Protection From Reconnaissance and Scan Attack Through NGFW (Next Generation Firewall)

Kyle Radzak
Christopher Ngo
Advisor: Jorge Crichigno, Ali Alsabeh

Department of Integrated Information Technology
University of South Carolina

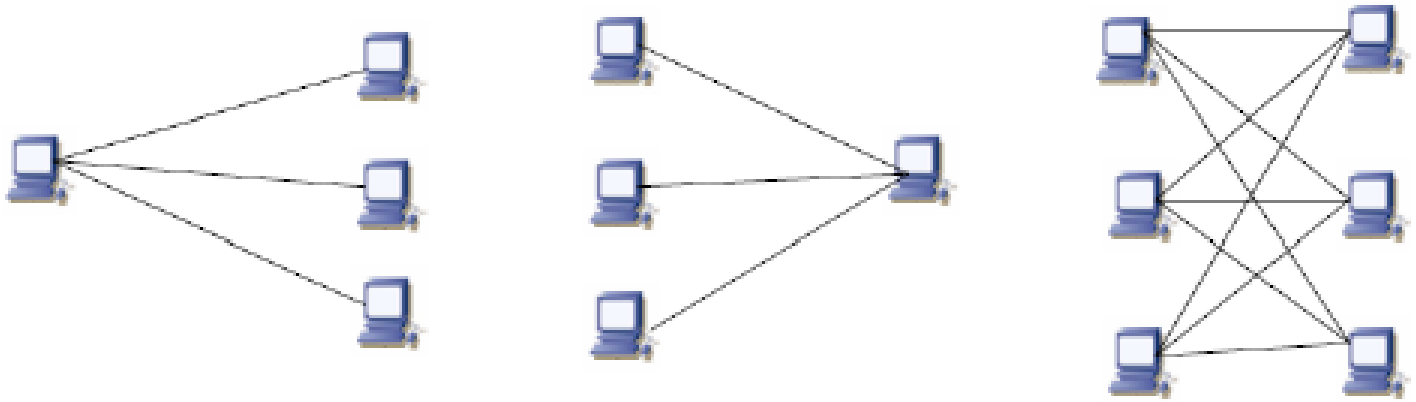
December 2020

Agenda

- Introduction to Network Security and Reconnaissance attacks
- Background Information
  - Reconnaissance and Scan Attacks
  - Palo Alto Firewall Systems
  - Implementation of Reconnaissance Protection to prevent port and host sweeps
- NMAP and hping3 Use
- Proposed Solution and Implementation
- Conclusion

Introduction

- Reconnaissance is the practice of information gathering. How this is applied to network security is when attackers attempt to gain information about the network's topology and vulnerabilities.
- A modern-day firewall is designed to monitor incoming and outgoing traffic in order to decide whether to allow or block specific based off rules.
- In order to prevent attackers from gaining information about a network, zone protection profiles using Reconnaissance Protection can be used to defend against port scans and host sweeps.



(a) Single Source port scan (One-to-many)

(b) Distributed port scan (many-to-one)

(c) Distributed port scan (many-to-many)

Background Information

- Reconnaissance (or recon) attacks is the action of unauthorized discovery and mapping of networks and vulnerabilities
  - When directed at an endpoint, such as a PC, a recon attack is also called host profiling.
  - If successful, an attacker can see which ports are active and open.
  - Recon attacks are more than likely accompanied by a more intrusive attack such as DoS attack.

```
root@bt:~# nmap -sU 10.10.19.202

Starting Nmap 4.68 ( http://nmap.org ) at 2012-03-03 21:43 EST
Interesting ports on 10.10.19.202:
Not shown: 1472 closed ports
PORT     STATE         SERVICE
53/udp   open|filtered domain
88/udp   open|filtered kerberos-sec
123/udp  open|filtered ntp
135/udp  open          msrpc
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
389/udp  open|filtered ldap
445/udp  open|filtered microsoft-ds
464/udp  open|filtered kpasswd5
500/udp  open|filtered isakmp
1032/udp open|filtered iad3
1034/udp open|filtered activesync-notify
1059/udp open|filtered nimreg
3456/udp open|filtered IISrpc-or-vat
4500/udp open|filtered sae-urn
MAC Address: 00:50:56:98:00:9F (VMWare)

Nmap done: 1 IP address (1 host up) scanned in 15.72 seconds
```

NetLab lab 14: Discovering Security Threats and Vulnerabilities

Background Information

- Next Generation Firewall System

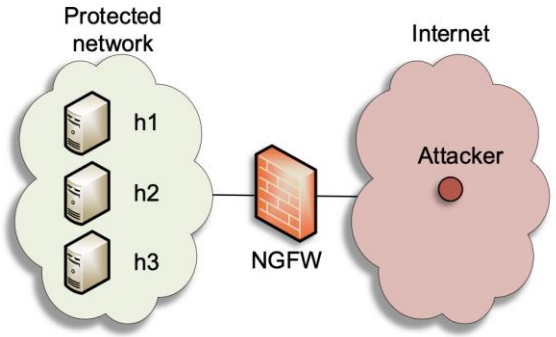
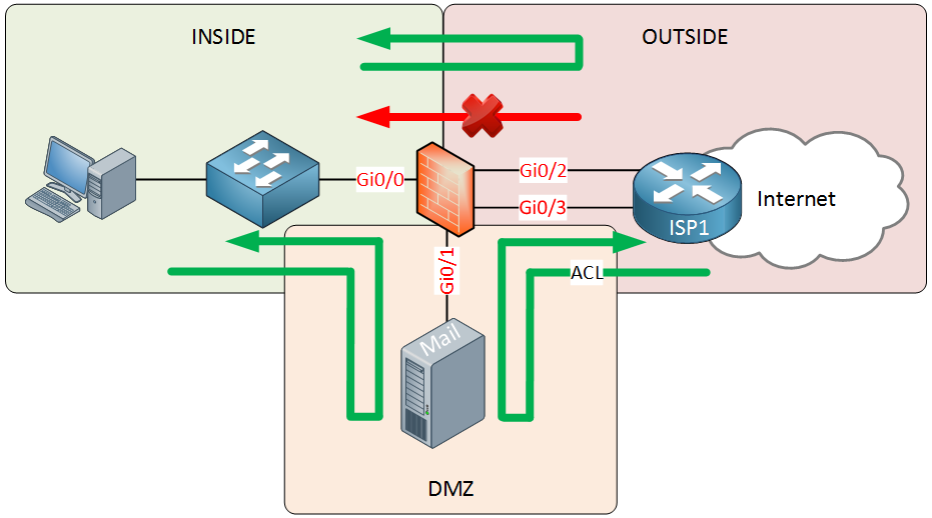


Figure 1. Network topology.

- Zones protect the network by segmenting it into smaller, more easily managed areas.
- Zones also prevent uncontrolled traffic from flowing through the firewall. This is because each interface has to be assigned a Zone. Therefore, this prevents inappropriate traffic from entering a zone it does not belong

Proposed Solution and Implementation

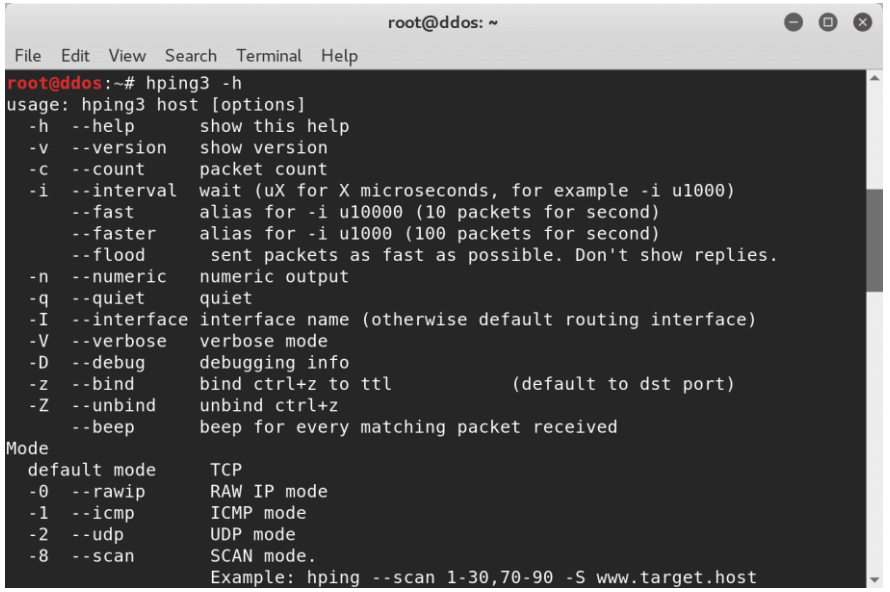
- Creating a zone protection and vulnerability protection profile are critical to protecting the network and are the best methods of fending off a Reconnaissance and Scan Attack.



- Zone protection and vulnerability protection have created a net of defense from external sources gaining valuable information on the network.
- We will be creating unique profiles on our Next Generation Firewall to ward off these types of attacks as well as ensuring the proper ports are sealed off to these types of attacks.

NMAP and hping3 Use

- Nmap and Hping3 are open-source tools used for cyber defense and attacks
- Nmap scans for network devices and open ports
- We used Nmap to identify tcp/udp ports that could be flooded and attacked
- Hping3 was used to perform a flood attack on open ports of the network and was an exemplary of how the firewall was able to deny the pings
- Nmap and Hping3 commands are tools that can be used by any hacker to get into the targeted network



Conclusion

- With the implementation of a zone and vulnerability protection profiles, we can ensure a high level of security and safety are maintained. The probability that information behind the firewall will be breached, altered, or compromised by malicious external actors will be greatly reduced.