Hack-a-Home: Trojan Horse
Hakeem, Brandon

Project Overview:
The objective of this project was to simulate a home network using EVE-NG, and then perform the penetration test to attempt to identify the vulnerabilities in the network, emphasizing firmware. This report will include the details of network configuration, the method used for penetration testing, the results of the penetration testing, and the part played by firewalls even in the home networks of individuals who are not very tech-savvy.

1. Network Architecture:

1. 1 EVE-NG Lab Configuration:
The virtual lab was built using the following network components: The virtual lab was built using the following network components:

- **AlienVault Cybersecurity**: Used on a large scale as a Security Information and Event Management system for detecting and mitigating network threats.
- **Cisco CSR 1000V (XE 16. x)**: A Cisco 9300 hw-based virtual router utilizing Cisco IOS XE software for emulating enterprise routing and security.
- **Juniper vEVO Router**: A copy of Juniper's routing platform operating in a virtual environment with enhanced networking capabilities and security.
- **OPNsense**: A free-firewall software meant for routing in ensuring that the edges of the networks are secured.
- **VyOS**: A network operating system that integrates the aspects of commercial routing, firewalls, as well as VPNs.

1. 2 Network Setup:
The virtual network consisted of a typical home network with extra levels of difficulty, such as multiple subnets, firewalls, and routers for different devices and areas. The intention was to provide conditions as close to the real world and the use of various devices as possible and to be able to check out potential weaknesses.

2. Penetration Testing Methodology:

2. 1 Tools and Techniques:

- **Nmap**: Its utility was applied to network mapping and recognizing of available ports, services, and possible weaknesses inside the network.

- **PuTTY**: For running the SSH connections and for the management of switches and routers in the network.
- **VirtualBox** and **QEMU**: Used to provision and control virtual machines in the context of the EVE-NG platform.

2. 2 Commands Used:

- Initial Network Scan: sudo nmap –scan business law for dummies -host-depth high horizontal 192. 168. 1. 0/24
- Focused Scans on Identified Hosts: Focused Scans on Identified Hosts:
    - **nmap** -sS -O -p 1-65535 192. 168. 1. 191
    - **smbclient** -L \\\\192. 168. 1. 191
    - **vncviewer** 192.168.1.191:5900

3. Findings and Analysis:

3. 1 Vulnerabilities Discovered:

- **Open VNC Ports**: Present on one of the network devices; this is dangerous as it might allow remote access.
- **SMB Services**: SMB was operational at some of the devices without passing through the authentication process thus making the devices reachable.
- **Outdated Firmware**: The virtual devices had exposed firmware in some of the virtual devices which if not updated were vulnerable to being exploited.

3. 2 Importance of Firmware Updates

Firmware updates are extremely important as far as the security of the network devices is concerned. What emerged from the testing was that firmware could and was a big weakness to attackers, as they can take advantage of outdated firmware which has holes that have been fixed in subsequent firmware. Regular updates of firmware are important even for home networks since threats to a network can change over time.

4. Importance of Firewalls:

4. 1 Firewall Configurations:

The deployment of OPNsense and VyOS firewalls was instrumental in protecting the network. These firewalls were configured to:

- **Filter traffic** between different network zones.
- **Block unauthorized access** to sensitive services.

- **Log and monitor** suspicious activity.

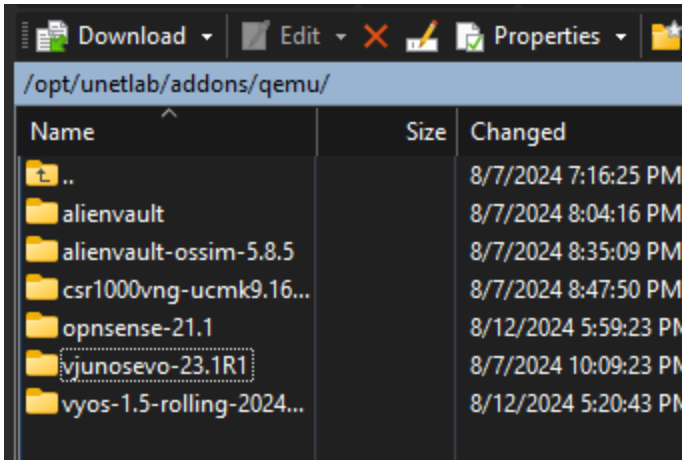
4. 2 Firewall Effectiveness:
Network firewalls considerably diminished the havoc that was possible with the networking. At times, there were attempts at penetration into the network however, these were futile in the face of firewalls which successfully denied the intruders access and offered log data that could be used in investigations.

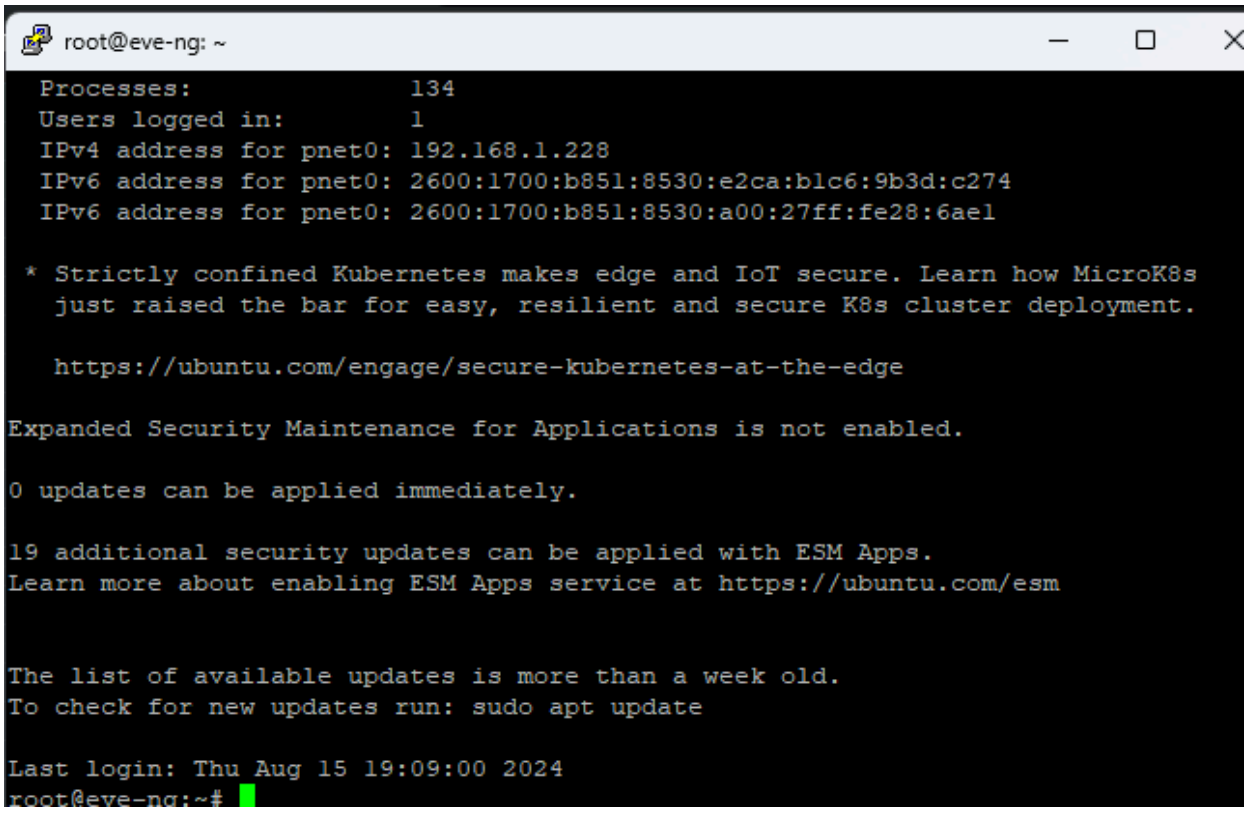
5. Conclusion:
From this project, people learned the need to make sure their networks are well secured, even if they are at home. Working in the EVE-NG laboratory proved to be valuable and allowed researching multiple aspects of network security – effects of firmware updates and others, the importance of firewalls, etc. The study proved that vulnerabilities as such can be exploited when the usual aspects of protection, like the update of firmware, and configuration of a firewall are not dealt with accordingly.

In the case where there are fewer computer/network-literate users, they must at the bare minimum correctly configure the firewalls and have up-to-date firmware on their network device for the best security available to them.

6. Recommendations:

Regular Firmware Updates: Make sure that firmware on all devices connected to the network is updated to the current state to minimize threats known to be present.
Firewall Implementation: Use available firewalls to mediate traffic and protect areas of your network.
Continuous Monitoring: The following are some recommendations: Using programs like Alien Vault for constant surveillance so that any visible clear threats can be dealt with immediately.


Download
Edit
Properties
/opt/unetlab/addons/qemu/
Name
Size
Changed
..
8/7/2024 7:16:25 PM
alienvault
8/7/2024 8:04:16 PM
alienvault-ossim-5.8.5
8/7/2024 8:35:09 PM
csr1000vng-ucmk9.16...
8/7/2024 8:47:50 PM
opnsense-21.1
8/12/2024 5:59:23 PM
vjunosevo-23.1R1
8/7/2024 10:09:23 PM
vyos-1.5-rolling-2024...
8/12/2024 5:20:43 PM


root@eve-ng: ~
Processes: 134
Users logged in: 1
IPv4 address for pnet0: 192.168.1.228
IPv6 address for pnet0: 2600:1700:b851:8530:e2ca:b1c6:9b3d:c274
IPv6 address for pnet0: 2600:1700:b851:8530:a00:27ff:fe28:6ae1
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
19 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Thu Aug 15 19:09:00 2024
root@eve-ng:~#

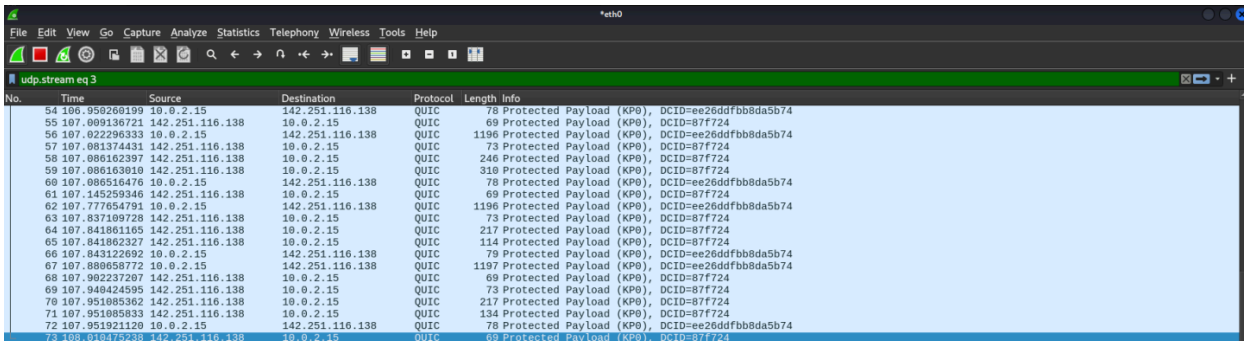
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 15:19 EDT
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; proto
col 2.0)
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
32769/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd
Service Info: OS: Linux; Device: broadband router; CPE: cpe:/o:linux:linux_ke
rnel, cpe:/h:actiontec:mi424wr

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 15:20 EDT
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 11:63:48:f2:f5:5a:b5:d2:89:a0:70:49:bb:ca:07:46 (ECDSA)
|_  256 12:bb:3e:3c:7a:db:91:55:8c:9f:7e:fa:9c:d5:fa:54 (ED25519)
80/tcp    open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
32769/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd
Service Info: OS: Linux; Device: broadband router; CPE: cpe:/o:linux:linux_kernel, cpe:/h:actiontec:mi424wr

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

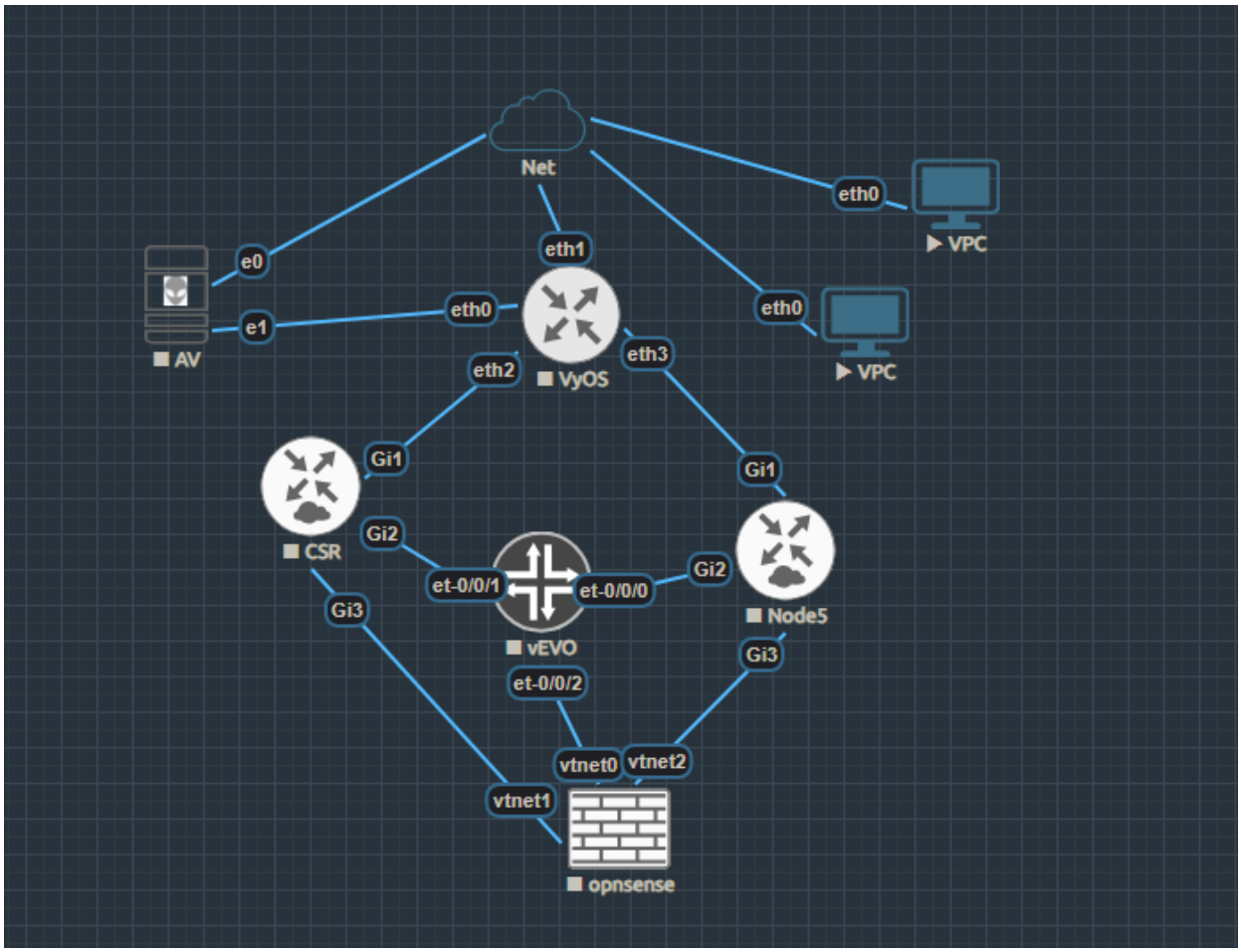
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 15:21 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.88% done; ETC: 15:25 (0:03:18 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 6.35% done; ETC: 15:25 (0:02:57 remaining)
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0071s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
32769/tcp open  filenet-rpc

Nmap done: 1 IP address (1 host up) scanned in 114.64 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-sql-injection -p 80 192.168.1.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 15:38 EDT
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0068s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 15:39 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 4.88% done; ETC: 15:40 (0:01:37 remaining)
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0014s latency).
Nmap scan report for dsldevice.attlocal.net (192.168.1.254)
Host is up (0.0094s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 24.77 seconds
```




```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script exploit 192.168.1.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-15 16:57 EDT
Nmap scan report for eve-ng.attlocal.net (192.168.1.228)
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
32769/tcp open  filenet-rpc
```


Net
eth0
VPC
e0
eth1
e1
eth0
AV
VyOS
eth0
VPC
eth3
eth2
Gi1
Gi1
CSR
Gi2
et-0/0/1
et-0/0/0
Gi2
Node5
Gi3
vEVO
Gi3
et-0/0/2
vtnet0
vtnet2
vtnet1
opnsense