Project Analysis

PREFORMING A VUNERABILITY

ASSEMENT ON A SECURED NETWORK

MATHIAS SOVINE

UNIVERSITY OF ARKON

SPRING 2021

The project proposal was the first completed requirement of the project. The project proposal outlined the proposed initial configurations and design of the project's network. The proposal overviewed the processes for preforming the penetration techniques, exploitations, and securing the network. The project proposal was submitted and accepted. The project network was initially designed to include three routers, one switch, and four computers. The following configurations, tests, and corrections were made for each of the devices on the network.

Router A was connected to and a new login password was created. Router A was designed to provide a connection between Subnet-1 and Router B. Router A was configured to allow Subnet-1 connections to be made to the Router A's LAN interfaces. Router A's WAN port was connected to Router B. Subnet-1 was created for PC-1 to connect to the project's network. Subnet-1's network address was configured to 172.18.0.0/24. The connection between Router A and Router B was configured with the network address 10.0.0.0/30.

Router A's default configuration to allow the WAN port to be the exit port for the default route was kept. Router A was initially configured to use the Routing Information Protocol (RIP). Router A's IPv4 SPI Firewall was enabled. The initial configuration of Router A would not allow ping traffic from PC-1 to Router B or allow ping traffic from Router B to PC-1. Router B did not support RIP. Router A's RIP routing protocol was disabled to allow for traffic to travel between PC-1 and Router B.

PC-1 was updated and upgraded to the latest software packages. OpenVAS was installed and configured. PC-1 was configured to use the static IP address 172.18.0.20/24 and was connected to Router A's LAN 2 port. A ping test was performed between PC-1 and Router A's LAN 2 port. The ping test was successful.

Router B was designed to provide connectivity between Router A and Router B. Router B was configured to provide Network Address Translation (NAT) between Router A and Router C. Router B's WAN port was connected to Router A. The WAN port was configured to use the IP address 10.0.0.2/30. Router B's LAN port 2 was connected to Router C. Router B's LAN port 2 was configured to use the IP address 10.0.0.5/30. Router B was setup to use a static route to provide a route between Router B and the HOME-OFFICE subnet.

The initial configuration of Router B allowed network traffic from Subnet-1 to Router B's WAN port and traffic form the HOME-OFFICE subnet to Router B's LAN port 2, but the initial configuration would not allow traffic to cross-over Router B and allow traffic between Subnet-1 and the HOME-OFFICE subnet to connect. Router B's Network Address Translation was turned off. The ethernet cable connected to Router B's LAN port 2 from Router C was unplugged and plugged into Router B's WAN port. The ethernet cable connected to Router B's WAN port from Router A was unplugged and plugged into Router B's LAN port 2. The IP address for Router B's WAN port was changed to 10.0.0.5/30 and the IP address of Router B's LAN port 2 was changed to 10.0.0.2/30. A ping test was run from PC-3 to PC-1 and from PC-1 to PC-3. The ping tests revealed a successful communication connection.

Router C was designed to provide a connection between the HOME-OFFICE subnet and Router B. An ethernet cable was initially connected between Router B's LAN port 2 and Router C's G0/0 interface. The G0/0 interface was assigned the IP address 10.0.0.6/30. Router C's G0/0 ethernet connection was changed to Router B's WAN port during troubleshooting. Router C's G0/1 interface was setup to use the two sub-interfaces – G0/1.10 and G0/1.20. An ethernet cable initially connected Router C's G0/1 interface with Switch 1's F0/8 interface. The G0/1.10 sub-interface was assigned the IP address 192.168.10.1 and the G0/1.20 sub-interface was assigned

the IP address 192.168.20.1. Router C was configured with a default gateway to exit through the G0/0 interface. Router C was designed to use Network Address Translation for traffic between the G0/1 and G0/0 interfaces. An inbound ACL was created on the G0/0 interface to allow HTTP, HTTPS, and ICMP traffic. An inbound ACL was created on the G0/1.10 sub-interface to allow all traffic. An inbound ACL was created on the G0/1.20 sub-interface to allow only FTP traffic to the WORK VLAN and to allow all traffic to other networks.

The initial configuration of the Network Address Translation prohibited traffic from communicating successfully to Subnet-1. Network Address Translation was removed from Router C. Ping tests were run from PC-4 and PC-3 to PC-1 to test connectivity. The ping tests were successful. The initial configuration of Router C experienced bottlenecking issues between Router C's G0/1 interface and Switch 1's F0/8 interface. The ethernet cable connected to Switch 1's F0/8 interface was unplugged and plugged into Switch 1's G0/0 interface. Simultaneous ping tests were run on PC-1, PC-4 and PC-3 to PC-2 to test the bottleneck issue. The issue was resolved.

Switch 1 was configured to provide VLAN WORK and PLAY designation. Switch 1's f0/1 and f0/2 interfaces were assigned to VLAN 10 or the WORK VLAN. Switch 1's f0/3 interface was assigned to VLAN 20 or the PLAY VLAN. Initially Switch 1's f0/8 interface was configured for trunking VLAN communication between Switch 1 and Router C's G0/1 interface. All unused interfaces were shutdown. A bottleneck issue was detected between Router C and Switch 1's initial configuration. The ethernet cable connected to Switch 1's F0/8 interface was unplugged and plugged into Switch 1's G0/0 interface. Switch 1's G0/0 interface was turned on and Switch 1's f0/8 interface was shutdown.

PC-2 was connected to an internet connected network. Putty, FileZilla Server and OpenVas were installed and configured. PC-2's ethernet port was connected to Switch 1's f0/1 port. PC-2 was configured to use the static IP address 192.168.10.2/24. A ping test was performed between PC-2 and Router C's G0/1.10 sub-interface. The ping test was successful.

PC-3 was connected to an internet connected network. FileZilla Client software was installed and configured. PC-3's ethernet port was connected, using an ethernet cable, to Switch 1's f0/2 port. PC-3 was configured to use the static IP address 192.168.10.3/24. A ping test was performed between PC-3 and Router C's G0/1.10 sub-interface. The ping test was successful.

PC-4 was connected to an internet connected network. FileZilla Client software was installed and configured. PC-4's ethernet port was connected, using an ethernet cable, to Switch 1's f0/3 port. PC-4 was configured to use the static IP address 192.168.20.4/24. A ping test was performed between PC-4 and Router C's G0/1.20 sub-interface. The ping test was successful.

Network ping tests were run on each end device to another end device to verify that ICMP traffic could successfully be transmitted across the network.

Penetration testing was performed on the network. A nmap scan was performed on PC-1 to scan hosts on the WORK and PLAY VLANs. An OpenVAS scan was performed on PC-1 to scan both the WORK and PLAY VLANs. The OpenVAS scan on PC-1 was not successful in reporting vulnerabilities on the WORK and PLAY VLANs. An OpenVAS scan was performed on PC-2 to scan the WORK VLAN. The OpenVAS scan returned eight vulnerabilities. A summary and solutions were provided for each of the eight vulnerabilities. The receiving and sending emails were setup for the phishing email attack.

Vulnerabilities within the network were exploited. A phishing email attacker was performed from PC-1 to convince a user on PC-3 to provide Router B's login credentials. The phishing email attack used a website designed to replicate the login page of Router B. The created website provided a password login prompt where the user of PC-3 submitted the login password to Router B. The submitted login password for Router B was collected by the attacker on PC-1. The attacker on PC-1 connected to the legitimate Router B login page and used the collected credentials to login. The attacker was able to successfully login.

A Windows 7 exploit was performed by an attacker on PC-4 to launch a meterpreter shell session for remote control of PC-3. The payload for the connection was made using msfconsole. The attacker sent the payload to the file server on PC-2 using FileZilla. The user of PC-3 downloaded the payload from PC-2. The user on PC-3 opened the payload. The payload established and opened a meterpreter shell session on PC-4. The attacker on PC-4 was able to download a list of important files on PC-3 to PC-4. PC-4 downloaded and opened a secret formula file.

The initial configuration of Router C's G0/1.20 ACL did not allow files to be uploaded to the file server from PC-4. The FileZilla Server configuration was changed to set the port range for communication to include the ports 55400, 55401, and 55402. Router C was connected to. The ACL on Router C's G0/1.20 interface was changed to allow the ports 55400, 55401, and 55402 for communication. A test file was uploaded from PC-4 to PC-2 to test the configuration. The configuration was successful.

A man-in-the-middle attack was performed on a kali linux boot on PC-3 to capture traffic between PC-4 and PC-2. The kali linux boot was configured to the same static IP address 192.168.10.3/24 as the Windows operating system on PC-3. The attacker on PC-3 ran Ettercap. The list of network devices was scanned. In Ettercap, Router C's G0/1.10 interface was set to

Router C's G0/1.10 interface was set to target 1 and PC-2 was set to target 2. An ARP poisoning attack was run on PC-3. Wireshark was launched on PC-3 and a packet capture section was started on the eth0 interface. The user on PC-4 sent an important file to the file server on PC-2. The Wireshark packet capture section on PC-3 was stopped. The filter ftp-data was applied. The traffic from PC-4 to PC-2 was opened and the contents of the file were collected.

The penetration tests and exploits were secured against. Router C was configured to block ping attempts from traffic outside of the HOME-OFFICE subnet. A phishing email detection document was written. The discovered eight discovered vulnerabilities were secured. Instructions were written for sending a document over FTP securely. AVG was downloaded onto PC-3 to provide antivirus and antimalware security for PC-3.

The project was completed with a project presentation and the submission of a project binder.