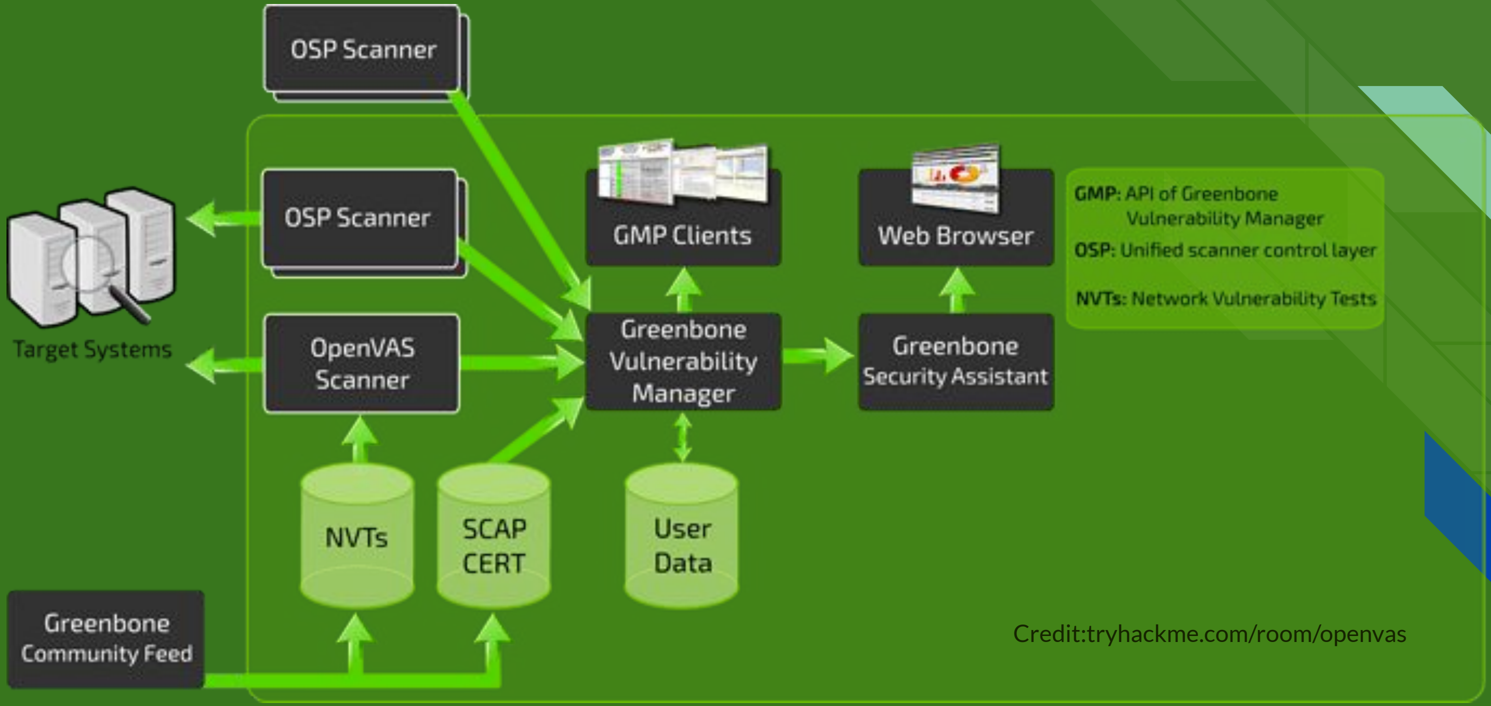
OpenVAS and Securing a Network BootCon 2023!

Presented by: Omar Rayo-Vazquez

What is OpenVAS?

- OpenVAS is a full-featured vulnerability scanner.
- Huge Database of NVTs and uses SCAP CERT
- GVM Framework Vulnerability/ Information Feed, Backend, Frontend



GMP: API of Greenbone Vulnerability Manager
OSP: Unified scanner control layer
NVTs: Network Vulnerability Tests

Credit:tryhackme.com/room/openvas

Why use OpenVAS?

- Friendly Reporting!
- Offers Solutions!
- Able to test IDS and IPS systems
- And no I am not sponsored by GVM.

Tools

- VirtualBox with 2 Ubuntu and 1 Kali box located on the same subnet
- UFW will be used on some Machines
- SSH to fix any vulnerabilities and perform authenticated scans
- Kali will be the administrator system
- The goal is to simulate a small organization that would like a vulnerability test done to it’s systems. Perform mitigations if possible.
- Google/Firefox/Bing
- Patience for troubleshooting

Vulnerabilities and Mitigations found

Ubuntu: Security Advisory: CVE-2019-17594 (192.168.100.6)Severity:8.8

Solution:

Sudo apt update && sudo apt upgrade && sudo apt dist-upgrade

Then set up UFW firewall and then authenticated scan broke.

P4.1 (192.168.100.4) had the firewall enable from the beginning and the rules were set up the same.

For know the firewall was disabled on P4.2 (192.168.100.6)

Vulnerabilities and Mitigations found

RETbleed: CVE-2022-29900 (all hosts) Severity:6.5

Solution:
POWERSHELL to fix on a VM

```
$env:PATH = $env:PATH + ";\Program Files\Oracle\VirtualBox"
```

Then

```
 VBoxManage modifyvm "NAME_OF_VM" --spec-ctrl on
```

https://forums.virtualbox.org/viewtopic.php?f=7&t=107103

https://www.how2shout.com/how-to/vboxmanage-command-not-found-in-windows-cmd-or-powershell

TCP TImestamps Information Disclosure

TCP Timestamps Information Disclosure (all hosts) Severity: 2.6

Solution:

mitigation: echo "net.ipv4.tcp_timestamps = 0" >> /etc/sysctl.conf && sysctl -p

Why Vulnerability scans are important!

An important point about a vulnerability scan is that it does not attempt to exploit any vulnerabilities. Instead, a vulnerability scan is a passive attempt to identify weaknesses. This ensures that the testing does not interfere with normal operations. Security administrators then assess the vulnerabilities to determine which ones to mitigate.

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide (pp. 758-759). YCDA, LLC. Kindle Edition.

The End

Resources used

www.Google.com

www.Tryhackme.com

https://www.virtualbox.org/manual/ch08.html

https://forums.virtualbox.org/viewtopic.php?f=7&t=107103

https://access.redhat.com/support/policy/updates/errata/#Production_Phases

https://phoenixnap.com/kb/how-to-update-kernel-ubuntu

https://bobcares.com/blog/openvas-reset-admin-password/

https://www.greenbone.net/en/

https://hub.docker.com/r/mikesplain/openvas/dockerfile

https://github.com/greenbone/openvas-scanner/blob/main/INSTALL.md