NETWORK SECURITY AUDIT REPORT

IIS CISC Workshop

Submitted By:

Prakhar Hans

Sai Krishna

Scope of Work

A simulated network, created in Cisco Packet Tracer, was audited for common and basic vulnerabilities. After analysis of the results, this network would be classified as having low-level security. There are five systems, with vulnerabilities. It is strongly recommended that these vulnerabilities be addressed, since these represent where the majority of basic attacks occur.

The major vulnerability found, is the absence of any Access Control Lists on some of the routers. Another key additional problem is that the routers are not password protected. This list includes several systems with vulnerabilities. It is recommended that this audit be re-performed after the name servers are cleaned up and identifiable vulnerabilities addressed.

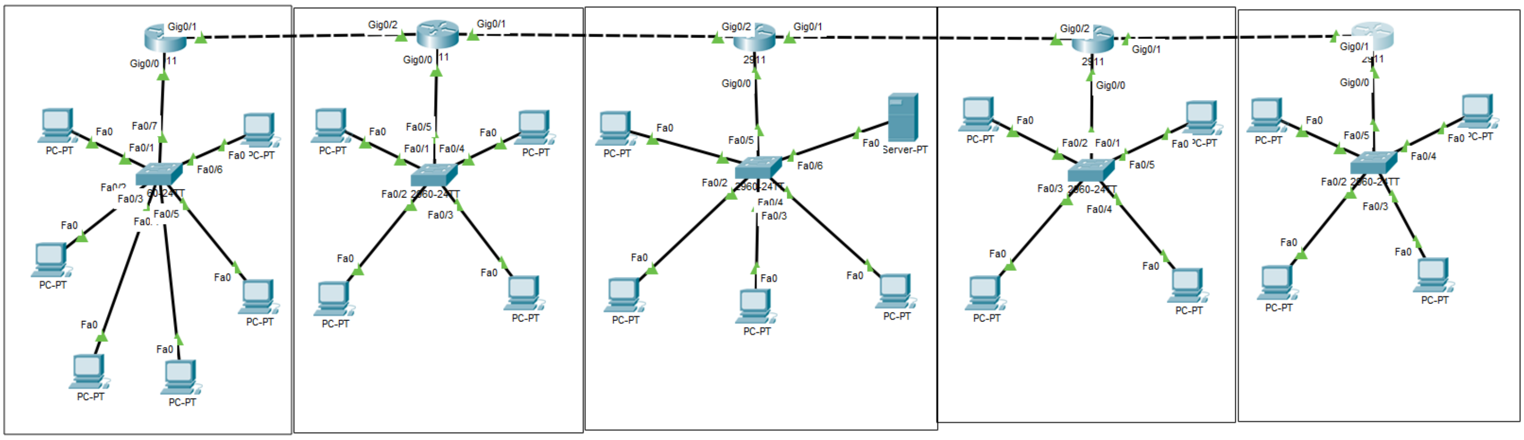
A number of vulnerabilities, oversights and mistakes appear to be a result of lack of follow-up or good training on procedures with the technical staff. These are detailed further in the main body of the report.

Standard & Framework

The software used for the Simulation of the network:

Cisco Packet Tracer 7.2.1.0218

Infrastructure of the Network created:



R1
10.0.0.0

R1 -> R2
20.0.0.0

R2
30.0.0.0

R2 -> R3
40.0.0.0

R3
50.0.0.0

R3 -> R4
60.0.0.0

R4
70.0.0.0

R4 -> R5
80.0.0.0

R5
90.0.0.0

Type of Assessment

For the assessment of the simulated network, in order to figure out the security configuration, the configuration of all the devices was checked (i.e. routers and switches) This was done to figure out the presence/absence of all the necessary basic security features.

Basic Security features that was required:

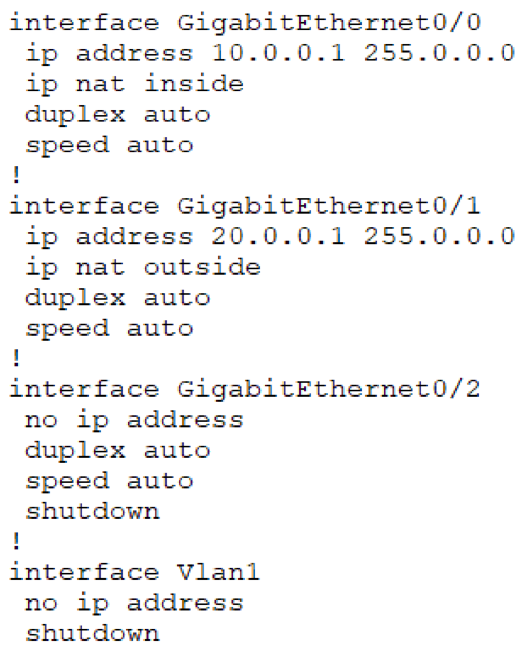
- Port Security on the routers, to allow/deny certain number of ports on the switches.
- Access Control Lists on the routers, to filter the unauthorized packets inside a certain network

Approach

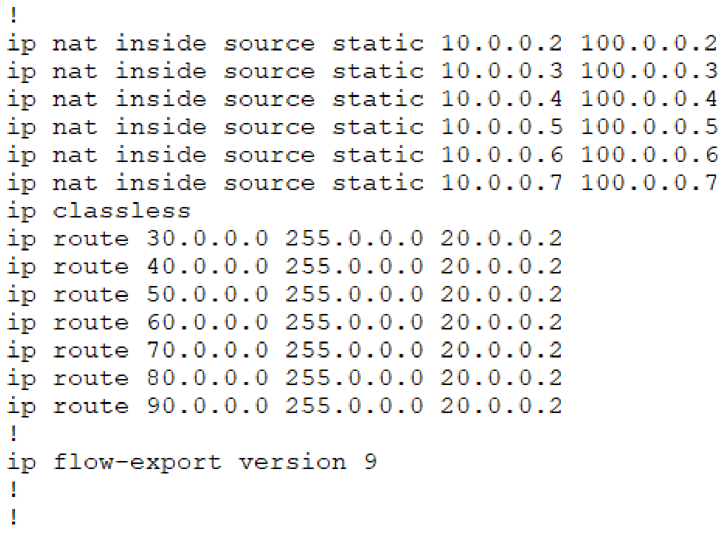
The audit is performed by checking the configuration of all the different routers to see all the security features that were applied on them.

Following are the configurations of all the Routers, and the Switches connected in their network, along with the details of all the particular security features applied on the corresponding devices. This configuration is found out by running the command **'`sh running_config`'**.

Router 1 (R1):

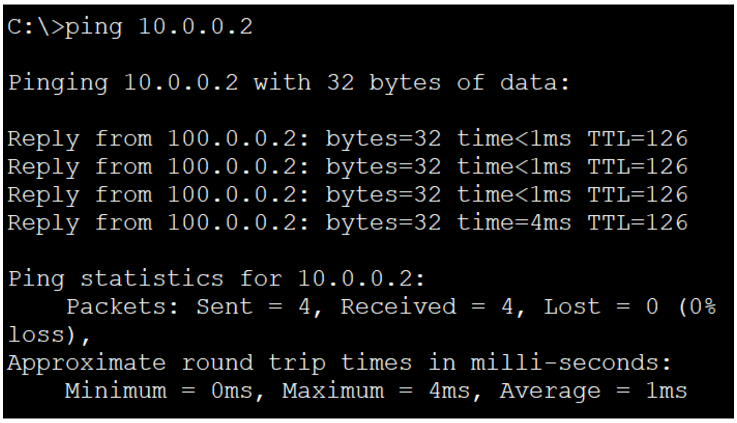


```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.0.0.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 20.0.0.1 255.0.0.0
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
```



```
!
ip nat inside source static 10.0.0.2 100.0.0.2
ip nat inside source static 10.0.0.3 100.0.0.3
ip nat inside source static 10.0.0.4 100.0.0.4
ip nat inside source static 10.0.0.5 100.0.0.5
ip nat inside source static 10.0.0.6 100.0.0.6
ip nat inside source static 10.0.0.7 100.0.0.7
ip classless
ip route 30.0.0.0 255.0.0.0 20.0.0.2
ip route 40.0.0.0 255.0.0.0 20.0.0.2
ip route 50.0.0.0 255.0.0.0 20.0.0.2
ip route 60.0.0.0 255.0.0.0 20.0.0.2
ip route 70.0.0.0 255.0.0.0 20.0.0.2
ip route 80.0.0.0 255.0.0.0 20.0.0.2
ip route 90.0.0.0 255.0.0.0 20.0.0.2
!
ip flow-export version 9
!
!
```

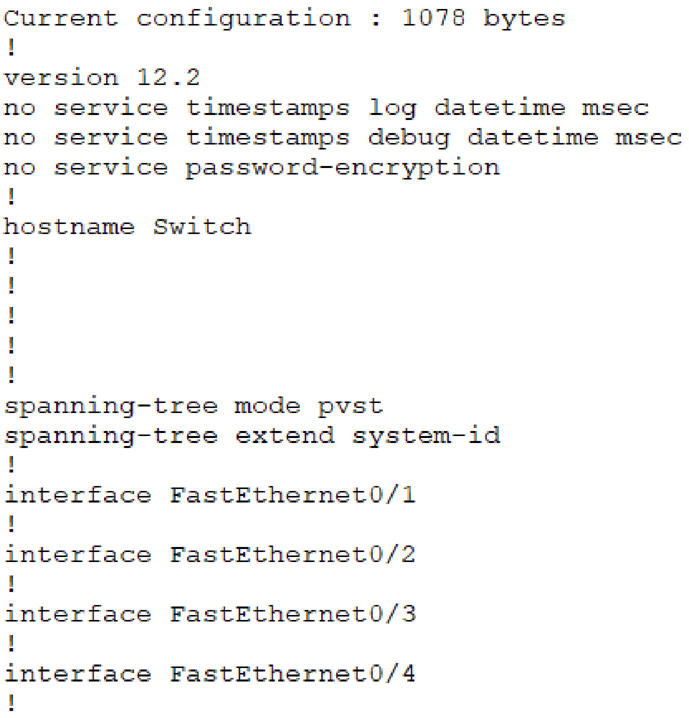
1. The configuration of Router 1 shows us that this particular router has Static NAT configured on it that connects to the public network (100.0.0.0).
   The following picture shows that when pinged from any outside network, the response is sent from the translated Public IP address, instead of the assigned private IP address.



```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 100.0.0.2: bytes=32 time<1ms TTL=126
Reply from 100.0.0.2: bytes=32 time<1ms TTL=126
Reply from 100.0.0.2: bytes=32 time<1ms TTL=126
Reply from 100.0.0.2: bytes=32 time=4ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

2. The connection is properly routed to all the rest of the networks in the simulation.
3. There is **No Access Control List** configured on this router.
4. There is **No Password Protection** on this router.

Switch 1:



```
Current configuration : 1078 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
```

1. The configuration of Switch 1 is basic, with nothing extra security features configured on it.

Router 2 (R2):

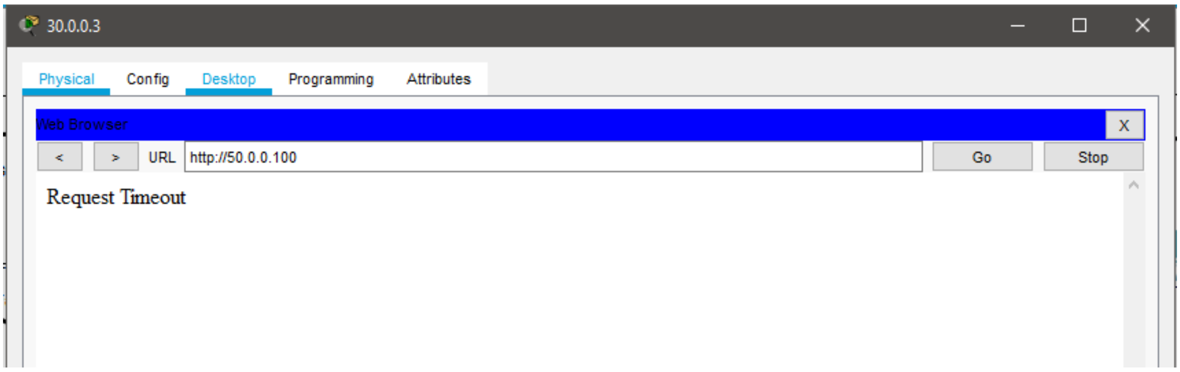
```
interface GigabitEthernet0/0
 ip address 30.0.0.1 255.0.0.0
 ip access-group 110 in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 40.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 20.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
```

```
ip classless
ip route 10.0.0.0 255.0.0.0 20.0.0.1
ip route 50.0.0.0 255.0.0.0 40.0.0.2
ip route 60.0.0.0 255.0.0.0 40.0.0.2
ip route 70.0.0.0 255.0.0.0 40.0.0.2
ip route 80.0.0.0 255.0.0.0 40.0.0.2
ip route 90.0.0.0 255.0.0.0 40.0.0.2
!
ip flow-export version 9
!
!
access-list 110 deny tcp host 30.0.0.3 host 50.0.0.100 eq www
access-list 110 permit tcp any any
access-list 110 permit icmp any any
!
!
!
```

1. The configuration of Router 2 is basic with no address translation.
2. The connection is properly routed to all the rest of the networks in the simulation.
3. There is an Extended-type Access Control List configured on the port GigabitEthernet0/0 for the inside traffic.

   The ACL rule on this router denies all the http requests from one IP address in the network (30.0.0.3) to an IP address in the network 50.0.0.0 (specifically to the IP 50.0.0.100). All other traffic is permitted.

   The following picture shows that when the http server (50.0.0.100) is accessed from the IP address in this network (30.0.0.3), the connection is dropped.

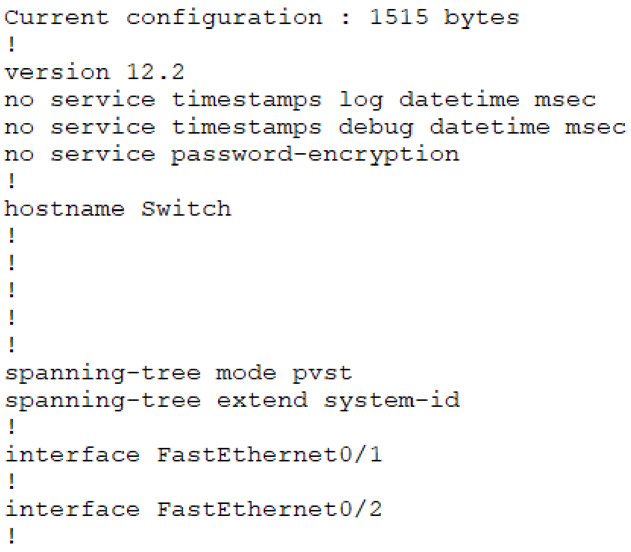


URL: http://50.0.0.100

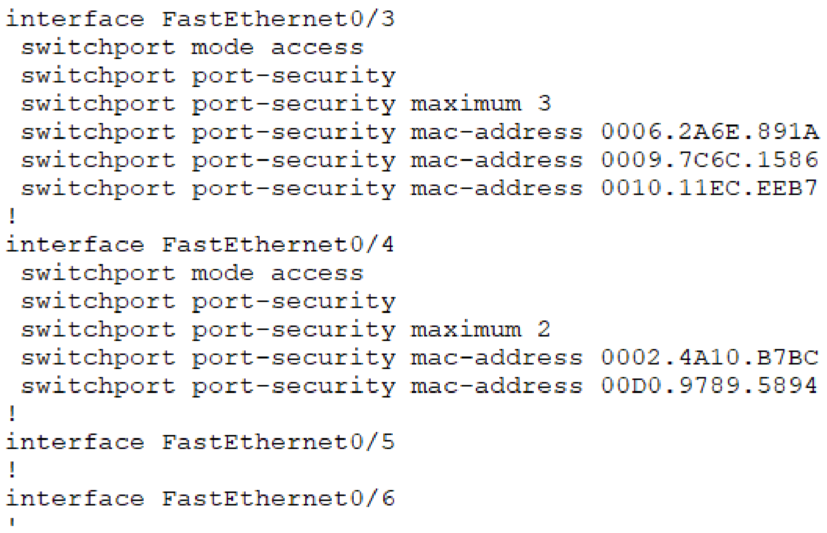
Request Timeout

4. There is **No Password Protection** on this router.

Switch 2:

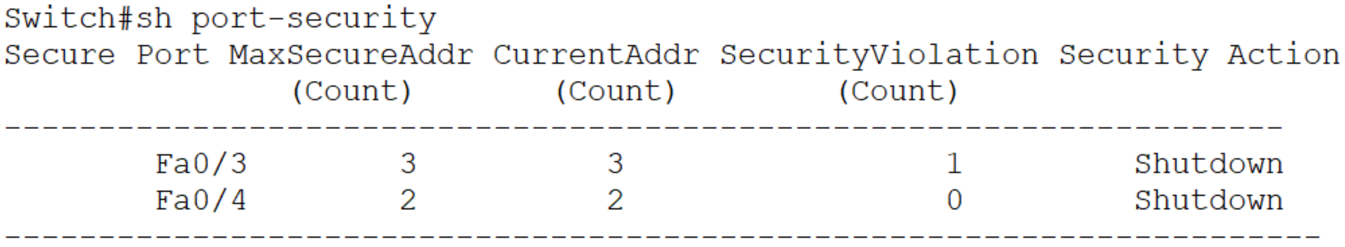


```
Current configuration : 1515 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
```



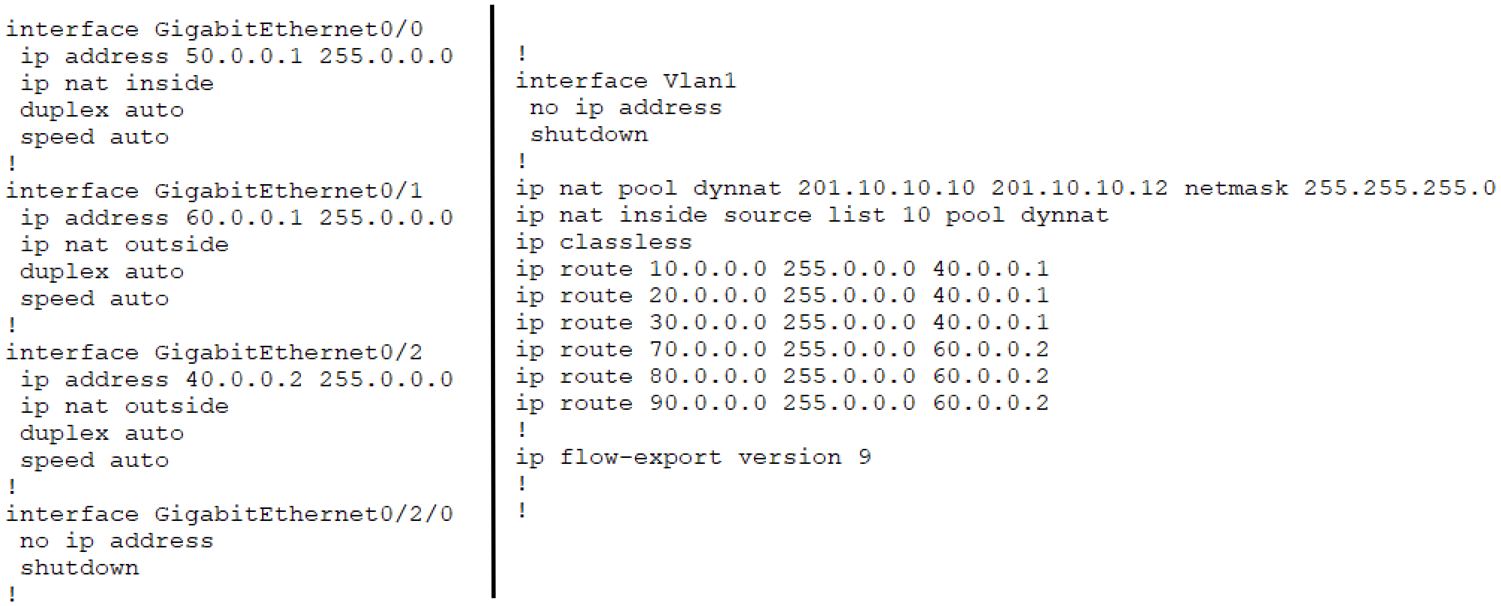
```
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address 0006.2A6E.891A
 switchport port-security mac-address 0009.7C6C.1586
 switchport port-security mac-address 0010.11EC.EEB7
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address 0002.4A10.B7BC
 switchport port-security mac-address 00D0.9789.5894
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
```

1. The configuration of Switch 2 is basic, along with Port Security configured on two ports, i.e. FastEthernet0/3 and FastEthernet0/4
2. The Port-Security rule on port FastEthernet0/3 allows a maximum connection of 3 MAC addresses. The MAC addresses are non-sticky and are specified by the administrator of the network.
3. The Port-Security rule on port FastEthernet0/4 allows a maximum connection of 2 MAC addresses. The MAC addresses are non-sticky and are specified by the administrator of the network.
4. The following picture shows the number of attacks tried on this machine which were stopped because of the configuration of Port-Security. (Command: **`sh port_security`**)



```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/3        3           3                 1         Shutdown
        Fa0/4        2           2                 0         Shutdown
----------------------------------------------------------------------
```

Router 3 (R3):

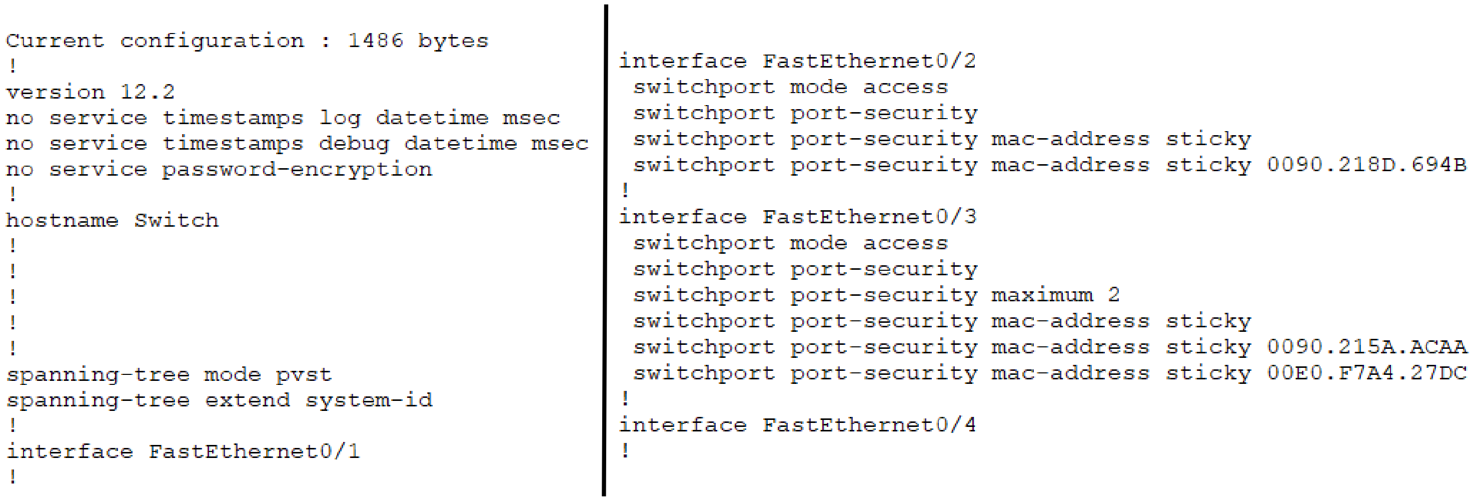


```
interface GigabitEthernet0/0
 ip address 50.0.0.1 255.0.0.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 60.0.0.1 255.0.0.0
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 40.0.0.2 255.0.0.0
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2/0
 no ip address
 shutdown
!
```

```
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool dynnat 201.10.10.10 201.10.10.12 netmask 255.255.255.0
ip nat inside source list 10 pool dynnat
ip classless
ip route 10.0.0.0 255.0.0.0 40.0.0.1
ip route 20.0.0.0 255.0.0.0 40.0.0.1
ip route 30.0.0.0 255.0.0.0 40.0.0.1
ip route 70.0.0.0 255.0.0.0 60.0.0.2
ip route 80.0.0.0 255.0.0.0 60.0.0.2
ip route 90.0.0.0 255.0.0.0 60.0.0.2
!
ip flow-export version 9
!
!
```

1. The configuration of Router 3 is basic with Dynamic NAT configured that translates the private IP into Public IP network 201.10.10.0 with the IP pool of 200.10.10.10 to 201.10.10.12
   The following picture shows that when pinged from any outside network, the response is sent from the translated Public IP address, instead of the assigned private IP address.
2. The connection is properly routed to all the rest of the networks in the simulation.
3. There is **No Access Control List** configured on this router.
4. There is **No Password Protection** on this router.

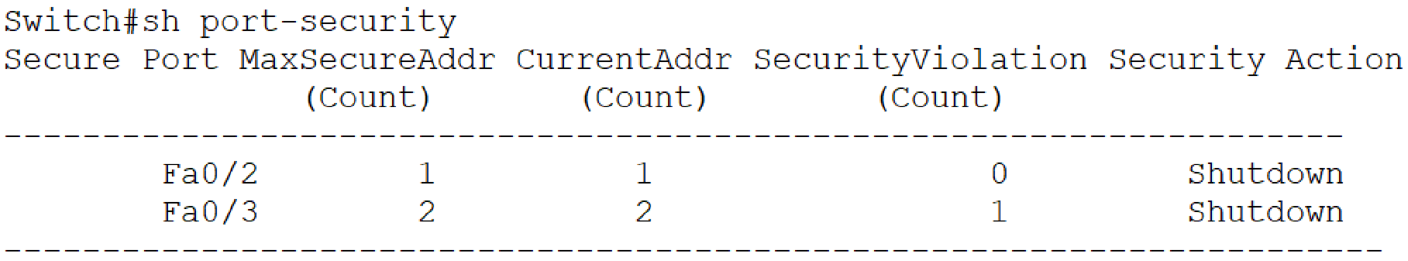
Switch 3:



```
Current configuration : 1486 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
```

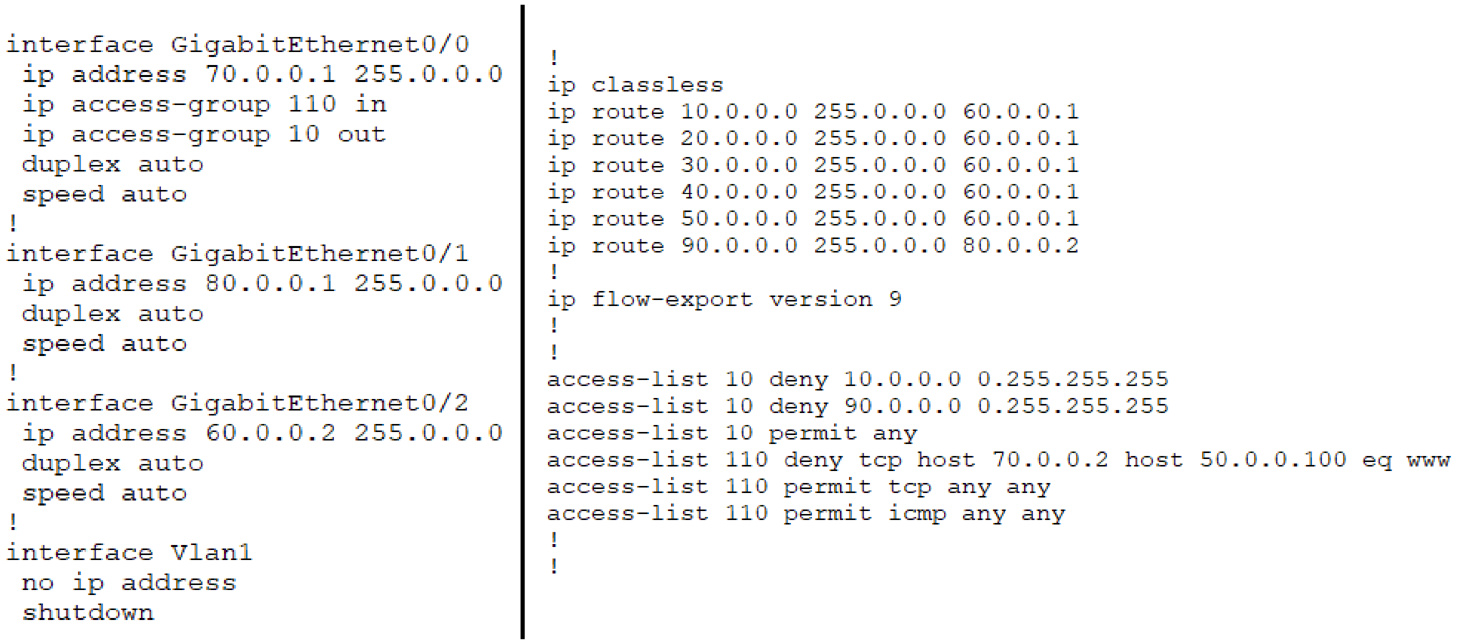
```
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.218D.694B
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.215A.ACAA
 switchport port-security mac-address sticky 00E0.F7A4.27DC
!
interface FastEthernet0/4
!
```

1. The configuration of Switch 3 is basic, along with Port Security configured on two ports, i.e. FastEthernet0/2 and FastEthernet0/3
2. The Port-Security rule on port FastEthernet0/2 allows a maximum connection of 1 MAC address. The MAC address is sticky.
3. The Port-Security rule on port FastEthernet0/4 allows a maximum connection of 2 MAC addresses. The MAC addresses are sticky.
4. The following picture shows the the number of attacks tried on this machine which were stopped because of the configuration of Port-Security.



```
Switch#sh port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/2        1           1                0          Shutdown
        Fa0/3        2           2                1          Shutdown
----------------------------------------------------------------------
```

Router 4 (R4):



```
interface GigabitEthernet0/0
 ip address 70.0.0.1 255.0.0.0
 ip access-group 110 in
 ip access-group 10 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 80.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 60.0.0.2 255.0.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
```

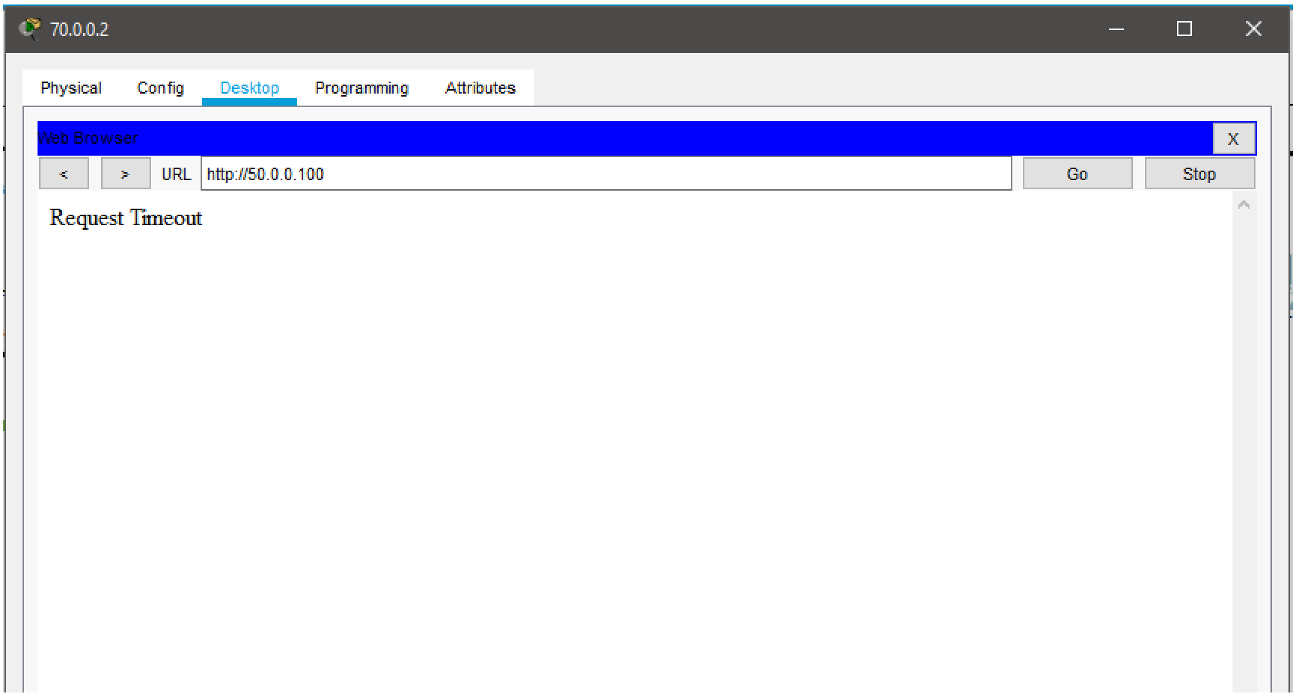
```
!
ip classless
ip route 10.0.0.0 255.0.0.0 60.0.0.1
ip route 20.0.0.0 255.0.0.0 60.0.0.1
ip route 30.0.0.0 255.0.0.0 60.0.0.1
ip route 40.0.0.0 255.0.0.0 60.0.0.1
ip route 50.0.0.0 255.0.0.0 60.0.0.1
ip route 90.0.0.0 255.0.0.0 80.0.0.2
!
ip flow-export version 9
!
!
access-list 10 deny 10.0.0.0 0.255.255.255
access-list 10 deny 90.0.0.0 0.255.255.255
access-list 10 permit any
access-list 110 deny tcp host 70.0.0.2 host 50.0.0.100 eq www
access-list 110 permit tcp any any
access-list 110 permit icmp any any
!
!
```

1. The configuration of Router 2 is basic with no address translation.
2. The connection is properly routed to all the rest of the networks in the simulation.
3. There is a Standard-type Access Control List configured on the port GigabitEthernet0/0 for the outside traffic. The ACL rule on this port denies any traffic originating from the networks 10.0.0.0 and 90.0.0.0 and travelling to the network 70.0.0.0. All other traffic is permitted.

   There is an Extended-type Access Control List configured on the port GigabitEthernet0/0 for the inside traffic.

The ACL rule on this port denies all the http requests from one IP address in the network (70.0.0.2) to an IP address in the network 50.0.0.0 (specifically to the IP 50.0.0.100). All other traffic is permitted.

4. The following picture shows that when the http server (50.0.0.100) is accessed from the IP address in this network (70.0.0.2), the connection is dropped.



http://50.0.0.100

Request Timeout

5. There is **No Password Protection** on this router.

Switch 4:

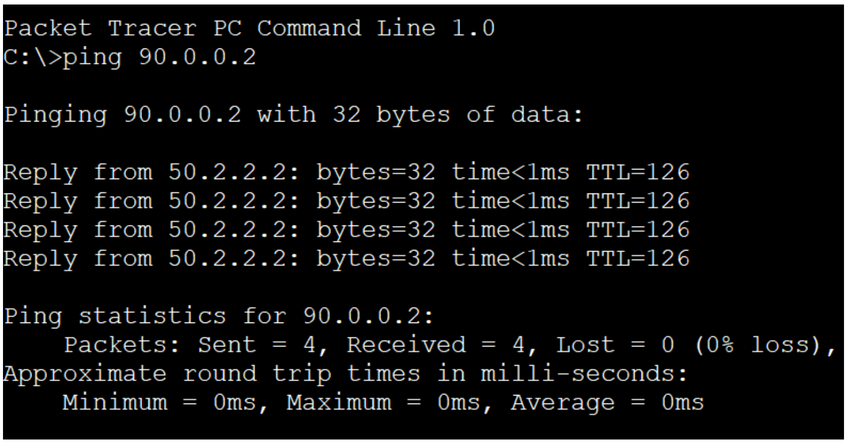
```
Current configuration : 1078 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
```

1. The configuration of Switch 4 is basic, with nothing extra security features configured on it.

Router 5 (R5):

```
!
interface GigabitEthernet0/0
 ip address 90.0.0.1 255.0.0.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 80.0.0.2 255.0.0.0
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip nat pool pat 50.2.2.2 50.2.2.2 netmask 255.255.255.255
ip nat inside source list 55 pool pat overload
ip classless
ip route 10.0.0.0 255.0.0.0 80.0.0.1
ip route 20.0.0.0 255.0.0.0 80.0.0.1
ip route 30.0.0.0 255.0.0.0 80.0.0.1
ip route 40.0.0.0 255.0.0.0 80.0.0.1
ip route 50.0.0.0 255.0.0.0 80.0.0.1
ip route 60.0.0.0 255.0.0.0 80.0.0.1
ip route 70.0.0.0 255.0.0.0 80.0.0.1
!
ip flow-export version 9
!
!
access-list 55 permit 90.0.0.0 0.255.255.255
!
!
```

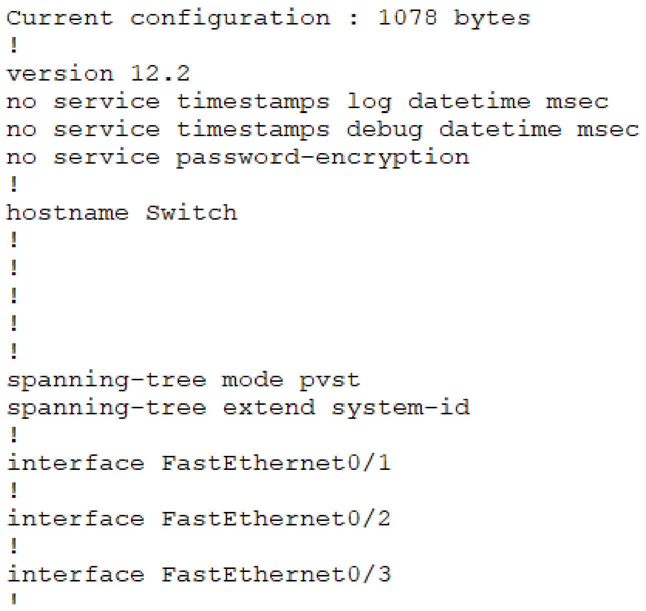
1. The configuration of Router 5 is basic with Port Address Translation configured, that translates the private IP addresses of the network to the pool of Public IP addresses 50.2.2.2. The following picture shows that when pinged from any outside network, the response is sent from the translated Public IP address, instead of the assigned private IP address.



```
Packet Tracer PC Command Line 1.0
C:\>ping 90.0.0.2

Pinging 90.0.0.2 with 32 bytes of data:

Reply from 50.2.2.2: bytes=32 time<1ms TTL=126
Reply from 50.2.2.2: bytes=32 time<1ms TTL=126
Reply from 50.2.2.2: bytes=32 time<1ms TTL=126
Reply from 50.2.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 90.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. The connection is properly routed to all the rest of the networks in the simulation.
3. There is **No Access Control List** configured on this router.
4. There is **No Password Protection** on this router.

Switch 5:



```
Current configuration : 1078 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
```

1. The configuration of Switch 5 is basic, with nothing extra security features configured on it.

Summary of findings:

After completing the audit of the simulation, we have found the following vulnerabilities in the various devices and networks configured in the simulation.

The simulation as a whole has a low-level security.

Router 1 (R1):

Vulnerability	Secure?	Type
Address Translation	Yes	Static NAT
Port Security	No	n/a
Access Control List	No	n/a
Password Protection	No	n/a

Router 2 (R2):

Vulnerability	Secure?	Type
Address Translation	No	n/a
Port Security	Yes	Switch 1 Fa0/3 (Non-Sticky) Fa0/4 (Non-Sticky)
Access Control List	No	n/a
Password Protection	No	n/a

Router 3 (R3):

Vulnerability	Secure?	Type
Address Translation	Yes	Dynamic NAT
Port Security	Yes	Switch 1 Fa0/1 (Admin Assigned MAC) Fa0/4 (Sticky)
Access Control List	Yes	Extended
Password Protection	No	n/a

Router 4 (R4):

Vulnerability	Secure?	Type
Address Translation	No	n/a
Port Security	No	n/a
Access Control List	YES	Standard
Password Protection	No	n/a

Router 5 (R5):

Vulnerability	Secure?	Type
Address Translation	Yes	Dynamic PAT
Port Security	No	n/a
Access Control List	No	n/a
Password Protection	No	n/a