**Week 8 Homework: Networking Fundamentals-Rocking your Network!**

**Phase 1: “I’d like to Teach the World to Ping”**

1. *Steps and commands used to complete the tasks*

Text

Description automatically generated











1. *Summary of your findings for each testing phase*

The only live IP address was 167.172.144.11/32

sysadmin@UbuntuDesktop:~$ fping -g 15.199.95.91/28

15.199.95.81 is unreachable

15.199.95.82 is unreachable

15.199.95.83 is unreachable

15.199.95.84 is unreachable

15.199.95.85 is unreachable

15.199.95.86 is unreachable

15.199.95.87 is unreachable

15.199.95.88 is unreachable

15.199.95.89 is unreachable

15.199.95.90 is unreachable

15.199.95.91 is unreachable

15.199.95.92 is unreachable

15.199.95.93 is unreachable

15.199.95.94 is unreachable

sysadmin@UbuntuDesktop:~$ fping -g 15.199.94.91/28

15.199.94.81 is unreachable

15.199.94.82 is unreachable

15.199.94.83 is unreachable

15.199.94.84 is unreachable

15.199.94.85 is unreachable

15.199.94.86 is unreachable

15.199.94.87 is unreachable

15.199.94.88 is unreachable

15.199.94.89 is unreachable

15.199.94.90 is unreachable

15.199.94.91 is unreachable

15.199.94.92 is unreachable

15.199.94.93 is unreachable

15.199.94.94 is unreachable

sysadmin@UbuntuDesktop:~$ fping -g 11.199.158.91/28

11.199.158.81 is unreachable

11.199.158.82 is unreachable

11.199.158.83 is unreachable

11.199.158.84 is unreachable

11.199.158.85 is unreachable

11.199.158.86 is unreachable

11.199.158.87 is unreachable

11.199.158.88 is unreachable

11.199.158.89 is unreachable

11.199.158.90 is unreachable

11.199.158.91 is unreachable

11.199.158.92 is unreachable

11.199.158.93 is unreachable

11.199.158.94 is unreachable

sysadmin@UbuntuDesktop:~$ fping -g 167.172.144.11/32

167.172.144.11 is alive

sysadmin@UbuntuDesktop:~$ fping -g 11.199.141.91/28

11.199.141.81 is unreachable

11.199.141.82 is unreachable

11.199.141.83 is unreachable

11.199.141.84 is unreachable

11.199.141.85 is unreachable

11.199.141.86 is unreachable

11.199.141.87 is unreachable

11.199.141.88 is unreachable

11.199.141.89 is unreachable

11.199.141.90 is unreachable

11.199.141.91 is unreachable167

11.199.141.92 is unreachable

11.199.141.93 is unreachable

11.199.141.94 is unreachable

1. *Network vulnerabilities discovered*

Can see what target hosts are responding and those that are not.

1. *Findings associated with a hacker*

Provides the hacker with an opportunity to find an open port that would ultimately allow them to get into your network and data.

1. *Recommended mitigation strategy*

Block ping messages

1. *OSI layer where findings were found*

OSI Layer 2-Data

**Phase 2: “Some Syn for Nothin”**

1. *Steps and commands used to complete the tasks*

Text

Description automatically generated

1. *Summary of your findings for each testing phase*

Text

Description automatically generated

1. *Network vulnerabilities discovered*

SSH port 22 is open

1. *Findings associated with a hacker*

Allows the hacker to see what the service is running to create a plan of attack.

1. *Recommended mitigation strategy*

Set up structure for continuous security monitoring in which tools can be utilized to assist with this process. Open port vulnerabilities seem to be easily mitigated with a good cybersecurity culture/hygiene.

1. *OSI layer where findings were found*

OSI Layer 4-Transport

**Phase 3: “I feel a DNS Change Comin’ On”**

1. *Steps and commands used to complete the tasks*



Text

Description automatically generated with low confidence

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated



1. *Summary of your findings for each testing phase*

Through the research it was discovered that they were actually being directed to the wrong site

1. *Network vulnerabilities discovered*

Possible lax guidelines on password development for employees.

1. *Findings associated with a hacker*

They were able to gain unauthorized access through SSH

1. *Recommended mitigation strategy*

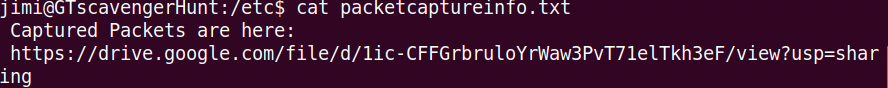
* Security team will monitor changes in important files (i.e. etc/hosts)
* Set a custom SSH port
* Integrate a server-side software firewall
* Disable root login
* Protocols need to be developed for strong password creation then limit max authentication attempts
* Set idle timeout intervals

*OSI layer where findings were found*

OSI Layer 7-Application

**Phase 4: “ShARP Dressed Man”**

1. *Steps and commands used to complete the tasks*



Graphical user interface, application

Description automatically generated

*Graphical user interface, text, application

Description automatically generated*

*Graphical user interface, text, application

Description automatically generated*

1. *Summary of your findings for each testing phase*

We have been attacked allowing someone to send falsified ARP messages over a LAN which has allowed the linking of an individual’s MAC address with the IP address with our computers(S) and/or server(s). This can allow them to intercept, modify or even stop data from flowing.

1. *Network vulnerabilities discovered*

There are vulnerabilities with our data and networks as this hacker has altered routing on the network.

1. *Findings associated with a hacker*

The hacker is doing a Man in the Middle attack known as ARP Spoofing/Poising attack.

1. *Recommended mitigation strategy*

This will not be a quick fix but once we recognize that this occurring we could:

* Rely on VPN’s to get into system
* Rely on trust relationships
* Use a static ARP
* Set-up packet filtering
* Integrate malware monitoring systems
* Run spoofing attacks and keep track of what works and what failed so as to stay ahead of the hackers
* Use cryptographic network protocols including TLS, SSH, HTTPS.

1. *OSI layer where findings were found*

OSI Layer 7-Application