CNIT 45500: Network Security

CNIT45500-010

Group 32

Ethn Hammond

Tyler Hiatt

Submitted To: Tony Wan

Date Submitted: 11/9/23

Date Due: 11/10/23

TABLE OF CONTENTS

EXECUTIVE SUMMARY

ET Corp's attack security of concept started with an install of exploitable machines like Metasploitable and UltimateLAMP, and the install of an attacker machine like Kali with services used to attack. Kali services that are used for attacking included Nessus for scanning, NMAP for port scanning, and synflooding techniques to overload the open ports on the victim machines. These methods were used to prove the vulnerability of open ports on vulnerable machines as well as the importance of using IDS and IPS solutions. Attacking with synfloods allowed for the Snort and Suricata machines to pick up the logs very clearly for analysis.

BUSINESS CASE

ET Corp is deploying two different intrusion detection systems (IDS). All traffic in the environment will be port mirrored to an unbound interface on the IDS machine. The two different IDSs that will be implemented are called Suricata and Snort. After the implementation of these network intrusion detection systems, a Kali Linux machine will attack two vulnerable machines located on the DMZ. This attack will occur in order to see what logs and reports are generated on the IDS machines. Upon completion of the attack, the logs will be inspected. This will greatly enhance the security backbone of ET Corp, and network attacks will be able to be patched up more efficiently at the packet filter. Testing vulnerabilities on your own machines is vital to a company like ET Corp's success.

PROCEDURES

The formatting key of the following section will obey rules below: buttons are **bold**; options are *italicized*; text entered into the computer is in `Courier New style`; menu, folder navigation, and repetitive commands are shown with the pipe symbol and are *italicized*: *Start* | *Programs* | *MS Office* | *Word*.

VM Installation and Configuration

VMs were installed for testing with two vulnerable VMs and one Kali Linux attacker VM on the DMZ network.

1. Created a Metasploitable VM based off a template found in RTFM.
2. Created an UltimateLAMP VM based on a template found in RTFM.
3. Created a Kali Linux VM from an ISO in RTFM.
4. Installed Nessus services on the Kali Linux VM.
5. Attached one pfSense DMZ port group NICs onto the metasploitable and UltimateLAMP VMs.
6. Attached a private A NIC to the Kali Linux VM.
7. Created an Ubuntu VM from an ISO off of RTFM to house the Snort/Suricata IDS.
8. Added two pfSense DMZ port group NICs onto the Ubuntu VM.

Probing the Vulnerable VMs

Before true attacks were to be carried out, it was important to do some scanning of ports and services that could be vulnerable to attack. This was done with NMAP on the Kali Linux machine.

1. Logged into the Kali VM to initiate NMAP tasks.
2. Used the nmap 192.168.1.13 and nmap 192.168.1.104 commands to scan.
3. Documented the reports of open ports from the machine scans.
4. Used dpkg -i 'Nessus-6.11.1-debian6_amd64.deb' to install Nessus onto the Kali Machine.
5. Launched nessus with /bin/systemctl start nessusd.service.
6. Opened Nessus by searching https://cnit455g32:8834 on a browser.
7. Entered login credentials and clicked 'basic network scan' to scan the network for hosts on 192.168.0.0/16.

Installing and Configuring Suricata

Suricata was important to be installed before attacks because it can capture logs from the network and prospective attacks and store them to be viewed in the future.

1. Sudo add-apt-repository ppa:oisf/suricata-stable
2. Installed Suricata using sudo apt install
3. Edited the file /etc/suricata/suricata.yaml and added ens33 to the afpacket interface.
4. Uncommented the log files we needed in /etc/suricata/suricata.yaml
5. Edited the above file and added the following lines:
    a. default-rule-path: /var/lib/suricata/rules

       Rule-files:

    b. Suricata.rules

6. Sudo nano /etc/systemd/system/suricata.service
    a. [Unit]
    b. Description=Suricata IDS/IPS
    c. After=network.target
    d.
    e. [Service]
    f. ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens33
    g.
    h. [Install]
    i. WantedBy=default.target
7. Entered sudo systemctl start suricata.service
8. Entered sudo systemctl status suricata.service
9. Entered sudo suricata-update update-sources

Installing and Configuring Snort

Snort was installed and configured to capture logs further when an attack is carried out on either the metasploitable or UltimateLAMP machines.

1. Entered sudo apt install snort
2. Configured wizard with appropriate IP addresses
3. Entered sudo systemctl start snort
4. Started test internet session and verified logs in /var/log/snort

Creating a Port Mirroring Session

Port mirroring through VMware vSphere was necessary to capture traffic on the network. This was done through the ESXi network page on the vSwitch.

1. Navigated to VMware VSphere and navigated to the virtual switch
2. Selected Configure and then selected Port Mirroring
3. Created a new port mirroring session and selected all sources except IDS machine
4. Selected the destination source to the IDS machine

Attacking Metasploitable and UltimateLAMP VMs

The chosen attack was a synflood over NETBIOS for the metasploitable machine, and a synflood over HTTP for the UltimateLAMP.

Metasploitable

1. Opened a terminal window on Kali.
2. Used nmap 192.168.1.104 to see the vulnerable ports on metasplotable.
3. Used sudo mfconsole to enter the attack console.
4. Entered use auxiliary/dos/tcp/synflood to enter the synflood attack.
5. Used set RHOST 192.168.1.104 to set the host to attack.
6. Entered set RPORT 139 to set the port to attack over.
7. Looked at the attack overview with show options.
8. Entered run to start the attack.

UltimateLAMP

1. Opened a terminal window on Kali.

2. Used nmap 192.168.1.13 to see the vulnerable ports on metasplotable.
3. Used sudo mfconsole to enter the attack console.
4. Entered use auxiliary/dos/tcp/synflood to enter the synflood attack.
5. Used set RHOST 192.168.1.13 to set the host to attack.
6. Entered set RPORT 80 to set the port to attack over.
7. Looked at the attack overview with show options.
8. Entered run to start the attack.

Snort/Suricata

1. Looked at /var/log/snort/snort.alert.fast to see the alerts from the attack.

2. Investigated the /var/log/suricata/eve.json file for the attack timestamps and details.

RESULTS

The lab resulted in a lab testing environment containing vulnerable machines as Metasploitable and UltimateLAMP with open ports such as 139 and 80 that were scanned with Nessus and NMAP. After a port scanning tool was run on NMAP, ports were revealed as open and exploitable. The ports were exploited via a synflood attack from the Kali Linux VM. IDS and IPS systems were installed as Suricata and Snort VMs and were used to capture logs from the attacks over the network. Physical and Logical diagrams can be seen below in Figures 1.1 and 1.2. As logs are captured, they can be analyzed to view incidents and analyze what ports in the network are vulnerable and give insight into tactics that adversaries use and how to patch a system from further intrusion.

Figure 1.1: Screenshot of the Logical Diagram

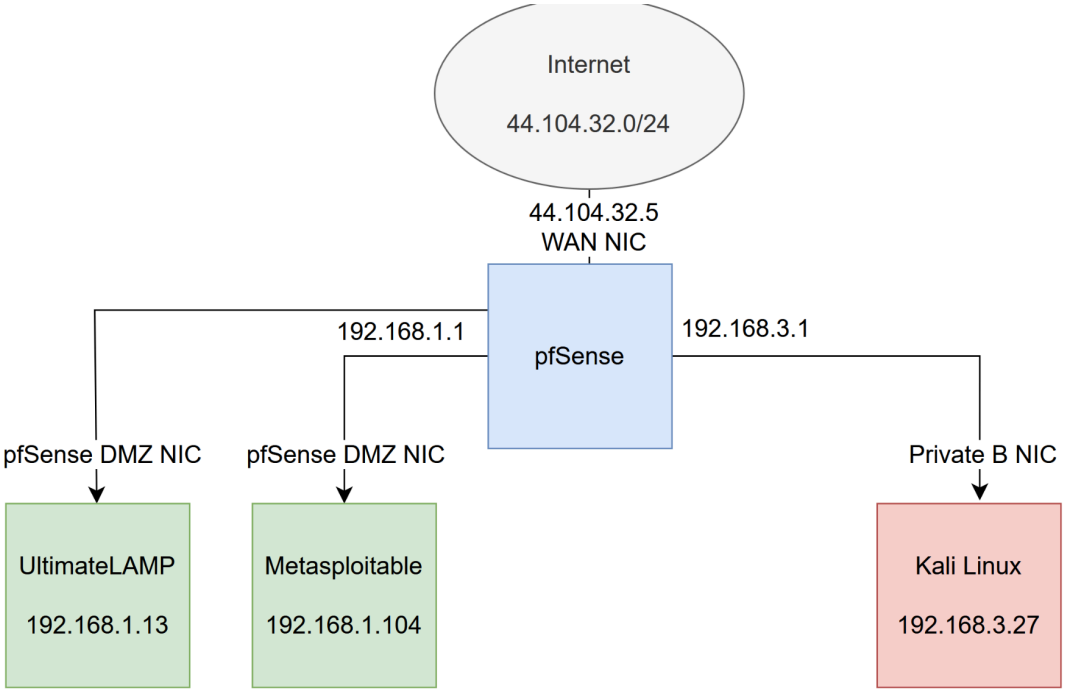
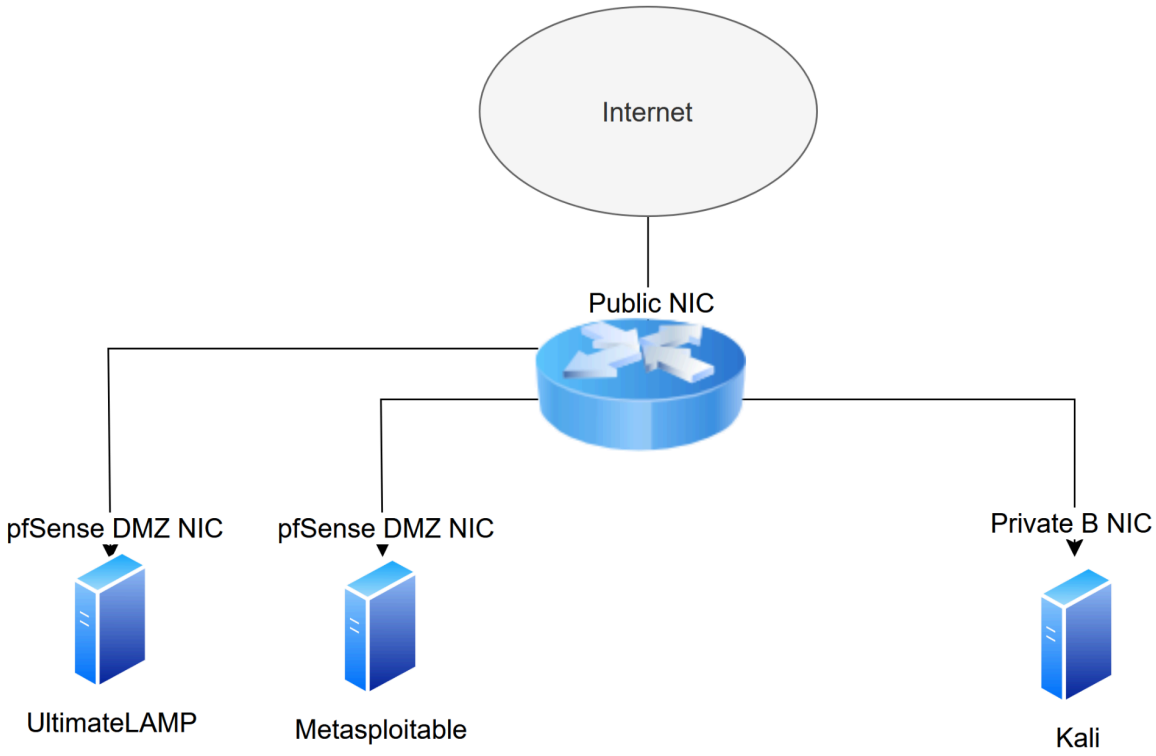


Figure 1.2: Screenshot of the Physical Diagram



CONCLUSIONS AND RECOMMENDATIONS

Upon completion of the recommended architecture, there is only one aspect that would have improved efficiency. This recommendation is the use of an unbound NIC for the sniffing interface. The port mirroring session needs to have a destination of an unbound NIC in the DMZ. Although the IDSs worked without this additional NIC, this is not the recommended architecture, and it is important to have the management NIC separate from the sniffing NIC. After completing this separation, the attack was completed and the architecture could be considered complete.

REFERENCES

Administrator. (n.d.). *Home*. Cisco Networking, VPN Security, Routing, Catalyst-Nexus Switching, Virtualization Hyper-V, Network Monitoring, Windows Server, CallManager, Free Cisco Lab, Linux Tutorials, Protocol Analysis, CCNA, CCNP, CCIE. https://www.firewall.cx/tools-tips-reviews/network-protocol-analyzers/performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html

How to install suricata on ubuntu 22.04. Virtono Community. (2023, June 22). https://www.virtono.com/community/tutorial-how-to/how-to-install-suricata-on-ubuntu-22-04/

Snort setup guides for emerging threats prevention. (n.d.). https://www.snort.org/documents

Suricata User guide. Suricata User Guide - Suricata 7.0.3-dev documentation. (n.d.). https://docs.suricata.io/en/latest/

APPENDIX A: PROBLEM SOLVING

Problem 1

Problem Description: In order to build the architecture correctly, the sniffing NIC needs to be separate from the management interface NIC. This needed to be changed, as both were on the same NIC.

Problem Solutions: Change the port mirroring destination to the unbound NIC for the sniffing interface.

Solutions Attempted: The only solution that was a potential solution was completed.

Final Solution: The only solution worked, as this was the only way to correctly implement that architecture.

Problem 2

Problem Description: Suricata and Snort need to be able to send emails to the administrators when an incident occurs on the network. However, the emails were not working.

Problem Solutions: Double check that the firewall allows mail through, ensure the correct email is entered in, ensure the mail configs are correct, and ensure the mail is not being sent to spam.

Solutions Attempted: All solutions shown above were attempted throughout the troubleshooting process.

Final Solution: The final solution was never recovered, and all potential solutions failed. Email alerts are still not set up correctly.