SAPIENZA
UNIVERSITÀ DI ROMA

FACULTY OF INFORMATION ENGINEERING, INFORMATICS AND STATISTICS

Practical Network Defense

ASSIGNMENT 3

Students:
Natnael Solomon Fantu,
Elizaveta Lapiga,
Chiara Menghini,
Alessio Scanu.

Academic Year 2023/2024

1 Initial Brainstorming

For this assignment, we followed the guidelines from the Network Hardening lecture to outline the scope of activities. We have defined the key protection measures for management plane, control plane and data plane. In the following paragraph, we identified a list of activities along with their implementation and evaluations

2 Protection Plan Definition, Implementation and Evaluation

2.1 Management plan protection

2.1.1 Strong password policy

We change the default password on each device in the ACME network and applied a strong password policy to ensure bruteforce resiliance. To change the firewalls password we used the OPNsense interface, while for the other devices we used the terminal.

- **main FW password:** &8U%N)FT
- **internal FW password:** Z#t2qggv
- **arpwatch password:** %8aQ!dB7
- **dnsserver password:** R5y!sL2&
- **logserver password:** p1%O2!kX
- **web server:** M%4kD)n8
- **proxy server:** f7W&3b$R
- **greenbone:** Z6*qL!x3
- **graylog:** T!9nM$1k
- **.100 pc (kali):** J2Q@#Adb

2.1.2 Encrypted communication

To secure the usage of OPNsense GUI FWs we switched from the HTTP to the HTTPS protocol, enabling encrypted communication.

2.1.3 Configuration of NTP service on internal interface

Inside the FWs we configured the NTP service under the Services section. This service ensures synchronization of all devices and enables temporal comparison of logs.

2.1.4 Configuration of a syslog server

We accessed the System: Settings: Logging / targets section, then we added a new logging target with the following specifications:

- IP address of logserver
- Port: 514
- Protocol: UDP

This allow us to collect and manage logs.

2.2 Control plain protection

2.2.1 Protect against too many ICMP messages

We went in the section main FW: Shaper: Settings

- Inside the section Pipes tab, we added a limitation to 10 Kbit/s without selecting mask. This will prevent our network from being flooded with packets in case of an attack.
- Inside the Rules tab, we added a rule for WAN about ICMP packets from any source and for any destination, using the limitation defined in Pipes tab as target.

2.2.2 Block potentially malicious ICMP messages

- We went in the section main FW: Rules: Floating and we added a Block rule at the top of the list for ICMP redirect packets from any source to any destination on the DMZ and EXTERNAL interfaces, ensuring the rule type was set to "in" since the packets enter the interface. This will prevent man-in-the-middle attacks.
- We went in the section main FW: Rules: WAN, then we added a block rule in the first position for ICMP packets of type Destination Unreachable with outbound direction from any source to any destination. We have decided to block their usage to prevent network exposure to attacks like network mapping and denial of services.

2.3 Data plain protection

2.3.1 Block packets with spoofed IP address

We have already blocked all of the traffic which was not specified in the previous tasks. To prevent all the traffic going out of DMZ we edited our previous rules by specifying the source as the DMZ network, instead of adding a pass rule for packets originating from the DMZ net. We created similar rules in internal interfaces on both FWs to block all packets with source IP addresses that are not consistent with the network topology.

2.3.2 Allow only packets that match the traffic expected on the network

We already set most of the rules in the previous assignments. We only added the rule inside the main FW in WAN interface, we allowed the traffic from internet to proxyserver, TCP port 3128. This implementation was chosen because it follows the principle of least privilege, promoting better security by restricting permissions to only what is necessary.

3 Protection plan evaluation and Final Remarks

As a final remark, it is important to note that there are many ways to implement network hardening. In our work, we utilized the most fundamental principles at the network, transport, and application levels. However, there remains the possibility to enhance network protection at the data link level.

- To ensure bruteforce resiliace we applied strong password policy.
- On the devices with GUI we implemented encrypted communication protocol(HTTPS).
- We configured a reliable NTP server to synchronize all devices, enabling temporal comparison of logs.
- We configured syslog mechanism to collect and manage logs.
- To avoid ICMP flood attack we put a limit on ICMP traffic.
- In order to manage dangerous ICMP packets we filter the ICMP redirect packets by adding a block rule