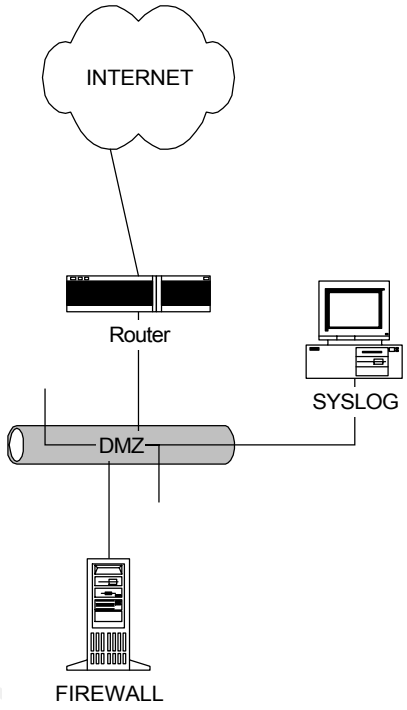
# Global Information Assurance Certification Paper

**Donald J Kuntz II**
**GIAC Firewall and Perimeter Protection Curriculum**
**Practical Assignment for SANS Security DC 2000**
**July 5 – 10, 2000**

For this assignment we are to set up a perimeter defense that will block a list of ports, which are the most commonly probed and attacked. I will be using a Cisco 2611 router running 12.0 5T1 IOS with two Ethernet interfaces and one serial interface. The following is a basic diagram of the network.




The router is the first line of defense in a multi-layer approach to perimeter security. The router will augment the firewall, which is our main defense against attack, by blocking the ports that are commonly used in probes and attacks. This approach will stop the majority of the script kiddies but it will only slow down a determined intruder from probing and attacking the firewall.

**Access Control List**

The way we configure the router to block ports is through the use of access control list. Access control list are packet filters, which are used by the router, to determine whether to forward or to drop packets at the interface to which they applied. The criteria that the router uses is based one or all of the following; source address, source port, destination address, and destination port. Filtering on the source address and port is the least secure method because they are easily spoofed.

There are several types of access control list that can be used on the Cisco router. The IP extended access list is the one we will use for this assignment. The IP extended access list can be either numbered, starting at 100 to 199, or it can be named. I will use the named IP extended access list because it easier to associate a named with it's intended function. (ex. internetfilter, egressfilter).

Our main focus here is to present to you the basic format on creating and implementing access control lists on Cisco routers. For more in-depth knowledge or to find out more about the other access control lists you can go to following sites:

http://www.cisco.com/

http://www.knowcisco.com/

**Basic concepts**

Before we get started on creating a named access list we must first go over some basic concepts associated with them. The router will test every incoming packet against the conditions in the access list line-by-line start at the top of the access list working its way to the bottom. At the first match, the router will stop to determine whether if it should reject or to forward the packet. Because the router stop testing the packet after the first match the order of the access list is important. As a general guideline, you should place a specific rule before a general rule. If the router cannot make a match with any of the conditions in the access list, by default, it will reject that packet.

You cannot make a change to any statement within a named access list. You must first delete the statement and then reenter the statement, which will then be appended at the end of the access list. Because of this, you may find it easier to save the configuration to a TFTP server, make your changes to the file using a text editor, then save it back up to the router.

If a 0 bit appears in the mask, the corresponding bit location in the access list address must be the same as the packet address for the criteria to match. If a 1 bit appears in the mask, it is not tested against the packet. (Ex. 192.168.1.0 0.0.0.255 any address from the 192.168.1.0 network will match). A "host" in the mask denotes a specific ip address and "any " in the mask denotes any ip address.

Command descriptions use the following convention:

- **boldface:** indicates any keywords that are to be written as shown
- [x]: indicates arguments that are optional
- {x}: indicates a require argument
- {x | y | z}: indicates that you must choice one of the arguments

Key words used in access list:

- log - means send any match to a syslog
- permit - means the packet will be forwarded
- deny - means the packet will be dropped
- operator can a qualifying condition like the following
    - eq means equal to a specific port number

- range means a range of port
- gt means greater than the port

**Named Access Control List**

The syntax for creating a named IP extended access list is:
router(config)# **ip access-list extended** {name of the access list}

The basic syntax for creating an entry in the extended access list is:

{permit | deny}{protocol type} {source address | source-wildcard} {destination address | destination-wildcard}{protocol-specific-options} [log]

Cisco will convert some protocol type number into their symbolic names. The following is a list of those names:

| | |
|---|---|
| ahp | Authentication Header Protocol |
| eigrp | Cisco's EIGRP routing protocol |
| esp | Encapsulation Security Payload |
| gre | Cisco's GRE tunneling |
| icmp | Internet Control Message Protocol |
| igmp | Internet Gateway Message Protocol |
| igrp | Cisco's IGRP routing protocol |
| ip | Any Internet Protocol |
| ipinip | IP in IP tunneling |
| nos | KA9Q NOS compatible IP over IP tunneling |
| ospf | OSPF routing protocol |
| pcp | Payload Compression Protocol |
| pim | Protocol Independent Multicast |
| tcp | Transmission Control Protocol |
| udp | User Datagram Protocol |

A complete listing of protocol types can be found at: ftp://ftp.isi.edu/in-notes/iana/assignments/protocol-numbers

The syntax for applying the access list to the interface

Router(config-if)**# ip access-group** {name of the access list} **in** | **out**

For an inbound access the router will check to see if the packet will match any statement before it decides either to route or to drop the packet. While for the outbound access list, the router will receive the packet from one of its interface, route to the controlled interface, and then it is check against the access list to see if it will forward or drop the packet. It is best to apply an access list so that the packet can be dropped as soon as possible to save on the router CPU resources.

**ICMP Command Syntax**:

{**permit** | **deny**} **icmp** {source address | source-wildcard | **any**}{destination address | destination-wildcard | **any**}[icmp-type [icmp-code] | icmp-message]

deny icmp any any echo

This statement will drop all icmp echo request.

Cisco will convert some icmp type and code into symbolic names. The following is a list of those names:

| | |
|---|---|
| administratively-prohibited | Administratively prohibited |
| alternate-address | Alternate address |
| conversion-error | Datagram conversion |
| dod-host-prohibited | Host prohibited |
| dod-net-prohibited | Net prohibited |
| echo | Echo (ping) |
| echo-reply | Echo reply |
| general-parameter-problem | Parameter problem |
| host-isolated | Host isolated |
| host-precedence-unreachable | Host unreachable for precedence |
| host-redirect | Host redirect |
| host-tos-redirect | Host redirect for TOS |
| host-tos-unreachable | Host unreachable for TOS |
| host-unknown | Host unknown |
| host-unreachable | Host unreachable |
| information-reply | Information replies |
| information-request | Information requests |
| log | Log matches against this entry |
| log-input | Log matches against this entry, including input interface |
| mask-reply | Mask replies |
| mask-reply | Mask replies |
| mask-request | Mask requests |
| mobile-redirect | Mobile host redirect |
| net-redirect | Network redirect |
| net-tos-redirect | Net redirect for TOS |
| net-tos-unreachable | Network unreachable for TOS |
| net-unreachable | Net unreachable |
| network-unknown | Network unknown |
| no-room-for-option | Parameter required but no room |
| option-missing | Parameter required but not present |
| packet-too-big | Fragmentation needed and DF set |

| | |
|---|---|
| parameter-problem | All parameter problems |
| port-unreachable | Port unreachable |
| precedence | Match packets with given precedence value |
| precedence-unreachable | Precedence cutoff |
| protocol-unreachable | Protocol unreachable |
| reassembly-timeout | Reassembly timeout |
| redirect | All redirects |
| router-advertisement | Router discovery advertisements |
| router-solicitation | Router discovery solicitations |
| source-quench | Source quenches |
| source-route-failed | Source route failed |
| time-exceeded | all time exceededs |
| time-range | Specify a time-range |
| timestamp-reply | Timestamp replies |
| timestamp-request | Timestamp requests |
| tos | Match packets with given TOS value |
| traceroute | Traceroute |
| ttl-exceeded | TTL exceeded |
| unreachable | All unreachables |

A complete listing of icmp types and code can be found at: ftp://ftp.isi.edu/in-notes/iana/assignments/icmp-parameters

**TCP Command Syntax:**
{**permit** | **deny**} **tcp** {source address | source-wildcard | **any**}[operator source-port | source-port]{destination address | destination-wildcard | **any**}[operator destination-port |destination port]

permit tcp any host 192.168.1.10 eq smtp log

This statement will forward any tcp packet destined for port 25 and then log the match to a syslog.

The established keyword will allow any tcp packet that has the ACK or RST flag set. With the numerous scanners, which can spoof the ACK and RST flags the established keyword can be easily thwarted, so I normally will not use it.

Cisco will convert some TCP port numbers into symbolic names. This symbolic names are in reference to the well-known TCP port numbers to which their services was registered with IANA. . The following is a list of those names and the ports:

| | |
|---|---|
| bgp | Border Gateway Protocol (179) |
| chargen | Character generator (19) |
| cmd | Remote commands (rcmd, 514) |
| daytime | Daytime (13) |

| | |
|---|---|
| discard | Discard (9) |
| domain | Domain Name Service (53) |
| echo | Echo (7) |
| exec | Exec (rsh, 512) |
| finger | Finger (79) |
| ftp | File Transfer Protocol (21) |
| ftp-data | FTP data connections (used infrequently, 20) |
| gopher | Gopher (70) |
| hostname | NIC hostname server (101) |
| ident | Ident Protocol (113) |
| irc | Internet Relay Chat (194) |
| klogin | Kerberos login (543) |
| kshell | Kerberos shell (544) |
| login | Login (rlogin, 513) |
| lpd | Printer service (515) |
| nntp | Network News Transport Protocol (119) |
| pim-auto-rp | PIM Auto-RP (496) |
| pop2 | Post Office Protocol v2 (109) |
| pop3 | Post Office Protocol v3 (110) |
| smtp | Simple Mail Transport Protocol (25) |
| sunrpc | Sun Remote Procedure Call (111) |
| syslog | Syslog (514) |
| tacacs | TAC Access Control System (49) |
| talk | Talk (517) |
| telnet | Telnet (23) |
| time | Time (37) |
| uucp | Unix-to-Unix Copy Program (540) |
| whois | Nicname (43) |
| www | World Wide Web (HTTP, 80) |

A complete listing of tcp port numbers can be found at: ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers%7E

**UDP Command Syntax:**

{**permit** | **deny**} **udp** {source address | source-wildcard | **any**}[operator source-port | source-port]{destination address | destination-wildcard | **any**}[operator destination-port |destination port]

deny udp any any eq 389

This statement will block all udp packet destined for port 389.

Cisco will convert some UDP port numbers into their symbolic names. Here again, those

symbolic names are to be used as a reference to associate the well-known UDP port numbers with their services that were registered with IANA. The following is a list of those symbolic name and the well-known ports:

| | |
|---|---|
| biff | Biff (mail notification, comsat, 512) |
| bootpc | Bootstrap Protocol (BOOTP) client (68) |
| bootps | Bootstrap Protocol (BOOTP) server (67) |
| discard | Discard (9) |
| dnsix | DNSIX security protocol auditing (195) |
| domain | Domain Name Service (DNS, 53) |
| echo | Echo (7) |
| isakmp | Internet Security Association and Key Management Protocol (500) |
| mobile-ip | Mobile IP registration (434) |
| nameserver | IEN116 name service (obsolete, 42) |
| netbios-dgm | NetBios datagram service (138) |
| netbios-ns | NetBios name service (137) |
| netbios-ss | NetBios session service (139) |
| ntp | Network Time Protocol (123) |
| pim-auto-rp | PIM Auto-RP (496) |
| rip | Routing Information Protocol (router, in.routed, 520) |
| snmp | Simple Network Management Protocol (161) |
| snmptrap | SNMP Traps (162) |
| sunrpc | Sun Remote Procedure Call (111) |
| syslog | System Logger (514) |
| tacacs | TAC Access Control System (49) |
| talk | Talk (517) |
| tftp | Trivial File Transfer Protocol (69) |
| time | Time (37) |
| who | Who service (rwho, 513) |
| xdmcp | X Display Manager Control Protocol (177) |

A complete listing of UDP port numbers can be found at: ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers%7E

## Practical Assignments

**Assignment 1:** Block "spoofed" addresses- packets coming from the outside your company sourced from internal address or private addresses. Also block source routed packets.

Private IP addresses, as assigned in RFC 1918, are to be used within the organization's local area networks and are not to be routed over the Internet. So any incoming packets with these addresses could be considered to be misrouted packets, a hostile attempt to probe, attack, or to disrupt normal traffic flows. Since I have no IP multicast (class D) or any need for the experimental (class E) those IP addresses will also be blocked from entering my network.

This statement, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will bock all packets with a source IP address of 0.0.0.0 and then log it to a syslog

deny ip host 0.0.0.0 any log

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets with a source IP address of the private address as defined by RFC 1918 and then log it to a syslog.

deny ip 10.0.0.0 0.255.255.255 any log
deny ip 172.16.0.0 0.0.255.255 any log
deny ip 192.168.0.0 0.0.255.255 any log

This statement, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets with a source IP address of a multicast (class D) or experimental IP address (class E) range and then log it to a syslog

deny ip 224.0.0.0 31.255.255.255 any

This statement, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets with a source IP address of my network and then log it to a syslog

deny ip mynetwork 0.0.0.255 any log

This statement, part of the INTERNEETFILTER access list, when applied to the inbound Internet connection will block all packets with a source IP address of Loopback interface and then log it to a syslog

deny ip 127.0.0.0 0.255.255.255 any log

This statement, part of the EGRESSFILTER access list, when it applied to the inbound connection from my network it will prevent IP address spoofing coming from my network then log it to a syslog. This statement goes at the end of the access list so that I can prevent all ICMP echo replies, time exceeded, and unreachable from exiting my network under any circumstances.

permit ip mynetwork 0.0.0.255 any

Source routing is option in the IP packet that allows the user to determine the path that they want to take to specific site.

The vulnerability is that a person can initiate a TCP connection specifying an explicit path that will override the route selection process. The following statement will allow the router to drop all ip datagram with source routing option bits set. This command is applied through global configuration mode:

no ip source-route

**Assignment 2:** Block the ports used by Login services (telnet, SSH, FTP, NetBIOS,

rlogin)

Telnet protocol provides a standardize interface that can used to access the resources of another host as if was locally attached. After the two hosts negotiated a mutual understanding, consisting of the data format, duplex type, and echo function, either one of the hosts can propose additional options to be used.

Vulnerabilities: Since telnet transmit username, passwords and commands in the clear they are susceptible sniffer-type attack also the password are susceptible to brute-force cracking attacks

FTP protocol is one the most used protocol used on the Internet. It is used to transmit data from one host to another.

Vulnerabilities: Username, password, and commands are transmitted in clear text making them susceptible to sniffer-type of attacks also password susceptible to brute-force cracking attacks. Misconfigured server enable user root access and server abuse. Several FTP versions have denial of service vulnerabilities.

SSH is a packet-binary protocol that provides a secure end-to-end tunnel meant to be used instead of common insecure protocol like telnet and FTP.

Vulnerabilities: Several version of SSH were found to be susceptible to buffer overflow attacks which allowed malicious code to executed at root level and also the ability to read environmental variables and kerberos credentials.

The following statement, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 21 thru to 23 and then log it to a syslog.

```
deny   tcp any any range ftp telnet log
```

rlogin will allows a user to remotely login to a machine without a password if the following conditions are meet. The call must originate from a privilege TCP port, caller name and IP address must be listed as a trusted partner, and finally the caller must correspond with the IP address.

Vulnerabilities: rlogin is vulnerable to buffer over which can cause the execution of arbitrary code at the root level.

This statement, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP 512 thru 515 and then log it to a syslog.

```
deny   tcp any any range exec lpd log
```

**Assignment 3:** Block the ports used by RPC and NFS (Portmap/ rpcbind, NFS, lockd)

Portmap/rpcbind: Portmap/rpcbind is responsible for maintaining a registrar of RPC programs and which ephemeral ports they are using. The portmap/rpcbind provides for four server procedures; PMAPPROC_SET- call by the RPC server to set a register, PMAPPROC_UNSET a call by the RPC server to remove a register, PMAPPROC_GETPORT call by an RPC client to obtain a port number for a given

program, and PMAPPROC_DUMP return all entries in the port mapper database.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 109 thru 111 or to UDP port 111 and then log them to a syslog.

```
deny   tcp any any range pop2 sunrpc log
deny   udp any any eq sunrpc log
```

NFS: NFS protocol enable machines to share file across the network through the use of the RPC API. Instead of the server keeping stateful track of which clients are accessing which files it uses what is called a file handle. A file handle is a file issued to the client by the server upon a request for a file. The file handle is to be return to the server when the client needs access to that file.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP port 2049 or to UDP port 2049 and then log it to a syslog.

```
deny   tcp any any eq 2049 log
deny   udp any any eq 2049 log
```

Lockd: Lockd is used to maintain file integrity. Since NFS is a stateless service, a server does not know if more than one client is accessing the same file. To prevent multiple clients from having access to a file at the same time, the lock manager places a lock on the file until the client is finished with the file.

Vulnerabilities: Recently RPC and NFS were found to vulnerable to a denial of service by forcing lockd to crash and several buffer overflows, which can allow an execution of arbitrary code at the root level. RPC can be used in the reconnaissance of the network by forcing portmap to execute a PMAPPROC_DUMP.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP port 4045 or to UDP port 4045 and then log it to a syslog.

```
deny   tcp any any eq 4045 log
deny   udp any any eq 4045 log
```

**Assignment 4:** Block the ports used by NetBIOS in Windows NT.

NetBIOS is an application programming interface (API) that allows for an application on one host to talk to an application on another host, the use session management services, name management services, and user datagram services do this.

The name service, for each host, is attached to UDP port 137. The name service will try get as much information about services available on the network by periodically notifying its neighbors, through the use of broadcast, that up and offering services.

Session management service is responsible for establishing and maintaining the connection between two hosts through the use of TCP port 139

Datagram management service is responsible for sending information when a response is not required this is accomplished through the use UDP datagrams. This server

resides on UDP port 138.

Vulnerabilities: Vulnerabilities ranging from denial of service attack, reconnaissance of the network, brute force password cracks, and resetting of services

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 135, 139, 445, UDP ports 135, 137, 138, 445 and then log it to a syslog.

```
deny   tcp any any eq 135 log
deny   udp any any eq 135 log
deny   udp any any range netbios-ns netbios-dgm log
deny   tcp any any eq 139 log
deny   tcp any any eq 445 log
deny   udp any any eq 445 log
```

**Assignment 5:** Block ports used by X Windows.

X Windows was developed to provide a method exporting the graphical display of a program to a remote or local host. This is done by the use of client-server type model. The server is a dedicated program responsible for controlling the terminal. The clients send the server the information to be displayed and then server sends back the application information about the user input. The communication between the server and the client is done through the use of X protocol.

Vulnerabilities: Denial of service attack causing the keyboard and mouse to freeze eventually causing the host to lock up. Predictable port usage, incrementing by one for each connection after the first, makes it susceptible to be scanned. The use of weak authentication, improved in later version, makes it susceptible to brute force attacks.

This statement, is part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 6000 thru 6255 and then log it to a syslog

```
deny   tcp any any range 6000 6255 log
```

**Assignment 6:** Block ports used by Naming services (DNS to all machines that are not DNS servers, DNS zone transfers except from external secondaries, LDAP)

DNS is a distributed database used to map hostname to IP address and to provide electronic mail routing information. LDAP protocol defines the transport and format of messages between the client and the X.500-like directory used to store user information, such as username and password

Vulnerabilities: DNS servers are subject to several types of attacks. Reconnaissance attacks are used to acquire information about your network through the use of zone transfers. Cache poisoning is used to redirect someone to a different site.

LDAP has some buffer overflows that can cause 100% utilization of the CPU rendering the system essentially unusable. Along with buffer overflows some version recently had password and authentication problems.

Windows 2000 Denial of service attack: Sending a stream of binary 0 to UDP port 53 will cause 100% CPU utilization.

At present my ISP is maintaining my external DNS servers so there is no reason

for DNS queries to enter my network so I will block them at the router. These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 53, 389 or to UDP ports 53, 389 and then log it to a syslog

```
deny   tcp any any eq domain log
deny   udp any any eq domain log
deny   tcp any any eq 389 log
deny   udp any any eq 389 log
```

**Assignment 7:** Block ports used by Mail services (SMTP to all machines that are not external mail relays, POP, IMAP)

SMTP: Simple Mail Transfer Protocol is responsible for the exchange of mail between two hosts. The exchange of mail is down by mail transfer agent (MTA). There are several version of MTA of which Sendmail is the most popular.

POP: Post Office Protocol is simple protocol that allows the retrieval of email from the server and deletes it.

IMAP: Internet Message Access Protocol has both client and server functions. The server has the ability to store message for multiple user, and the client has the capability to manage message on the server as well as to selective retrieve them.

Vulnerabilities: The majority of vulnerabilities for these services are buffer overflow caused by sending a string of characters resulting either in locking up the host or the ability to run malicious code at the root level.

The first statement is to allow SMTP from any IP address to my mail server's IP address followed the other statements blocking all packets destined to TCP ports 25,109 thru 111, and 143 and then log it to a syslog. The permit statement must go first to allow the packets to the mail and then deny those ports to non-mail server.

```
permit tcp any host mail.mynetwork eq smtp
deny   tcp any any eq smtp log
deny   tcp any any range pop2 sunrpc log
deny   tcp any any eq 143 log
```

**Assignment 8:** Block ports used by Web services (HTTP and SSL except to external Web servers, may also want to block common high–order HTTP port choices)

HTTP: Hypertext Transfer Protocol is design to transfer hypertext markup language (HTML) documents from one host to another. HTML documents may contain text, links to other pages, graphic images, audio, video clips, Java applets, and VRML a script language.

HTTP is based on request-response activity. The browser opens a connection to the server and then sends a request to retrieve information from the server. The server sends back the request, in the form of HTML page, back to the browser and then closes the connection.

Vulnerabilities are most the buffer overflow type causing either a denial of service or the ability to run arbitrary code.

Since we do not maintain any Web servers we will block HTTP request

into our network. These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 80, 8000, 8080, 8888 and then log it to a syslog

```
deny   tcp any any range finger www log
deny   tcp any any eq 8000 log
deny   tcp any any eq 8080 log
deny   tcp any any eq 8888 log
```

**Assignment 9:** Block ports used by Small Services.

Small service was once used as a debugging and measurement tools. Upon a established connection or received datagram the small server would respond with either the time of day, a stream of data, a list current user, a short message, or any data received would be sent back

Vulnerabilities are reconnaissance attacks and denial of service.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 1 thru 19, UDP 1 thru 19 and then log it to a syslog

```
deny   tcp any any range 1 chargen log
deny   udp any any range 1 19 log
```

**Assignment 10:** Block ports used by miscellaneous services (TFTP, finger, NNTP, NTP, LPD, syslog, SNMP, BGP, SOCKS)

TFTP was design to fit into read-only memory and to be used only during bootstrap process of diskless systems. TFTP provides no security and susceptible denial of service attack and file alteration.

Finger command is used find out what user are logged onto a system. This is a reconnaissance tool to find user name to used later in brute force crack attack.

NNTP is used both by server-to-server and client-to-server communication to share large amounts of information and to conduct user forums and discussion groups. They are vulnerable to buffer overflows in which arbitrary code can be executed.

LPD is used to print locally or over the network. They are vulnerable to authentication and user privilege where one may get access to root.

Syslog is the defacto standard for network logging of system and network events. The vulnerabilities are denial of service by attacking the equipment causing the equipment to reset or crash.

SNMP was design to let heterogeneous system and equipment to talk to each other, report data, and to allow modification to their settings over the network. The vulnerabilities of SNMP are that hosts can be remotely reconfigured or valuable information can be retrieved from your network.

SOCKS is a standard for circuit-level gateway that doesn't require as much overhead as the more conventional proxy servers. They are vulnerable to buffer overflow causing the unit to crash.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all packets going to TCP ports 69, 79, 80, 119, 123,

161, 162, 179, 512 thru 515,1080, UDP ports 161,162,514 and then log it to a syslog.

```
deny   udp any any eq tftp log
deny   tcp any any range finger www log
deny   tcp any any eq nntp log
deny   tcp any any eq 123 log
deny   tcp any any range 161 162 log
deny   udp any any range snmp snmptrap log
deny   tcp any any eq bgp log
deny   tcp any any range exec lpd log
deny   udp any any eq syslog log
deny   tcp any any eq 1080 log
```

**Assignment 11:** Block ICMP messages (incoming echo request (ping and windows traceroute, outgoing echo replies, time exceeded, and unreachable)

ICMP is used communicate error message and other condition of importance. The problem with ICMP is that can give out valuable information to map your network.

These statements, part of the INTERNETFILTER access list, when applied to the inbound Internet connection will block all incoming echo request (ping) and windows trace routes from coming into the network and then log it to a syslog

```
deny   icmp any any echo log
deny   icmp any any traceroute log
```

These statements, part of the EGRESSFILTER access list, when applied to the inbound connection from my network will block all outgoing echo replies, replies from windows trace routes and unreachable replies from leaving my network and then log it to a syslog.

```
deny   icmp any any echo-reply log
deny   icmp any any time-exceeded log
deny   icmp any any unreachable log
```

By default, the router will send back an unreachable message back to the sender after dropping a packet. To prevent the router from sending out unreachable message use the following command at interface attached to Internet connection. This command is issued in the interface configuration mode.

```
no ip unreachables
```

**Final Router Configuration**

This is the final router configuration, which was used to meet all eleven requirements in the practical assignment section.

```
version 12.0
no service pad
service tcp-keepalives-in
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname router
!
no logging console
enable secret <removed>
!
username <removed> password 7 <removed>
!
memory-size iomem 10
ip subnet-zero
no ip source-route
no ip finger
ip tcp selective-ack
no ip domain-lookup
!
no ip bootp server
ip audit notify log
ip audit po max-events 100
!
!
process-max-time 200
!
interface Ethernet0/0
 description CONNECTION TO THE DMZ
 ip address mynetwork 255.255.255.0
 ip access-group EGRESSFILTER in
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 no cdp enable
!
interface Serial0/1
 description CONNECTION TO THE INTERNET
 ip address A.B.C.D 255.255.255.248
 ip access-group INTERNETFILTER in
 no ip redirects
 no ip unreachables
 no ip directed-broadcast
 no ip proxy-arp
 no ip route-cache
```

```
 no ip mroute-cache
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 A.B.D.2
no ip http server
!
!
ip access-list extended EGRESSFILTER
 deny   icmp any any echo-reply log
 deny   icmp any any time-exceeded log
 deny   icmp any any unreachable log
 permit ip mynetwork 0.0.0.255 any
ip access-list extended INTERNETFILTER
 deny   ip host 0.0.0.0 any log
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 127.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.0.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 deny   ip 224.0.0.0 31.255.255.255 any
 deny   ip mynetwork 0 0.0.0.255 any log
 permit tcp any host mail.mynetwork eq smtp
 deny   tcp any any eq smtp log
 deny   tcp any any eq domain log
 deny   udp any any eq domain log
 deny   tcp any any range 1 chargen log
 deny   udp any any range 1 19 log
 deny   tcp any any range ftp telnet log
 deny   tcp any any eq 37 log
 deny   udp any any eq time log
 deny   udp any any eq tftp log
 deny   tcp any any range finger www log
 deny   tcp any any range pop2 sunrpc log
 deny   udp any any eq sunrpc log
 deny   tcp any any eq nntp log
 deny   tcp any any eq 123 log
 deny   tcp any any eq 135 log
 deny   udp any any eq 135 log
 deny   udp any any range netbios-ns netbios-dgm log
 deny   tcp any any eq 139 log
 deny   tcp any any eq 143 log
 deny   tcp any any range 161 162 log
 deny   udp any any range snmp snmptrap log
 deny   tcp any any eq bgp log
 deny   tcp any any eq 389 log
```

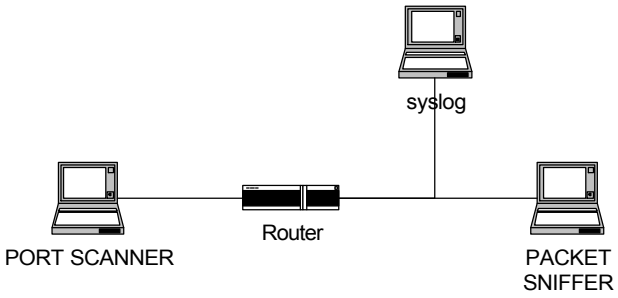
```
 deny   udp any any eq 389 log
 deny   tcp any any eq 443 log
 deny   tcp any any eq 445 log
 deny   udp any any eq 445 log
 deny   tcp any any range exec lpd log
 deny   udp any any eq syslog log
 deny   tcp any any eq 1080 log
 deny   tcp any any eq 1999 log
 deny   udp any any eq 1999 log
 deny   tcp any any eq 2049 log
 deny   udp any any eq 2049 log
 deny   tcp any any eq 4045 log
 deny   udp any any eq 4045 log
 deny   tcp any any range 6000 6255 log
 deny   tcp any any eq 8000 log
 deny   tcp any any eq 8080 log
 deny   tcp any any eq 8888 log
 deny   icmp any any echo log
 deny   icmp any any traceroute log
 permit ip any mynetwork 0.0.0.255
logging trap debugging
logging source-interface Ethernet0/0
logging 192.168.1.113
no cdp run
!
line con 0
 exec-timeout 5 0
 login local
 transport input none
line aux 0
 exec-timeout 5 0
 login local
line vty 0 4
 exec-timeout 5 0
 login local
!
scheduler interval 500
end.
```

**Testing Access Lists**

Now that we are finished creating the access lists we need to test them. This is to insure that they functioning they way we intended them to work. It is better to find out

now then later.

To test the access list we will need the use of two computers, one running a port scanner and other running a packet sniffer. The port scanner will be placed on the outside of your network to simulate traffic coming in and the packet sniffer place on the inside to simulate your hosts inside.




We will port scan both the router and the packet scanner to insure that we have sufficiently harden the router as well as blocked the appropriate ports. The packet sniffer will used to verify that the ports are being blocked and the logging to syslog is working.

When we are satisfied that everything is working properly we can put the unit into production.

**References:**

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

TCP/IP Tutorial and Technical Overview
by Martin W. Murhammer, Orcun Atakan, Stefan Bretz, Larry R Pugh, Kazunari, David H Wood

Firewalls and Internet Security Repelling the Wily Hacker
by William R Cheswick, Steven M Bellovin

Designing Network Security
by Merike Kaeo

Security Focus web site http://www.securityfocus.com
Security Portal web site http://www.securityportal.com