

**Deliverable 2 – Network Security Vulnerabilities**

**Group - 2  
Members:**

**Bhargav Gosai (100902330)**

**Shweta Kestwal (100900888)**

**Priyanshu Shah (100897637)**

**Manjot Kaur (100896951)**

**Course: INFT1100  
Professor: Chris Whidden**

Network Vulnerability 1:

**Segmentation of servers:**

One major problem in current network is that web server and data server are on same subnet which makes entire network vulnerable if an attacker manages to hack into web server. Not only attacker can travel across the network pretty easily but can misconfigure the network and steal the sensitive information. Attacks that can occur due to lack of segmentation of server are listed below.

* Privilege escalation
* Data theft
* Insider attacks

1. Privilege escalation: If the attacker gains access of web server, they can use that access to escalate their privilege to gain access of data server and steal or alter information or can compromise entire system.
2. Data theft: If web server is compromised, all other servers would be at risk too as travelling through same subnet will be easy for the attacker and the attacker can easily steal any data available on our servers.
3. Insider attacks: segregation pf duties might prove to be useless if segmentation of network is not done correctly, in this case an employee with web server access can also access data server easily if they want to which is not a good practice for an organization.

Security standards to follow: The solution for this situation is to follow ISO 27001 A 13.1 Network Security Management standard which states that all and any public accessible domains should be inside a De-Militarized zone (DMZ) and the internal LAN should be behind a firewall protection. The idea behind this is that assuming attacker compromises and breaks into our web server, he or she still might not be able to break into our LAN since it is separated from public servers and that way damage can be minimum.

Network Vulnerability 2:

**Open Ports:**

Open ports may not be that big of an issue but considering the situation of our servers we need to make sure that firewalls and ports are not misconfigured. If an attacker gains access to the network, open ports may provide him an easy way to navigate around the network or allow malicious traffic to pass through.

Poorly configured ports may lead to attacks such as:

* Brute force attacks
* Man-in-the-middle attacks
* Malware infections
* Remote code execution attacks

1. Brute force attacks: Attacker can try to use open ports to log into employee accounts by using automated tools to guess login credentials of employees.
2. Man-in-the-middle attacks: Attacker can intercept the traffic passing through these open ports and sensitive information can be compromised.
3. Malware infections: Attacker can use these open ports ton inject virus, trojan or worms into our network.
4. Remote code execution: Similar to malware infection, attacker can also inject codes that can give him unauthorized access and compromise the privacy of network and information.

Security standards to follow: To mitigate the risk related to open ports we should follow the ISO 27001 A 8.20 Network Security Control standard which indicates that network and network devices should be secured, managed and controlled to protect the information in network and other facilities from compromise via network. The standards covers various aspects such as establishing controls to safeguard assets, maintaining up to date documentation of network diagrams and configuration files of devices, logging and monitoring, use of firewalls, hardening network devices, detecting and filtering systems connections to the network, etc.

**2. Describe the below configurations  
 a. Password and lockout configuration**

i. Actual CLI commands to configure

* Switch Configuration

S1(config)# line console 0

S1(config-line)# password Contoso@123

S1(config-line)# login

S1(config-line)# exit

S1(config)# enable password Cisco@123

S1(config)# exit

S1# config t

S1(config)# enable secret Contoso@245

S1(config)# exit

S1# conf t

S1(config)# service password-encryption

S1(config)# login block-for 60 attempts 3 within 60

S1(config)# exit

* Router Configuration

R1(config)# line console 0

R1(config-line)# password Contoso@123

R1(config-line)# login

R1(config-line)# exit

R1(config)# enable password Cisco@123

R1(config)# exit

R1# config t

R1(config)# enable secret Contoso@245

R1(config)# exit

R1# conf t

R1(config)# service password-encryption

#### R1(config)# banner motd "Unauthorized Access Prohiited!"

R1(config)# login block-for 60 attempts 3 within 60

R1(config)# exit

**Explanation:**

In order to secure the Contoso network, we'll start by enabling the password on the console so that whenever a user wants to log in to the system, they must input the password to confirm whether they are a verified user or not. Next, in order to improve security, we will enable the password for privileged mode, which details the unique privileges granted to particular users, such as administrators or other senior level users. After enabling this, we will now encrypt the password using enable secret, which will replace the original text with a new encrypted password. You can verify this by executing the show run command. The enable and console passwords are still in plain text even if the password for access privilege mode has been encrypted. To encrypt both passwords, use the service encryption command. And we will add the message of the day for unauthorized users, so whenever any unauthorized person tries to access to the network, they will get the warning message "Unauthorized Access Prohibited. Additionally, we will block logins by suspending the network for 60 seconds and denying access to anyone who makes more than three unsuccessful attempts by using login block command. This will help us to protect from brute-force attack.

**b. Port Security**  
 i. Access Port Workstations

S1# conf t

S1(config)# interface GigabitEthernet0/1

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 1

S1(config-if-range)# switchport port-security mac-address sticky

S1(config-if-range)# switchport port-security violation restrict

S1(config-if-range)# spanning-tree portfast

S1(config-if-range)# end

ii. Access Port Servers

S1# conf t

S1(config)# interface GigabitEthernet0/2

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 4

S1(config-if-range)# switchport port-security mac-address sticky

S1(config-if-range)# switchport port-security violation restrict

S1(config-if-range)# spanning-tree portfast

S1(config-if-range)# end

iii. Access Port Not used

S1# conf t

S1(config)# interface GigabitEthernet0/3

S1(config-if-range)# switchport mode access

S1(config-if-range)# switchport port-security

S1(config-if-range)# switchport port-security maximum 1

S1(config-if-range)# switchport port-security violation shutdown

S1(config-if-range)# end

**Explanation:**

We will now enable security on the ports after enabling security on the switch and router. We will thus use switchport mode for that, which switches the port into an access port to connect to workstations and other endpoints. The port security will then be enabled, limiting the number of MAC addresses to prevent DDOS attacks and unauthorized access. We will also set the maximum number of MAC addresses that can connect to the port in order to restrict the MAC address. In addition, we will add the sticky MAC address to safeguard the network. By doing this, the switch will be able to discover the MAC address, and if it is secure, it will store it in memory as a secure MAC address. Also, we will provide the Violation Restrict command, which will close the port whenever a violation occurs, to limit the breach. In order to quickly recover the port after shutdown, we use the portfast command. This will enable the ports to enter a forwarding state without waiting for STP or get stuck in loops. By doing this, the connection time to the port will be reduced.

**c. Router Hardening**

R1>enable

R1#configure terminal

R1(config) #username admin privilege 15 Contoso@123

R1(config) #line vty 0 15

R1(config) #login local

R1(config) #no service finger

R1(config) #no service pad

R1(config) #no service tcp-small-servers

R1(config) #no service udp-small-servers

R1(config) #ip inspect name MYFW http

R1(config) #ip inspect name MYFW ftp

R1(config) #ip access-list extended MYACL

R1(config) #permit tcp any any eq www

R1(config) #permit tcp any any eq ftp

R1(config) #interface GigabitEthernet0/0

R1(config) #ip access-group MYACL in

R1(config) #service password-encryption

R1(config) #enable password Contoso@123

R1(config-if) #line console 0

R1(config-if) #password Contoso@123

**Explanation:**

Here we disabled redundant services and setting up access control for certain traffic. We have also turned on password encryption and enabled the admin password. Moreover, we have configured IP inspection to monitor traffic and filter unwanted traffic.

**d. Route to the internet**

**i.** ACL for network

R1(config) #access-list 1 permit 10.2.8.4 0.0.0.63

R1(config) #access-list 1 deny any

R1(config-if) #interface GigabitEthernet0/0

R1(config-if) #ip address 192.168.2.1 255.255.255.0

R1(config-if) #ip access-group 2 in

**Explanation:**

We'll implement the access control list to lessen network traffic. We will then apply this traffic to one interface of the router that is configured with the IP address, define the subnet mask, grant the permit to route the traffic, and refuse all other traffic on the network. This will help us in preventing unauthorized traffic and network access. Moreover, it can be used to filter traffic and block particular ports or protocols, which will reduce attacks performed by malicious sources.

**ii.** Primary and backup default route to the internet

R1(config) #ip route 192.168.2.57 255.255.255.0 10.2.8.0

R1(config) # ip route 0.0.0.0 0.0.0.0 192.168.2.57

R1(config) # router ospf 2

R1(config-router)# default-information originate

**Explanation:**

To avoid network failures, we will use primary and backup default route. So, in case the primary route fails the backup route will help us to ensure the continuous internet connectivity. This can help to assure continuity of operations and prevent network service disruptions.

**e. Access control list**

R1(config) #access-list 1 permit 10.2.8.0 0.0.0.63

R1(config) #access-list 2 permit 10.2.11.0 0.0.0.254

R1(config) #access-list 3 permit 10.2.32.0 0.0.0.63

R1(config) #access-list 4 permit 10.2.27.0 0.0.0.31

R1(config) #access-list 5 permit 10.2.2.0 0.0.0.63

R1(config) #access-list 6 permit 10.2.5.0 0.0.0.255

R1(config) #access-list 7 permit 10.2.18.0 0.0.0.63

R1(config) #access-list 8 permit 10.2.24.0 0.0.0.254

R1(config) #interface GigaBitEthernet0/0

R1(config-if) #ip access-group 1 in

R1(config-if) #ip access-group 8 out

R1(config-if) #interface GigabitEthernet0/1

R1(config-if) #ip access-group 2 in

R1(config-if) #interface GigabitEthernet0/2

R1(config-if) #ip access-group 3 in

R1(config-if) #interface GigabitEthernet0/3

R1(config-if) #ip access-group 4 in

R1(config-if) #interface GigabitEthernet1/0

R1(config-if) #ip access-group 5 in

R1(config-if) #interface GigabitEthernet1/1

R1(config-if) #ip access-group 6 in

R1(config-if) #interface GigabitEthernet1/2

R1(config-if) #ip access-group 7 in

**Explanation:**

Here we filtered the in and out traffic for different subnets and work as end points for users. Different subnets are given access to different interfaces thus reducing the risk of unauthorized access.