 443 for tcp. The action is "accept" and the track is "long". The second rule will deny everything. The source and destination is "any". A new group will be created for the ports 80, 443, 8000, 8080 and 8888. The new group will be in the services and the action is "drop". A tremendous amount of logs will be generated from all the internal users trying to do some web surfing and it will continue to track "long". The Nmap tool can be used to test the new rules after they are in placed.

Assignment 9: "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

There are a few ports below 20 that an attacker can use E.g.,(the port 0 is Commonly used to help determine the operating system). This works because on some systems, port 0 is "invalid" and will create different response when connected vs. a normal closed port. Port 1 uses tcpmux signifying an attacker is probing for SGI Irix machines. Irix is the only major vendor that uses tcpmux. Port 7 uses echo and a common DoS attack is an

echo-loop. An attacker forges a UDP from one machine and sends it to the other. Then both machines bounce packets off each other as fast as they can. Port 11 uses sysstat and this is a unix service that will list all the running processes on a machine and who started them. Port 19 is chargen, this is a service that simply spits out characters. Hackers can take advantage of IP spoofing for denial of service attacks. Forging UDP packets between two chargen servers, or a chargen and echo may overload links as the two servers attempt to infinitely bounce the traffic back and forth. The time protocol provides a site-independent, machine readable date and time. The Time service sends back to the originating source the time in seconds since midnight on January first 1900(RFC868).

Cisco IOS has a command that will disable the small services easily rather than creating rules on a firewall. The following is the command to disable small services:

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

It is not that simple to block the time service in Cisco IOS. An Extended ACL must be generated because the Standard ACL will not block ports. Here is the Extended ACL:

```
access-list 101 deny tcp any any eq 37
access-list 101 deny udp any any eq 37
ip access-group 101 in
```

The Nmap utility will ensure that the newly created filters are working.

Assignment 10: Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog(514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)

Trivial File Transfer Protocol(TFTP) is normally use to boot diskless network equipment. TFTP provides little security and attackers may use it to download router configuration files from the server and will attempt to retrieve the password. Finger is a way of giving out information on a user. An attacker will use finger to see when administrative users are login or to find a user name and run a password guess attack to gain access. Network News Transfer Protocol(NNTP) is the predominant protocol used by computers (client/server) for managing the notes posted on Usenet newsgroup. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Line Printer Daemon(LPD) is part of the BSD print services. It listens for and accepts connections via TCP/IP to submit a print request. The lpd daemon relies on the LPD protocol to accept the job, and submit it to the requested printer. Syslog is a system logging utility. An organization might have a single system logging machine but it should never be put outside the internal network because attackers will to get at it. Simple Network Management Protocol(SNMP) is a very common port that intruders probe for. SNMP allows for remote management of devices. All the configuration and performance information is stored in a database that can be retrieved or set via SNMP. Border Gateway Protocol(BGP) is the recommended choice of the Exterior Gateway Protocols. Currently BGP provides the routing protocol that supports the current internet backbone. There is no need to have any Exterior Gateway Protocol in your local network.

SOCKS is a protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. This protocol tunnels traffic through firewalls, allowing many people behind the firewall access to the Internet through a single IP address. In theory, it should only tunnel inside traffic out towards the Internet. However, it is frequently misconfigured and allows hackers/crackers to tunnel their attacks inwards, or simply bounce through the system to other internet machines, masking their attacks as if they were coming from you.

The Cisco border router will be used to block the miscellaneous services. The ACLs will be applied to the inbound interface. The following Extended ACL are listed below:

```
access-list 101 deny udp any any eq 69
access-list 101 deny tcp  any any eq 119
access-list 101 deny tcp  any any eq 515
access-list 101 deny udp any any eq 514
access-list 101 deny tcp  any any eq 161
access-list 101 deny udp any any eq 161
access-list 101 deny tcp  any any eq 162
access-list 101 deny udp any any eq 162
access-list 101 deny tcp  any any eq 179
access-list 101 deny tcp  any any eq 1080
```

The finger service can be disable with “no service finger” command and NTP will be disabled with the interface command “no ntp enable”. As a result of the newly applied rules Nmap utility can be run to test if the rules are working.

Assignment 11: ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

Internet Control Message Protocol(ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol datagram; but the messages are processed by the IP software and are not directly apparent to the application user. UDP and IP can not communicate error conditions so ICMP handles it. ICMP is also use to map an entire network due to the fact all hosts listen and reply to ICMP. In addition, ICMP can be use maliciously as a conduit for DoS attempts. The most known DoS which ICMP uses are: Smurf, WinFreeze, Tribal Flood Network(TFN) and Loki.

An Extended Access Control List will be used to block the ICMP traffic. The following ACL will be placed on the incoming interface to stop echo request:

```
access-list 101 deny ICMP any any echo
```

The outside world will not be able to ping my network with the ACL. The next set of access-list should be created to handle the outgoing echo reply and time exceeded. The ACL for the outgoing interface will be:

```
access-list 102 deny icmp any any  echo-reply
access-list 102 deny icmp any any time exceeded
```

In addition, the access-list must be place on the outbound interface for them to properly work. Finally, the "no ip unreachables" command can be use to block the ICMP unreachable messages. The command must be place on an interface to work. As a result, the ICMP should be locked down due to the implemented ACLs. Try to run a ping test outside the network to test the new filters.

Conclusion:

Blocking the 11 assignments with the border router and firewall is a good start for securing a network. A strong perimeter defense should exist with a potent internal defense. Attackers are also coming from your internal network where security is needed. Defending the inside by updating all operating systems, and applications with the most recent patches, and removing all unnecessary services that are running on machines and make sure they are properly configured. Make sure all system logging is enabled and incorporate a strong authenticating system. Host based protection like TCP Wrappers can be used to filter some of the services that needs to run. TCP Wrappers would be an ideal tool to use with assignments 2(Login Services), 7(Mail) and 10(Misc.). Application tool like Tripwire would be perfect to check a server integrity. In addition, a switched network will prevent users against packet sniffing. The advantages of having security layers is to leave no single point of failure. This procedure will give you more time to react to a potential security break.

Resources:

www.sans.org

www.antionline.com

www.whatis.com

www.secinf.net

www.cisco.com

www.securityfocus.com

www.faqs.org

Hacking Exposed. Network Security, Secrets & Solutions by Stuart Mcclure, Joel Scambray and George Kurtz. Osborne/McGraw-Hill.

Sans Firewalls and Perimeter Protection course materials.