Cisco Router Security

• What are the two access privilege modes of the Cisco router?
Unprivileged: limited examination of router (Router>)
Privileged EXEC: detailed examination of router, debugging, testing, file manipulation (Router#)

• What is the approach for password for the privileged mode of the router?
enable password *insert password*
enable secret *insert password*

• How to ensure that all passwords in the router are stored in the encrypted form?
service password-encryption

• What is the difference between the Cisco router's startup and running configurations? How to save the running configuration into start up configuration?
All current changes are stored in the router's RAM. The startup is the configuration that is stored in the router's NVRAM. This configuration is run when the router is started up. Use the "write" command to save the current configuration to the startup configuration.

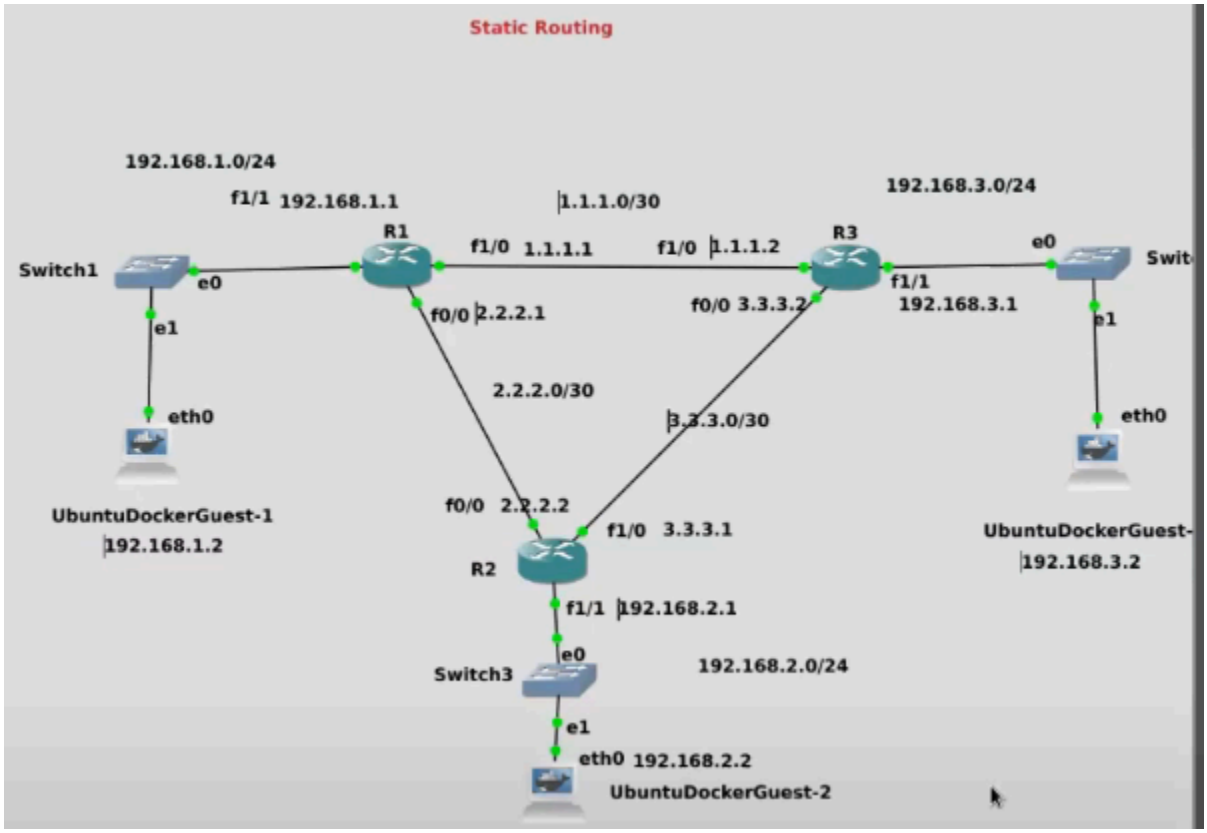
• Know and be able to configure all aspects of the Cisco router covered in class. For example, configuring the router interfaces, setting the router OSPF ID, etc.

Router>	- User EXEC mode
Router#	- Privileged EXEC mode
Router(config)#	- Configuration mode (notice the # sign indicates this is accessible only at privileged EXEC mode)
Router(config-if)#	- Interface level within configuration mode
Router(config-router)#	- Routing engine level within configuration mode
Router(config-line)#	- Line level (vty, tty, async) within configuration mode

Practical Routing, OSPF, and Security

• What is the difference between static and dynamic routing?
Static routing:

Entries are manually added to the forwarding table
The route the packets will take a predetermined route



ip route <subnet> <mask> <destination port>

```
R3(config)#ip route 192.168.1.0 255.255.255.0 1.1.1.1
R3(config)#
```

R3 -> R1

Dynamic routing:
Routing that can adapt to changes (if network devices are added, removed, and/or fail)
Routers will communicate with each other and will share the routing information (will update the routing table itself)
Simplify network configurations
Scalable with less overhead compared to static routing

• What is the difference between link state and distance vector routing?
Distance Vector Routing: Each router computes distance from itself to its next immediate neighbor (RIP, EIGRP, and BGP)
Does not build a full map of the network
Focuses more on the next hop towards the destination

Link State Routing: Each router shares knowledge of its neighbor with every other router in the network (OSPF and IS-IS)

Builds a full map of the network
Each router shares information
Maintains a database of the entire network

• Give an example of the distance vector and link state algorithms.

• What type of protocol is Routing Information Protocol (RIP)? Be able to understand examples and solve problems.
RIP is an example of a distance vector routing protocol.
Shares routing information with neighboring routers
An interior gateway protocol that operates within autonomous system
Limited to maximum 15 hops; The 16th hop advertisement means and invalid hop

RIP sends regula update messages (advertisements) to neighboring routers
Every 30 seconds that resets after successful advertisement
A route becomes invalid if it has not received a message for 180 seconds

• What type of protocol is Open Shortest Paths First (OSPF) protocol? Be able to understand examples and solve problems.
OSPF is an example of a link state routing protocol.
An interior gateway protocol that operates within autonomous system to build a full map of the network

• What is the Link State Advertisement (LSA) in OSPF? What is the Link State Database (LSDB)?
LSA is a message that the router uses to advertise the state of its links (information about each of its links to the other routers). All routers will collect LSA from other routers to create the LSDB.

• How does each router in OSPF create a map of the entire network?
Routers in OSPF create a map of the entire network by using the information given from LSAs to create LSDBs. Using the information about the state of each link, we can use that information to construct a view of the entire topology.l

• What is the process for two OSPF routers to become neighbors?
Step 1: A main router sends a Hello packet (message) to the neighbor. The message contains information such as the router's id, the link that it is advertising, the area number, and information on timers such as the dead timer.
Step 2: When the other neighboring router receives the information, the neighbor will check if the router's information matches up. It also checks if the routers have a link in the same subnet and if their timers values are the same.
Step 3: The neighboring router replies to the main router with the same information in Step 1.
Step 4: The main router checks if the information is correct.
Step 5: The routers are now neighbors and will exchange LSDB information with each other.

Step 6: The routers start routing and forwarding LSAs to each other.

• What is the difference between point-to-point and multi-access networks? How does OSPF handle each case?
Point-to-point network:
A link that connects exactly two neighbors to each other

Multi-access network:
A link that connects multiple neighbors through devices such as switches
When the router realize they are on the same multi-access network, routers will elect a designated router and one back-up designated router
All routers will ignore all LSA advertisements unless it comes from the designated router
The back-up designated router will get promoted to the designated router if the designated router fails

• Be able to configure OSPF routing given a topology. – Example: Consider a topology with three routers R1, R2, and R3. The routers are connected R1 = ⇒ R2 = ⇒ R3 = ⇒ R1. R1 has interface f0/0 connected to the interface f0/0 of R2. R2 has interface f0/1 connecting to the interface f0/0 of R3. Finally R3 has interface 1/0 connecting to the interface 1/0 of R3. Assuming all routers are Cisco 7200 routers, configure them to use OSPF to dynamically route in this topology (you will be given the Cisco router manual for such questions).

#config t
#router ospf 1
#router-id 1.1.1.1
Advertise interfaces on the network
#network <*subnet*> <*wildcard mask (inverse of subnet mask*) area 0
#network 192.168.1.0 0.0.0.255 area 0
#network 1.1.1.0 0.0.0.255 area 0
#network 2.2.2.0 0.0.0.255 area 0
(Change the area if the areas are different colors)

• How does OSPF authenticate packets to protect against packet spoofing and tampering? Be able to enable it in a Cisco router.
OSPF uses md5 mac function. The routers will share the same secret key. The routers will take the data of the packet and run it through the hash function. The digest of the mac function is then appended to the packet. The packet is then sent. When the receiving router receives the packet, the router will take the data and run it through the mac function. The router will then compare the digest to the original digest appended to the packet. Matching digest proves that the data has not been tampered.

```
R1(config)#interface f1/0
R1(config-if)#ip ospf mes
R1(config-if)#ip ospf message-digest-key 1 md5 cpsc456password
R1(config-if)#ip ospf au
R1(config-if)#ip ospf authentication me
R1(config-if)#ip ospf authentication message-digest
R1(config-if)#
```

Network Defense Fundamentals

• What is IP spoofing? Explain.
Sender changing his source address to something other than their real address. The destination and source IP would be changed.

• How can IP spoofing be used in security attacks?
IP spoofing can be used to hide the origin of the attack.

• What are the countermeasures to IP spoofing?
Ingress filtering is used for routers to block packets originating from outside their network, whose source address specifies a machine inside the network (e.g. A router receives a packet from outside the network but has a source IP from inside the network. The router would then reject the packet).
Egress filtering is used for routers to block packets originating from inside their network, whose source address specifies a machine outside of their network (e.g. A router receives a packet from inside the network but has a source IP from outside the network. The router would then reject the packet).

• How can IP spoofing be used to perform DoS attacks?
DoS refers to any attack designed to force a piece of machinery to become unavailable and unable to perform the basic functionality. This is possible since servers have finite bandwidth. Once the bandwidth is exhausted, the server starts dropping packets. DoS attackers often spoof to avoid detection.

• Know how to use hping3 for performing ping floods.
Ping flood attacks are attacks that overwhelm the system with numerous pings.

Using the Kali VM as the attacker's machine:
#hping3 -1 <target ip> -fast
(Sends 10 packets per second)

#hping3 -1 <target ip> -faster
(Sends about 100 packets per second)

#hping3 -1 <target ip> -flood

(Sends packets as quickly as possible)

#hping3 -1 --spoof <target ip> <target broadcast ip> --flood
-1: Use ICMP
--flood: Send packets as quickly as possible
--spoof or -a: Spoof source (victim) IP address

Internet Control Message Protocol (ICMP)

Smurf Attack:
Attacker sends an ICMP echo packet whose source IP is spoofed to be that of a victim system, to the broadcast address. Each system receives the message and floods the target system with ICMP echo response message.
Takes advantage of flooding to overwhelm the victim system with ICMP packets

Countermeasures:
Configure hosts and routers on the network, to ignore directed broadcast requests
This makes it so that addresses that end in ….255 do not rebroadcast the message to all systems on the network
Cisco router: R1(config-if)# no ip directed-broadcast
Linux Hosts: add net.ipv4.icmp_echo_ignore_broadcasts = 1 to /etc/sysctl.conf file

For weaker servers, ignore ICMP packets (via ping) altogether

Firewalling

• What is a firewall?
A firewall is a filtering device on a network that enforces network security policy and protects the network against external attacks. All traffic from inside to outside of the network and vice-versa must pass through the firewall. Only traffic authorized by the firewall security policy can pass. Firewalls decide what traffic is allowed in and out of the network based on the predefined security policy.

• According to NIST SP 800-41, what are the characteristics of a firewall?
NIST SP 800-41 standard defines the possible characteristics that a firewall can use to filter traffic.
1. IP Address and Protocol type: filtering based on source/destination IP addresses/ports, traffic direction and other transport layer characteristics (protocol types).
2. Application Protocols: controls access based on application protocol data.
Often used in application firewalls
The firewall is able to look at the HTTP request and response messages and enforce a security policy based on that.
3. User Identity: controls access based on user identity

Often used in application firewalls
Example: filtering SMTP email protocol data for spam messages
4. Network Activity: controls access based on network activity characteristics (e.g., time of the request)

Firewall capabilities: Define a traffic choke point in the network and protects against IP spoofing and routing attacks
Provide a location for monitoring the security events
Provide non-security functions: logging internet usage, network address translation (NAT)
Serve as platform for VPN/IPSec

• What are the limitations of the firewall?
A firewall cannot protect against attacks that bypass the firewall (e.g., connections from inside the organization to the outside that do not go through the firewall) and internal threats.

• What is a packet filter firewall? Be able to write and interpret rules and to spot configuration flaws.
A packet filtering firewall is a firewall that applies a set of rules to each packet based on the packet headers (has no awareness of higher level constructs such as connections).

Filters based on:
Source/destination IP
Source/destination port numbers
IP Protocol Field: defines the transport protocol
Interface: for firewalls with 3+ network interfaces, the interface from which the packet came from/going to

• What is the difference between the default and allow and default deny policies? Which one is the more secure one?
When no rules apply to a packet, a default rule is applied:
Default deny: what is not explicitly permitted is denied (Deny EVERYTHING)
Default forward: what is not explicitly denied is allowed (Allow all packets that are not specifically denied)

Default deny is the more secure option, preferred in the real world but is less flexible.

• Be able to configure the packet filtering functions of iptables.
“iptables --list” to see current iptable
“iptables --flush” to clear all rules

Chain INPUT are rules that are applied to packets entering your system.
Chain FORWARD is used for packet forward. You can configure your system so that when it gets a packet that matches certain rules to forward that packet to another destination.
Chain OUTPUT are rules that are applied to packets leaving your network.

iptables -A INPUT -p icmp -j DROP
-A: append a rule to a chain (in this case append to the input chain)
-p: specifies the protocol name (in this case it is ICMP which is used for pinging)
-j: what to do with the packet (in this case drop the packet)
There are three options with -j:
Drop the packet
Reject the packet and send an error to the sender notifying that the packet was dropped
Accept the packet

-D <which table to delete from> <rule number>: delete rule from the iptable

– Example: Write iptables rules to block all ICMP traffic to and from the system.
iptables -A OUTPUT -p icmp -j DROP
iptables -A INPUT -p icmp -j DROP

– Example: Write iptables rules to block all traffic on port 22
iptables -A INPUT -p any --sport 22 -j DROP
-p: any protocol
-sport <port number>: source port number

iptables -A OUTPUT -p any --sport 22 -j DROP

– Example: Write iptables rules to block traffic to host 192.168.2.2
iptables -A OUTPUT -p tcp --dest 192.168.2.2-j DROP
--dest <ip address>: destination ip address

iptables -A INPUT -p tcp --sport 192.168.2.2-j DROP

--dport: specifies the destination port

• What are the limitations of the packet filter firewall?
The packet filtering firewall cannot examine upper layer data (cannot prevent attacks that employ application-specific vulnerabilities or functions). It cannot examine application layer headers. The packet filter firewall can also be fooled by IP spoofing.

• What is the stateful firewall and how does it compare to a packet filter?
A stateful firewall is a firewall that is aware of connections. This firewall can examine packets in the context of which they are a part of. The firewall can enforce rules on the connections. Stateful firewalls maintain a directory of inbound/outbound TCP connections. Stateful firewalls allow us to define rules based on connections (e.g. no inbound connections on port 22).

• What is the application-level firewall? What are its advantages and limitations?

An application-level firewall (application-level proxies) is a firewall that runs on the application layer and is able to examine application-layer data. The firewall has to be created specifically for application layer protocols. The client needs to explicitly connect to the firewall and authenticate in order to be able to access remote systems.

Advantages:
General more secure than packet filters (instead of dealing with many combinations of TCP/IP packets that are allowed or disallowed, focus on a few specific protocols such as FTP)

Limitations:
Increased communications overhead due to two separate TCP connections (application-to-gateway and gateway-to-host)

• What is a circuit-level firewall? What are its advantages and limitations?
A circuit-level firewall is a firewall similar to the application-level gateway where it uses two connections, but it only tracks the state of the TCP/UDP sessions. It does not examine any application data but instead simply relays TCP segments. The firewall allows/denies decisions based on whether a packet belongs to an established and trusted connection.

Advantages:
Does not filter individual packets (simplifies rules)
Fast and efficient

Disadvantages:
Do not filter individual packets (reduces detection capabilities)
Requires frequent updates since the traffic is filtered with rules and policies that need regular updates for new threats and risks
The vendor needs to modify the TCP/IP implementation for their applications to the circuit-level proxy

• What are the different approaches to basing the firewall?
A firewall can be a stand-alone machine. A firewall can also be a software module in routers, switches, servers, or in pre-configured security appliances. A firewall can be software components that run on a host's system.

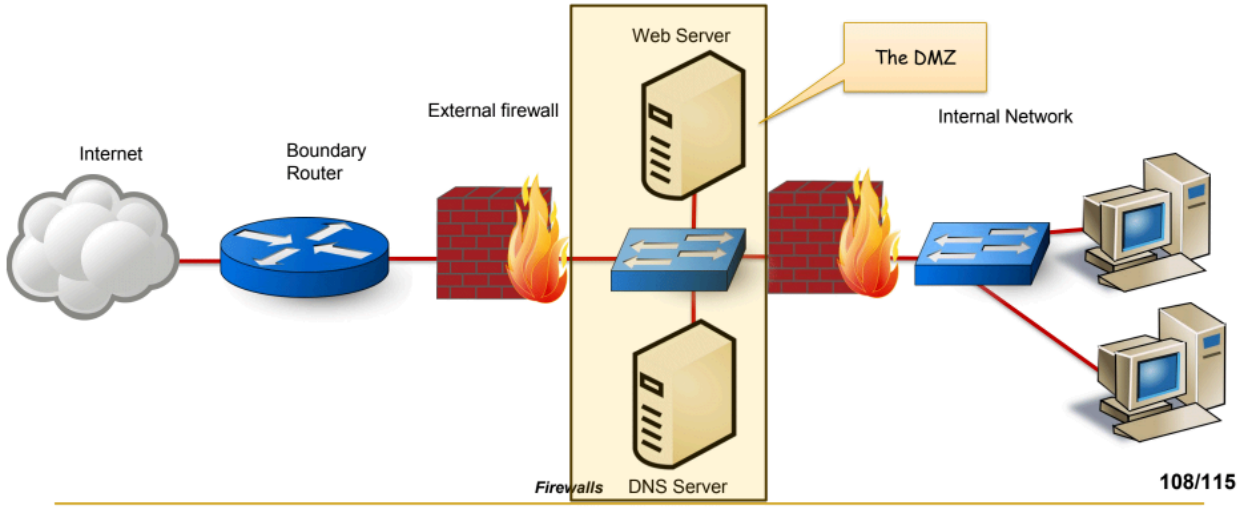
• What are the host-based firewalls?
A host-based firewall is a firewall software module used to secure a single host (e.g. ufw or iptables). It is a firewall dedicated to firewalling all incoming and outgoing traffic. This firewall has a very detailed view into your system so the firewall can enforce more powerful security policies (e.g. you can specify security policies so that certain applications can only send packets to certain IP addresses). A host-based firewall does not get affected when the network topology changes.

• What are the network device firewalls?

A network device firewall is a firewall that runs as a part of a firewall or a device dedicated as a firewall.

• What are the virtual firewalls?
A virtual firewalls are firewalls that are used in virtualized environments.

• What is the DMZ? How is it used for securing networks?
DMZ is the demilitarized zone. It is used to secure networks by separating the servers from the internal network. This is done by having an extra external firewall to protect the systems in the DMZ against threats. Another firewall separates the DMZ from the internal network.



• What are the advantages and disadvantages of having the two DMZ firewalls be from different vendors?
The DMZ is used to host public facing systems. The public systems are protected from the outside world by the external firewall. The external firewall will have a looser set of rules while the internal firewall will have much stricter policies.

The internal firewall has three roles:
Filters more strictly than the external firewall to defend the network from outside attacks
Shields the network and the DMZ from attacks from each other, which could come from malware in the DMZ or the network
Separates parts of the network from each other for more security.

• Be able to write pfSense firewall rules.

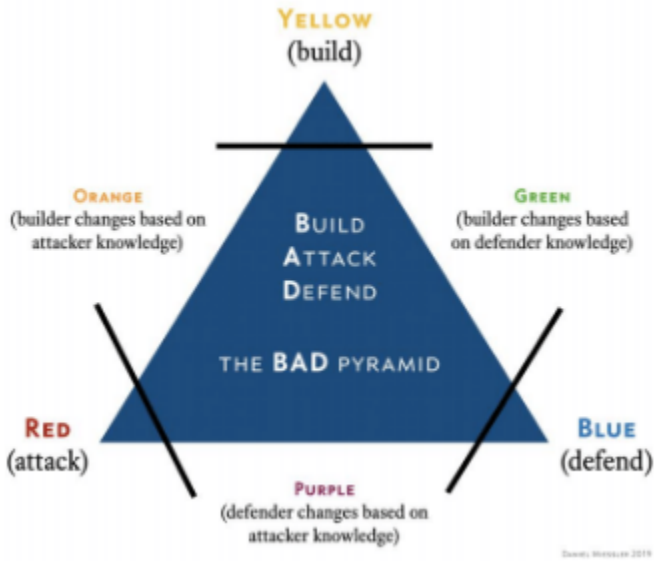
Penetration Testing

https://www.dropbox.com/scl/fi/8qr8f0ubkndeuk0vacfgo/Penetration-Testing.pdf?rlkey=s2zunku7dpg2qjz33kekelwz0&e=3&dl=0

• What is penetration testing?
A penetration testing is a legal and authorized attempt to locate and exploit vulnerable systems for the purpose of making those systems more secure.

• What is the objective of penetration testing?
The objective of penetration testing is to see how well the security of systems can hold up against certain tools and techniques used by attackers in order to discover the security vulnerability.

• What is the BAD pyramid?
The BAD pyramid relates to the structure of the company's security teams. The red team are the attackers. The goal of the red team is to attack the company's security systems. The blue team are the defenders. The goal of the blue team is to protect the company against any incoming attacks. The yellow team are the builders. The goal of the yellow team is to create systems and applications.



• Why are the penetration tests conducted?
Penetration tests are conducted to maintain their compliance requirements that need to be met. A company may want to have a stronger understanding of their security footprints (e.g. companies may want to discover weaknesses in network protocols, finding network and software misconfigurations, and software vulnerabilities).

• What is the difference between penetration testing and vulnerability assessment?
A vulnerability assessment is a review of systems to find potential vulnerabilities without attempts at exploitation. On the other hand, penetration testing is finding and exploiting system vulnerabilities as a proof-of-concept.

• What is the difference between black-box, white-box, and grey-box testing.
White Box: penetration tester is given access to all information about the system being tested.

Advantage: very thorough
Disadvantage: not completely realistic; the tester is not in the same position as the attacker, who typically starts with little to no information about the system

Black Box: penetration tester is given no information about the system.
Advantage: realistic; the tester is in the same position as an attacker.
Disadvantage: lack of knowledge of the system's inner workings, precludes the tester from testing some areas of the system.

Grey Box: A combination of white box and black box.
Attacks may have access to certain systems.

• What is the difference between ethical and unethical hackers?
Ethical hackers obtain authorization from the organization whose systems they plan to attack.
Unethical hackers attack without authorization.

• Know the stages of penetration testing and the importance of following a structured approach.
– Example: What is the difference between passive and active reconnaissance?
Stage 1: Reconnaissance: Gathering information about the target organization
Passive: gathering information about the target from publicly available resources. (e.g., Google-Fu, twitter pages of employees, pastebin posts, domain registries, etc.)
Active: using tools to interrogate the hosts of the target organization (not always legal without authorization! e.g., social engineering, nmap, etc.)

Stage 2: Scanning: scanning hosts of the target organization for:
• Open ports
• Vulnerable applications and systems
• Weak protection of transmitted data
• Mapping the topology of the network.

Stage 3: Exploitation: Gain access to the targeted resources!
• Obtain sensitive information
• Compromise the target and use to launch attacks against other targets (e.g., Metasploit Framework)

Stage 4: Post-Exploitation and Maintaining Access: Maintaining access to the compromised system across system reboots using SSH backdoor; Maintaining access to the compromised system:
• Establishing the value of the information on the compromised system.
• Maintaining access across system reboots.
• Cover tracks
• Clear logs
• Encrypt backdoor traffic
• Remove traces of exploitation

• Use rootkit to evade detection
• Use commonly used ports to mask traffic
• Use anonymization methods such as TOR, proxy, or VPN

Stage 5: Submit Written Reports Documentation includes:
• Vulnerability reports
• Proof-of-concept reports

• Be able to use the penetration testing tools discussed in class.