Vulnerability Scanning and Management

Written by Tyler Weiss

Exercise 1 - Installation

We are going to use Git in this exercise. Git is a version control software that tracks changes and versions of code. It allows multiple developers to manage the software development process to include code review, integration, versioning, merging and tracking. To check if git is installed use the '--versions' flag. If git is not installed use 'apt' to install it.

```
rec0nrat@ubuntu-nessus:~$ git --version
git version 2.34.1
rec0nrat@ubuntu-nessus:~$
```

```
sudo apt update
sudo apt install git
```

Using the 'clone' option will allow us pull down, or clone, a a repository to use on our local machine.

```
Example
git clone https://github.com/example/repo.git
```

Task 1

We will be deploying the “vulnscan” – Vulnerability Scanning with Nmap Scanner to run alongside nmap on your Ubuntu Server. This is an open source tool and highly effective. It won’t be as pretty or build nice reports like the paid vendor tools, but it gets the job done.

Use the 'find' command the locate the nmap executable in file system. Below is a link to a tutorial on the 'find' command.

https://www.digitalocean.com/community/tutorials/how-to-use-find-and-locate-to-search-for-files-on-linux

The name option will allow us to search for any file names matching the argument. Use the '-name' option to search for 'nmap'. Sudo may be required to search for file and directories that our user does not have permission to view. If nmap is not installed use 'apt' to install it.

```
rec0nrat@ubuntu-nessus:~$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.2 nmap-libssh2-1.8.2 libz-1.2.11 libpcre-8.39 libpcap-1.10.1 nmap-libdnet-1.1
2 ipv6
Compiled without:
Available nsock engines: epoll poll select
rec0nrat@ubuntu-nessus:~$
```

```
sudo find / -name nmap
```

```
rec0nrat@ubuntu-nessus:~$ sudo find / -name nmap
/usr/bin/nmap
/usr/share/doc/nmap
/usr/share/bash-completion/completions/nmap
/usr/share/lintian/overrides/nmap
/usr/share/nmap
/snap/core20/2264/usr/share/bash-completion/completions/nmap
/snap/core20/2182/usr/share/bash-completion/completions/nmap
/snap/core22/1122/usr/share/bash-completion/completions/nmap
/snap/core22/1033/usr/share/bash-completion/completions/nmap
rec0nrat@ubuntu-nessus:~$
```

The folder nmap is located is '/usr/share/nmap'.

When you read the instructions to install VULNSCAN, it states: “Please install the files into the following folder of your Nmap installation: Nmap\scripts\vulscan*”.
Navigate to the scripts folder in the nmap directory and list the contents.

```
rec0nrat@ubuntu-nessus:~$ cd /usr/share/nmap/scripts/
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts$ ls
acarsd-info.nse                    http-hp-ilo-info.nse                nping-brute.nse
address-info.nse                   http-huawei-hg5xx-vuln.nse          nrpe-enum.nse
afp-brute.nse                      http-icloud-findmyiphone.nse        ntp-info.nse
afp-ls.nse                         http-icloud-sendmsg.nse             ntp-monlist.nse
afp-path-vuln.nse                  http-iis-short-name-brute.nse       omp2-brute.nse
afp-serverinfo.nse                 http-iis-webdav-vuln.nse            omp2-enum-targets.nse
afp-showmount.nse                  http-internal-ip-disclosure.nse     omron-info.nse
```

Once in the directory we need to download the vulscan project to the scripts directory. To do this use the following commands.

```
git clone https://github.com/scipag/vulscan scipag_vulscan
sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
```

The first command clone the repository places it in a directory called 'scipag_vulscan'. The second command creates a symbolic link so that the script can be run from any location in the file system.

```
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts$ sudo git clone https://github.com/scipag/vulscan scipag_vulscan
Cloning into 'scipag_vulscan'...
remote: Enumerating objects: 297, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 297 (delta 12), reused 16 (delta 4), pack-reused 264
Receiving objects: 100% (297/297), 17.69 MiB | 22.23 MiB/s, done.
Resolving deltas: 100% (175/175), done.
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts$ sudo ln -s `pwd`/scipag_vulscan /usr/share/nmap/scripts/vulscan
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts$ ls
acarsd-info.nse                    http-huawei-hg5xx-vuln.nse          ntp-info.nse
address-info.nse                   http-icloud-findmyiphone.nse        ntp-monlist.nse
afp-brute.nse                      http-icloud-sendmsg.nse             omp2-brute.nse
```

```
broadcast-rip-discover.nse         http-useragent-tester.nse           rsync-brute.nse
broadcast-ripng-discover.nse       http-userdir-enum.nse               rsync-list-modules.nse
broadcast-sonicwall-discover.nse   http-vhosts.nse                     rtsp-methods.nse
broadcast-sybase-asa-discover.nse  http-virustotal.nse                 rtsp-url-brute.nse
broadcast-tellstick-discover.nse   http-vlcstreamer-ls.nse             rusers.nse
broadcast-upnp-info.nse            http-vmware-path-vuln.nse           s7-info.nse
broadcast-versant-locate.nse       http-vuln-cve2006-3392.nse          samba-vuln-cve-2012-1182.nse
broadcast-wake-on-lan.nse          http-vuln-cve2009-3960.nse          scipag_vulscan
broadcast-wpad-discover.nse        http-vuln-cve2010-0738.nse          script.db
broadcast-wsdd-discover.nse        http-vuln-cve2010-2861.nse          servicetags.nse
```

Navigate to the 'scipag_vulscan' directory and list the contents. The vulnerabilty scanner should be ready to use with nmap. Change directories back to the home directory.

```
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts$ cd scipag_vulscan/
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts/scipag_vulscan$ ls
_config.yml  cve.csv        logo.png     osvdb.csv  scipvuldb.csv      securitytracker.csv  update.sh  vulscan.nse
COPYING.TXT  exploitdb.csv  openvas.csv  README.md  securityfocus.csv  update.ps1           utilities  xforce.csv
rec0nrat@ubuntu-nessus:/usr/share/nmap/scripts/scipag_vulscan$ cd ~
rec0nrat@ubuntu-nessus:~$
```

Nmap can run scripts by using the '--scripts=<script>' option. Run the following command to use the vulnerability scanner.

```
sudo nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org
```

The vulnerability scanner will use pre-installed databases to generate results.
The following pre-installed databases are available at the moment:

- scipvuldb.csv - https://vuldb.com
- cve.csv - https://cve.mitre.org
- securityfocus.csv - https://www.securityfocus.com/bid/
- xforce.csv - https://exchange.xforce.ibmcloud.com/
- expliotdb.csv - https://www.exploit-db.com
- openvas.csv - http://www.openvas.org
- securitytracker.csv - https://www.securitytracker.com (end-of-life)

- osvdb.csv - http://www.osvdb.org (end-of-life

```
rec0nrat@ubuntu-nessus:~$ sudo nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 01:53 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.044s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed ports
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2012-5975] The SSH USERAUTH CHANGE REQUEST feature in SSH Tectia Server 6.0.4 through 6.0.20, 6.1.0 through 6.
```

Since there is a ton of input we should redirect the results to a file. This allows us to view and search the results more easily. Run the script again and save the output to 'scanme.nmap.org_vulnscan'.

```
sudo nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org >
scanme.nmap.org_vulnscan
```

```
rec0nrat@ubuntu-nessus:~$ sudo nmap -sV --script=vulscan/vulscan.nse scanme.nmap.org > scanme.nmap.org_vulnscan
rec0nrat@ubuntu-nessus:~$ ls
scanme.nmap.org_vulnscan
rec0nrat@ubuntu-nessus:~$
```

Now run a vulnerability scan on your local network using the following command and redirect the output to a file. Spend some time reviewing the scan results.

```
nmap -sV --script=vulscan/vulscan.nse <your network ID and CIDR>
```

```
rec0nrat@ubuntu-nessus:~$ sudo nmap -sV --script=vulscan/vulscan.nse 192.168.1.0/24 > 192.168.1.0_vulnscan
rec0nrat@ubuntu-nessus:~$
rec0nrat@ubuntu-nessus:~$
rec0nrat@ubuntu-nessus:~$ ls
192.168.1.0_vulnscan  scanme.nmap.org_vulnscan
rec0nrat@ubuntu-nessus:~$ less -i 192.168.1.0_vulnscan
```

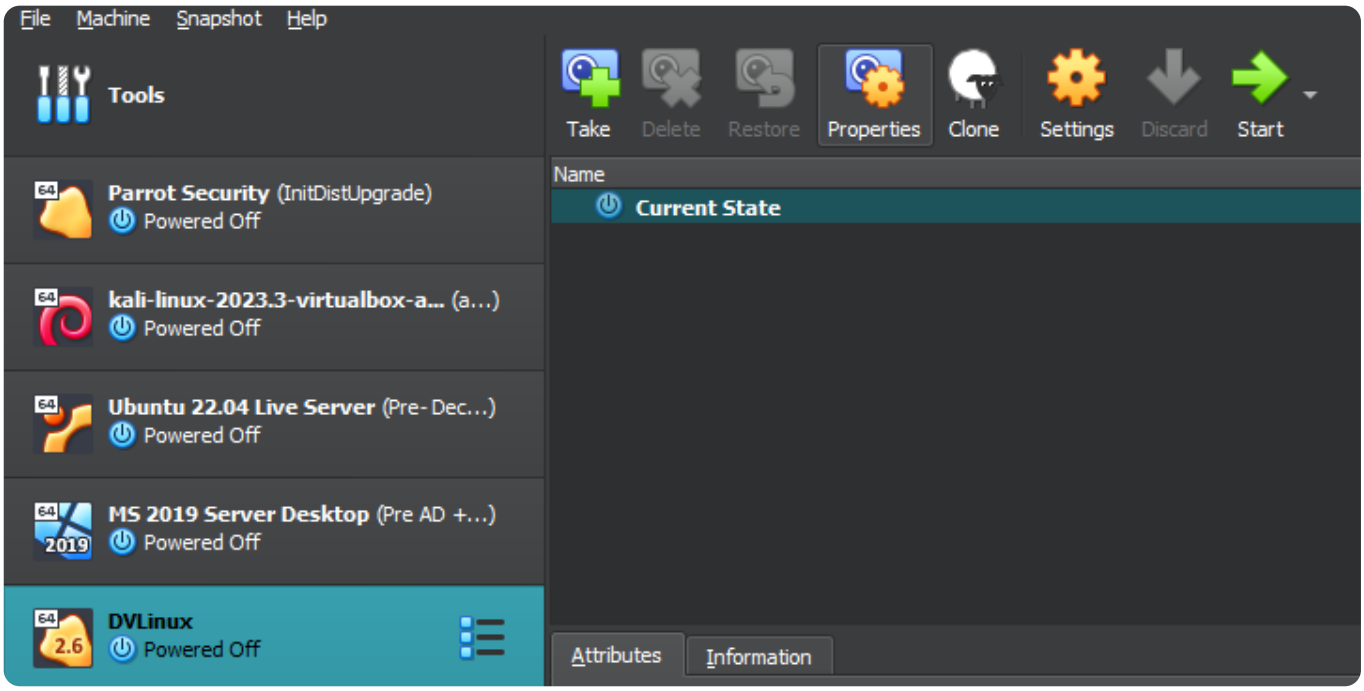
```
HCPINFORM while laStarting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 02:04 UTC
Stats: 0:02:32 elapsed; 252 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 02:07 (0:00:00 remaining)
Stats: 0:02:32 elapsed; 252 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 02:07 (0:00:00 remaining)
Stats: 0:02:32 elapsed; 252 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 02:07 (0:00:00 remaining)
Nmap scan report for LinksysRecHome (192.168.1.1)
Host is up (0.00077s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE     VERSION
53/tcp    open     domain      dnsmasq 2.78
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2013-0198] Dnsmasq before 2.66test2, when used with certain libvirt configurations, replies to queries from pr
ohibited interfaces, which allows remote attackers to cause a denial of service (traffic amplification) via spoofed T
CP based DNS queries.  NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3411.
| [CVE-2012-3411] Dnsmasq before 2.63test1, when used with certain libvirt configurations, replies to requests from p
rohibited interfaces, which allows remote attackers to cause a denial of service (traffic amplification) via a spoofe
d DNS query.
```

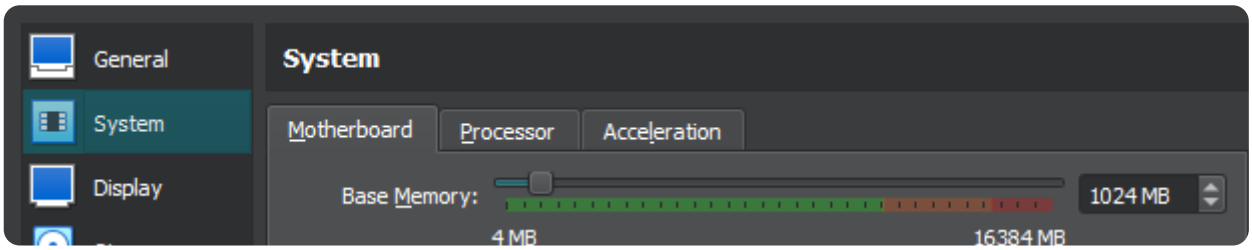
Lets run a scan against a purposely vulnerable machine. We will be downloading a version of Linux called “DamnVulnerableLinux”. You’ll never be “INSTALLING” the DVL operating system. You just boot to the ISO to make it work.

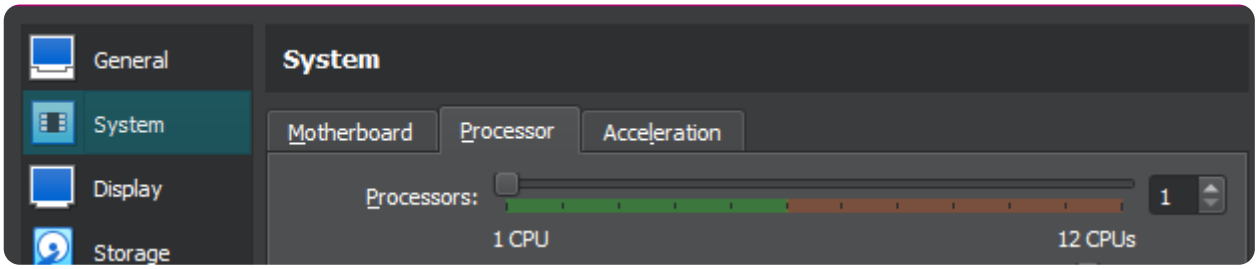
You can follow this walk through if you want:
https://www.computersecuritystudent.com/SECURITY_TOOLS/DVL/lesson1/index.html

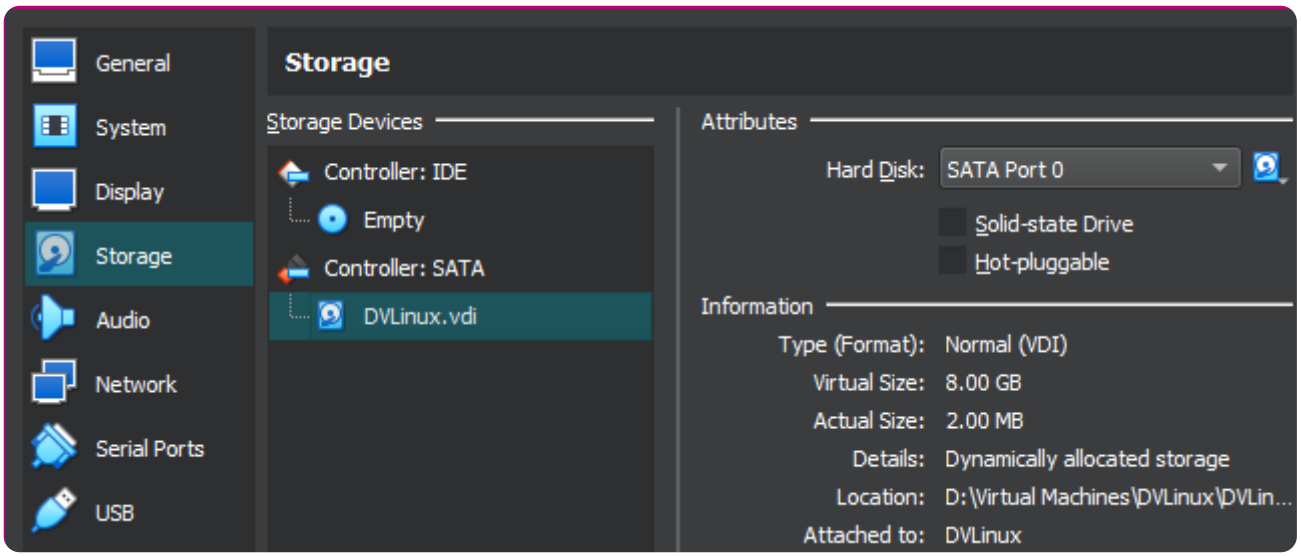
Download DVL 1.5
https://download.vulnhub.com/dvl/DVL_1.5_Infectious_Disease.iso

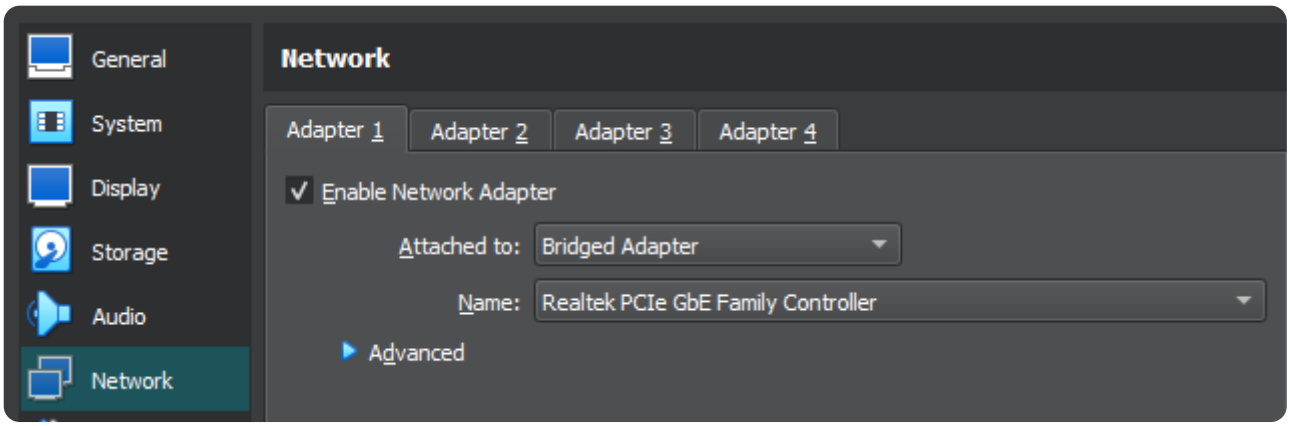
1. Create a NEW VM
2. Load the ISO into the VM
3. Set the memory to 512m
4. Set 1 Core of CPU
5. 8gb for Storage
6. Set Networking to BRIDGED
7. When you see BOOT: in the CLI, just hit the ENTER KEY
    1. a. This will boot you into the DVL
8. Username will be root
9. Password will be toor

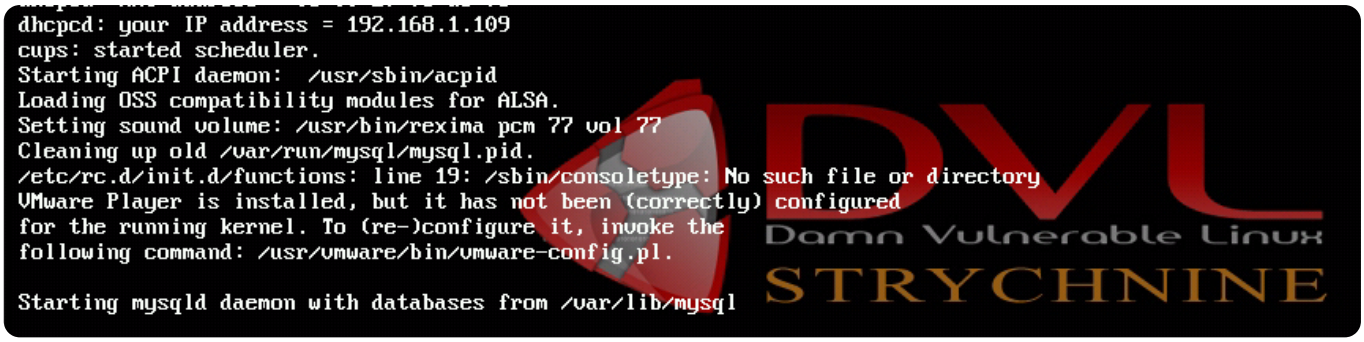

File Machine Snapshot Help
Tools
Take Delete Restore Properties Clone Settings Discard Start
Name
Current State
Parrot Security (InitDistUpgrade)
Powered Off
kali-linux-2023.3-virtualbox-a... (a...)
Powered Off
Ubuntu 22.04 Live Server (Pre-Dec...)
Powered Off
MS 2019 Server Desktop (Pre AD +...)
Powered Off
DVLinux
Powered Off
Attributes Information

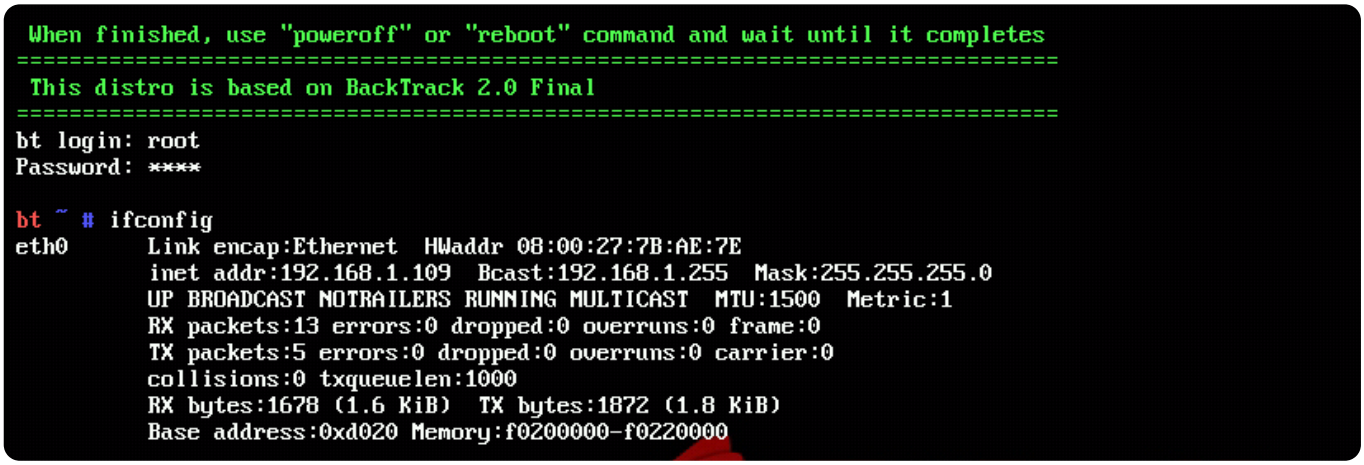

General
System
Display
System
Motherboard Processor Acceleration
Base Memory:
1024 MB
4 MB
16384 MB


General
System
Display
Storage
System
Motherboard Processor Acceleration
Processors:
1
1 CPU
12 CPUs


General
System
Display
Storage
Audio
Network
Serial Ports
USB
Storage
Storage Devices
Controller: IDE
Empty
Controller: SATA
DVLinux.vdi
Attributes
Hard Disk:
SATA Port 0
Solid-state Drive
Hot-pluggable
Information
Type (Format): Normal (VDI)
Virtual Size: 8.00 GB
Actual Size: 2.00 MB
Details: Dynamically allocated storage
Location: D:\Virtual Machines\DVLinux\DVLin...
Attached to: DVLinux







Once downloaded and the VM is setup use 'ifconfig' to find the IP addresss for the DVL. Run the vulnerability scanner against the IP address you just located. Review the output of the scan.

```
nmap -sV --script=vulscan/vulscan.nse <your DVL ip address>
```

```
rec0nrat@ubuntu-nessus:~$ sudo nmap -sV --script=vulscan/vulscan.nse 192.168.1.109
[sudo] password for rec0nrat:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-15 02:27 UTC
Nmap scan report for 192.168.1.109
Host is up (0.000069s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
631/tcp  open  ipp     CUPS 1.1
|_http-server-header: CUPS/1.1
| vulscan: VulDB - https://vuldb.com:
| [102573] Adam Kropelin adk0212 APC UPS Daemon up to 3.14.14 apcupsd.exe access control
| [20177] APC apcupsd 3.8.5 vsprintf memory corruption
| [20070] pdftops xpdf/xpdf-i/CUPS integer coercion
| [16450] APC apcupsd 3.7.2 Process ID File apcupsd.pid path traversal
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2009-1196] The directory-services functionality in the scheduler in CUPS 1.1.17 and 1.1.22 allows remote attac
kers to cause a denial of service (cupsd daemon outage or crash) via manipulations of the timing of CUPS browse packe
ts, related to a "pointer use-after-delete flaw."
| [CVE-2009-0791] Multiple integer overflows in Xpdf 2.x and 3.x and Poppler 0.x, as used in the pdftops filter in CU
```

Run the command again and save the output to a file. Identify 3 vulnerabilities and generate a short executive summary on each.

```
rec0nrat@ubuntu-nessus:~$ sudo nmap -sV --script=vulscan/vulscan.nse 192.168.1.109 > dvl_vulscan
rec0nrat@ubuntu-nessus:~$ ls
192.168.1.0_vulnscan  dvl_vulscan  scanme.nmap.org_vulnscan
rec0nrat@ubuntu-nessus:~$ less -i dvl_vulscan
```

```
| [20070] pdftops xpdf/xpdf-i/CUPS integer coercion
| [16450] APC apcupsd 3.7.2 Process ID File apcupsd.pid path traversal
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2009-1196] The directory-services functionality in the scheduler in CUPS 1.1.17 and 1.1.22 allows remote attac
kers to cause a denial of service (cupsd daemon outage or crash) via manipulations of the timing of CUPS browse packe
ts, related to a "pointer use-after-delete flaw."
| [CVE-2009-0791] Multiple integer overflows in Xpdf 2.x and 3.x and Poppler 0.x, as used in the pdftops filter in CU
PS 1.1.17, 1.1.22, and 1.3.7, GPdf, and kdegraphics KPDF, allow remote attackers to cause a denial of service (applic
ation crash) or possibly execute arbitrary code via a crafted PDF file that triggers a heap-based buffer overflow, po
ssibly related to (1) Decrypt.cxx, (2) FoFiTrueType.cxx, (3) gmem.c, (4) JBIG2Stream.cxx, and (5) PSOutputDev.cxx in
pdftops/. NOTE: the JBIG2Stream.cxx vector may overlap CVE-2009-1179.
| [CVE-2009-0577] Integer overflow in the WriteProlog function in texttops in CUPS 1.1.17 on Red Hat Enterprise Linux
 (RHEL) 3 allows remote attackers to execute arbitrary code via a crafted PostScript file that triggers a heap-based
buffer overflow.  NOTE: this issue exists because of an incorrect fix for CVE-2008-3640.
```

Vulnerabilities Discovered (3)

The out of date CUPS service allows a certain crafted UDP packet over IPP that causes a DoS, or service hang, to occur. Even though the impact of this attack is low the execution of the attack is easy to perform. The probability of this attack taking place in the near future is almost zero. This issue is best resolved by installing the latest version of CUPS. Solution: Update CUPS at https://www.cups.org/

```
| [CVE-2004-0558] The Internet Printing Protocol (IPP) implementation in CUPS before 1.1.21 allows remote attackers t
o cause a denial of service (service hang) via a certain UDP packet to the IPP port.
```

CVE-2004-0558

This report does not contain tags. Add tags via the comment box.

Details

cups-udp-dos (17389) **reported Sep 15, 2004**

The Common Unix Printing System (CUPS) is vulnerable to a denial of service attack. By sending a specially-crafted UDP packet to the IPP port, a remote attacker could cause a denial of service.

Consequences:

Denial of Service

CVSS 1.0 Base Score

3.5

Access Vector	Remote
Access Complexity	Low
Authentication	Not Required
Confidentiality Impact	None
Integrity Impact	None
Availability Impact	Partial

For Slackware Linux:
Upgrade to the latest cups package, as listed below. Refer to slackware-security Mailing List, Wed, 22 Sep 2004 13:38:36 -0700 (PDT) for more information. See References.

Slackware Linux 9.1, 10 and -current: 1.1.21-i486 or later

Remedy

Upgrade to the latest version of CUPS (1.1.21 or later), available from the CUPS Web site. See References.

Vulnerability Details : CVE-2004-0558

The Internet Printing Protocol (IPP) implementation in CUPS before 1.1.21 allows remote attackers to cause a denial of service (service hang) via a certain UDP packet to the IPP port.

Published 2004-09-28 04:00:00 Updated 2018-03-13 01:29:00 Source MITRE

View at NVD, CVE.org

Vulnerability category: Denial of service

Exploit prediction scoring system (EPSS) score for CVE-2004-0558

Probability of exploitation activity in the next 30 days: 3.72%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 91 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2004-0558

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
5.0	MEDIUM	AV:N/AC:L/Au:N/C:N/I:N/A:P	10.0	2.9	NIST

The XAMPP default accounts are using using default credentials. XAMPP is a web server solution stack package. An attacker can find these credentials via a basic internet search and gain access or information regarding the different services. The default credentials are listed below in the screen capture. This attack is trivial to perform and could possibly lead to major network compromise or data loss. The probability of this attack occurring is very low but is easy to resolve. The solution is to find any default credentials installed deployed by XAMPP and update them.

Solution: Audit the accounts via XAMPP and update using strong, complicated passwords. There should be no default credentials.

```
| [CVE-2009-0919] XAMPP installs multiple packages with insecure default passwords, which makes it easier for remote
attackers to obtain access via (1) the "lampp" default password for the "nobody" account within the included ProFTPD
installation, (2) a blank default password for the "root" account within the included MySQL installation, (3) a blank
 default password for the "pma" account within the phpMyAdmin installation, and possibly other unspecified passwords.
  NOTE: this was originally reported as a problem in DFLabs PTK, but this issue affects any product that is installed
 within the XAMPP environment, and should not be viewed as a vulnerability within that product. NOTE: DFLabs states t
hat PTK is intended for use in a laboratory with "no contact from / to internet."
```

CVE-ID

CVE-2009-0919 — Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

XAMPP installs multiple packages with insecure default passwords, which makes it easier for remote attackers to obtain access via (1) the "lampp" default password for the "nobody" account within the included ProFTPD installation, (2) a blank default password for the "root" account within the included MySQL installation, (3) a blank default password for the "pma" account within the phpMyAdmin installation, and possibly other unspecified passwords. NOTE: this was originally reported as a problem in DFLabs PTK, but this issue affects any product that is installed within the XAMPP environment, and should not be viewed as a vulnerability within that product. NOTE: DFLabs states that PTK is intended for use in a laboratory with "no contact from / to internet."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Vulnerability Details : CVE-2009-0919

XAMPP installs multiple packages with insecure default passwords, which makes it easier for remote attackers to obtain access via (1) the "lampp" default password for the "nobody" account within the included ProFTPD installation, (2) a blank default password for the "root" account within the included MySQL installation, (3) a blank default password for the "pma" account within the phpMyAdmin installation, and possibly other unspecified passwords. NOTE: this was originally reported as a problem in DFLabs PTK, but this issue affects any product that is installed within the XAMPP environment, and should not be viewed as a vulnerability within that product. NOTE: DFLabs states that PTK is intended for use in a laboratory with "no contact from / to internet."

Published 2009-03-16 19:30:01 Updated 2017-08-17 01:30:06 Source MITRE

View at NVD, CVE.org

Exploit prediction scoring system (EPSS) score for CVE-2009-0919

Probability of exploitation activity in the next 30 days: 1.06%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 82 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2009-0919

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST

A SQL injection is possible by sending a SQL statement to the index.php script using the id_kat parameter in the PHPWebNews plugin. It is extremely easy to exploit this vulnerability and could cause data loss or manipulation. The impact of this attack high and could easily lead to leaked/stolen credentials. Below is a screen shot of a publicly available exploit designed to steel usernames and password hashes. This vulnerability effects PHPWebNew 0.1-0.2. The probability of this exploit being seen in the near future very low but it could have serious consequences. As of yet there is no update for the plugin to resolve the issue. My recommendatio is to discontue use of the PHPWebNews plugin.

Solution: Discontinue use of PHPWebNews plugin.

```
| [CVE-2008-6813] SQL injection vulnerability in index.php in phpWebNews 0.2 MySQL Edition allows remote attackers to
 execute arbitrary SQL commands via the id_kat parameter.
```

CVE-2008-6813 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

SQL injection vulnerability in index.php in phpWebNews 0.2 MySQL Edition allows remote attackers to execute arbitrary SQL commands via the id_kat parameter.

QUICK INFO

CVE Dictionary Entry:
CVE-2008-6813
NVD Published Date:
05/22/2009
NVD Last Modified:
09/28/2017
Source:
MITRE

Vulnerability Details : CVE-2008-6813

SQL injection vulnerability in index.php in phpWebNews 0.2 MySQL Edition allows remote attackers to execute arbitrary SQL commands via the id_kat parameter.

Published 2009-05-22 11:52:39 Updated 2017-09-29 01:33:22 Source MITRE

View at NVD, CVE.org

Vulnerability category: Sql Injection

Exploit prediction scoring system (EPSS) score for CVE-2008-6813

Probability of exploitation activity in the next 30 days: 0.06%

Percentile, the proportion of vulnerabilities that are scored at or less: ~ 26 % EPSS Score History EPSS FAQ

CVSS scores for CVE-2008-6813

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST

X-Force Vulnerability Report

phpwebnews index.php SQL injection

CVE-2008-6813

This report does not contain tags. Add tags via the comment box.

Details

phpwebnews-index-sql-injection (43684) **reported Jul 3, 2008**

phpwebnews is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements to the index.php script using the id_kat parameter, which could allow the attacker to view, add, modify or delete information in the back-end database.

Consequences:

Data Manipulation

Remedy

No remedy available as of September 1, 2014.

CVSS 2.0 Base Score

7.5

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS 2.0 Temporal Score

7.1

Exploitability	High
Remediation Level	Unavailable
Report Confidence	Uncorroborated

PHPwebnews 0.2 MySQL Edition - 'id_kat' SQL Injection

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
5998	2008-6813	STORM	WEBAPPS	PHP	2008-07-03

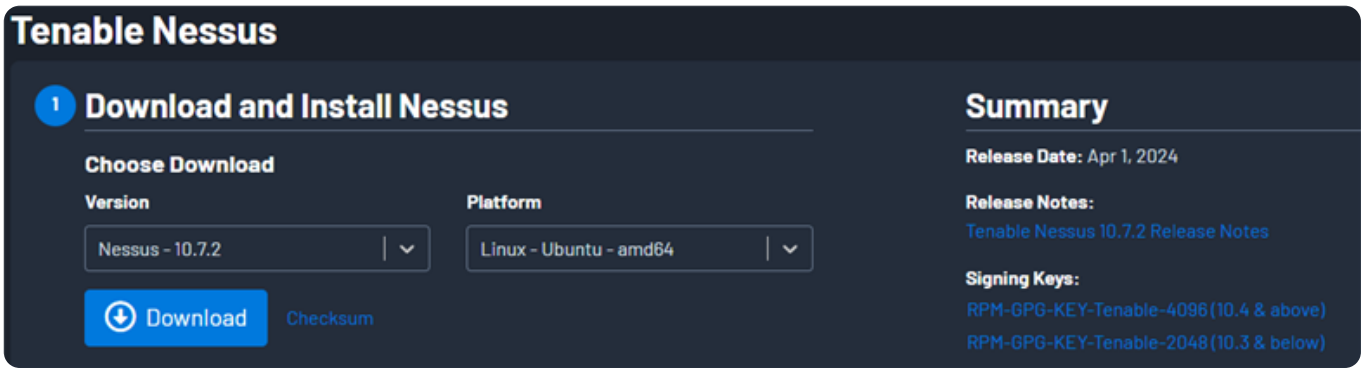
```
Exploit found by sToRm


phpWebNews v0.2 MySQL Edition (Surat kabar/News Management Online)
SQL Injection


SQL Injection
-------------

index.php?id_kat=null+UNION+ALL+SELECT+1,2,3,4,concat(user,0x3a,passwd),6,7,8,9,10,11,12,13+FROM+user--


$id_kat=$_GET[id_kat];
$m_conn = db_connect();
if ((empty($id_kat))||($id_kat==''))
    $m_sql = "select * from berita where status='tampil' and order by tgl desc";
else
    $m_sql = "select * from berita where status='tampil' and kode_kategori=$id_kat and isi_berita like %'$m_txt'% order by tgl desc";


Here, we have a classic SQL MySQL injection.  The GET variable "id_kat" isn't sanitized before being passed to the query.  By injecting our string, the query becomes:

select * from berita where status='tampil' and kode_kategori=null UNION ALL SELECT 1,2,3,4,concat(user,0x3a,passwd),6,7,8,9,10,11,12,13 FROM user-- and isi_berita like %'$m_txt'% order by tgl desc

The comment renders the rest of the query to be useless.  We are effectively grabbing the first user from the table "user", which is the admin.  You can inject the other strings with server variables and attempt
to fetch mysql.user hashes, if the conditions apply.

# milw0rm.com [2008-07-03]
```

https://www.exploit-db.com/exploits/5998

Exercise 2 -

Task 1 - Download Nessus Installer

From your Host OS, navigate in your browser to https://www.tenable.com/downloads/nessus?loginAttempted=true.
Select Nessus 10.7.0 on the Linux – Ubuntu – amd64 Platform



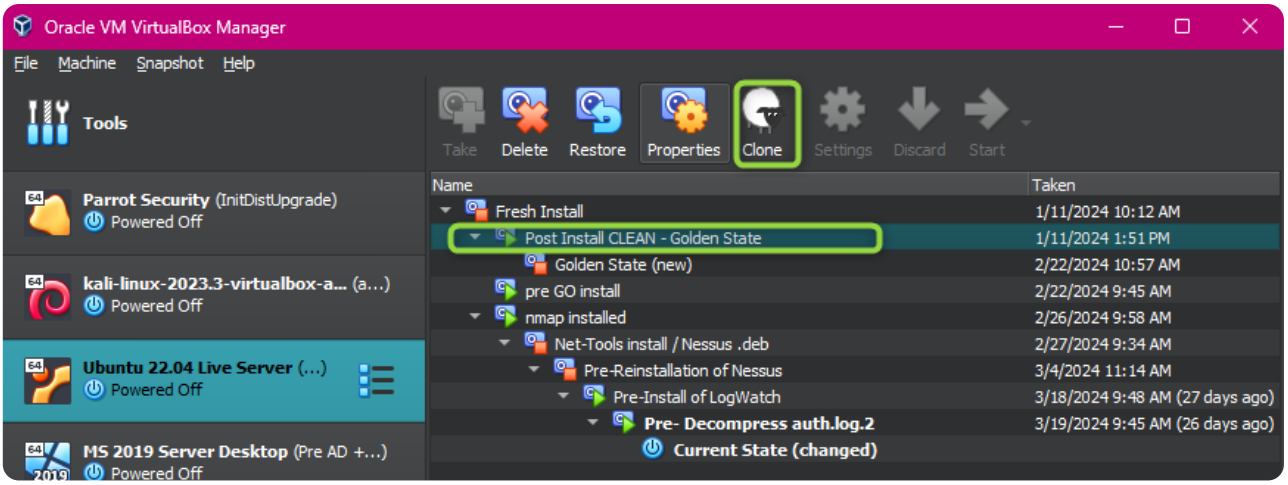
Once the installer file is downloaded to your host machine we need to use 'scp' to copy the file to the Linux server that we will use to run Nessus.

Task 2 - Clone Ubuntu Server

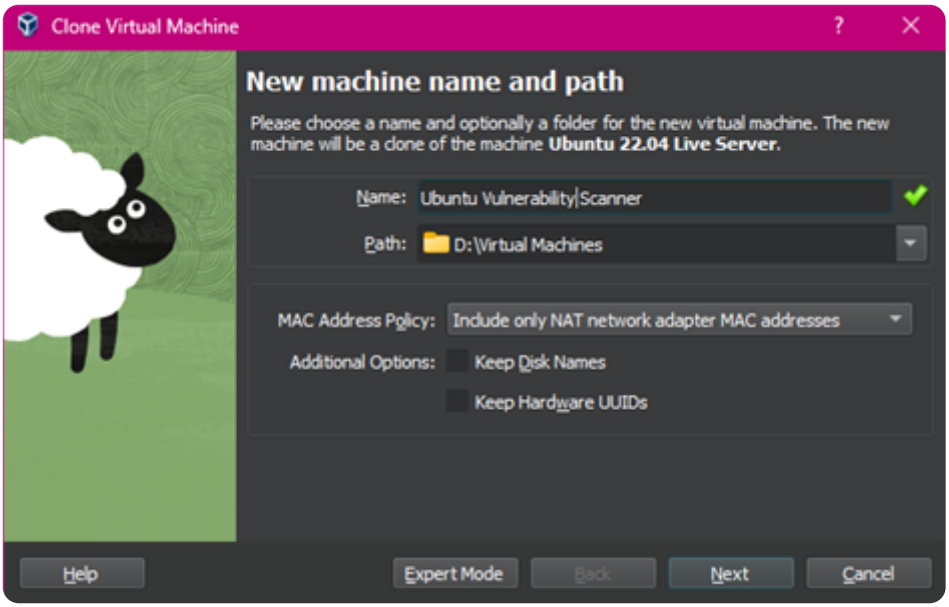
First thing we are going to do is CLONE your Ubuntu Server VM from its original CLEAN snapshot.

By creating a "Golden State" snapshot of a VM it is trivial and quick to create a clone. The new VM should only take a few minutes to clone and run.

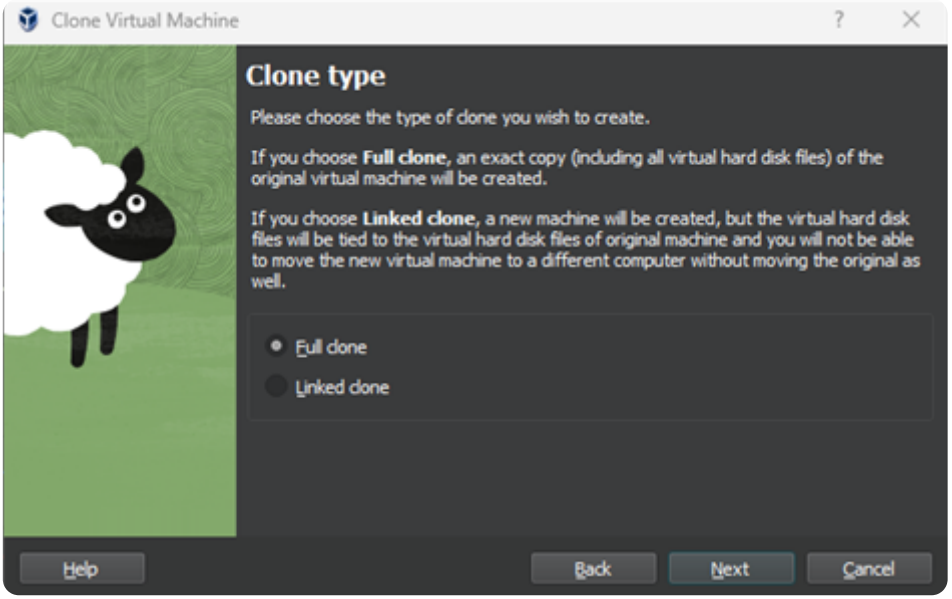
1. Load up the Virtual Box VirtualBox Manager
2. Power off all VM's in Virtual Box
3. Select the Ubuntu Server VM object on the left hand side
   1. Select the button on the right hand side and have the snapshots loaded in the details pane.



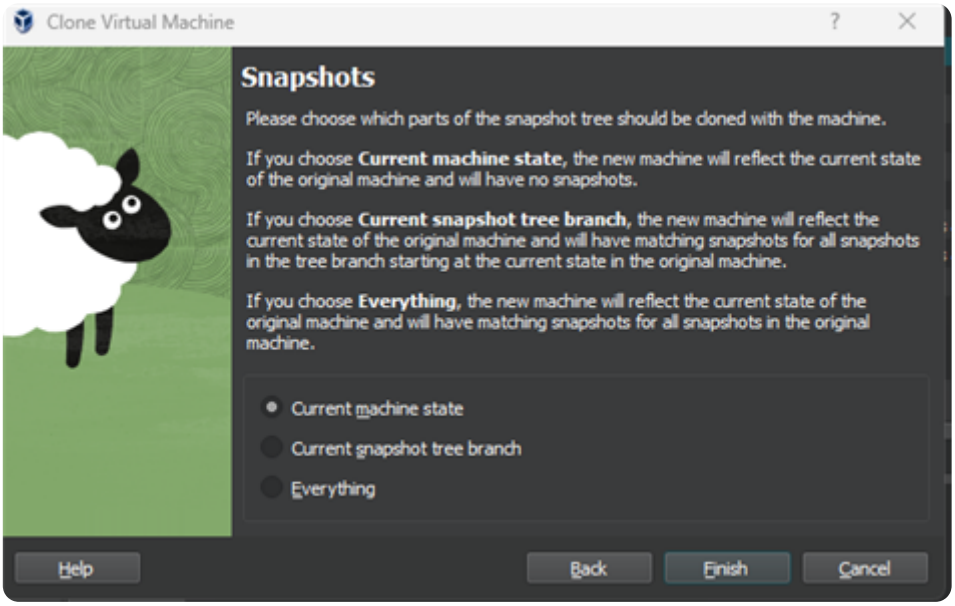
4. Select a snapshot, in the right-side window, that is the best clean installation you have.
5. Once selected click the 'Clone' button with the sheep.
6. Rename the new VM something along the lines of "Ubuntu Vulnerability Scanner" and click 'Next'.



7. Make sure 'Full clone' is selected and click 'Next'.



8. Select 'Current machine state' and click 'Finish'.



This will create a clean image of your server. The clone will take only a minute to deploy. This is how IT professionals are able to spin-up new systems in minutes reliably. Double check that all the settings for the cloned server are correct. They should be the same as the original VM but if you need to make changes this is also the time to do that.

Task 3

Prerequisites:

- Ubuntu Server 22.04 Installed, Updated, Upgraded and running in Virtual Box

- Ubuntu Guest VM Networking settings is set to Bridged Mode in Virtual Box
- The Ubuntu Guest VM is running
- Have an open CLI in your HOST OS, and test that you can SSH into the Guest VM

Powerup your new VM and ssh into the server via your Host terminal. Pull up another command prompt and navigate to the location of the nessus installer file you downloaded in task 1. List the contents of the directory to prove that the file is there. Now 'scp' the file to the Linux server. If you need a reference for using 'scp' use the link below. https://linuxize.com/post/how-to-use-scp-command-to-securely-transfer-files/

```
PS C:\Users\tyler> cd "D:\Virtual Machines"
PS D:\Virtual Machines> dir


    Directory: D:\Virtual Machines


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          2/8/2024   8:26 PM                AntiSyphon Training
d-----          6/4/2021   3:09 PM                Backgrounds
d-----          6/7/2021   7:59 PM                Ducky Scripts
```

```
PS D:\Virtual Machines> dir *.deb


    Directory: D:\Virtual Machines


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/27/2024   9:30 AM       68540738 Nessus-10.7.0-ubuntu1404_amd64.deb
-a----         4/14/2024  10:47 PM       69388694 Nessus-10.7.2-ubuntu1404_amd64.deb


PS D:\Virtual Machines> scp .\Nessus-10.7.2-ubuntu1404_amd64.deb rec0nrat@192.168.1.220:
rec0nrat@192.168.1.220's password:
Nessus-10.7.2-ubuntu1404_amd64.deb                                            100%   66MB  42.2MB/s   00:01
PS D:\Virtual Machines>
```

```
rec0nrat@ubuntu-nessus:~$ ls -l Nessus*
-rw-rw-r-- 1 rec0nrat rec0nrat 69388694 Apr 15 05:47 Nessus-10.7.2-ubuntu1404_amd64.deb
rec0nrat@ubuntu-nessus:~$
```

Task 4

The .deb file is not executable and needs it's permissions modified so that we can run the installer. This is due to the fact that the file was downloaded over the internet and Linux is protecting us from executing it immediately after download. Use 'chmod +x <file>' to add execute permissions to the file.

```
rec0nrat@ubuntu-nessus:~$ chmod +x Nessus-10.7.2-ubuntu1404_amd64.deb
rec0nrat@ubuntu-nessus:~$ ls
192.168.1.0_vulnscan  dvl_vulscan  Nessus-10.7.2-ubuntu1404_amd64.deb  scanme.nmap.org_vulnscan
rec0nrat@ubuntu-nessus:~$
```

It's time to install and setup the Nessus vulnerability scanner. We'll use the following walkthrough as a reference for installation.
https://docs.tenable.com/nessus/Content/InstallNessusLinux.htm

The install guide above requires the use of 'dpkg' to install the .deb file. With 'dpkg' there are a couple flags you will probably use when installing a program. The first is the '-i' flag which means install. The '-r' flag removes, or uninstalls, a program. To list installed packages use the '-l' flag. When listing packages there are quite a few of them so use grep to display only packages you are interested in. If you are having dependency issues try running 'sudo apt install -f' which will attempt to fix broken dependencies.

Use 'dpkg -i' to install Nessus.

```
rec0nrat@ubuntu-nessus:~$ sudo dpkg -i Nessus-10.7.2-ubuntu1404_amd64.deb
dpkg: warning: files list file for package 'nessus' missing; assuming package has no files currently installed
(Reading database ... 146478 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.2) over (10.7.1) ...
Setting up nessus (10.7.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
```

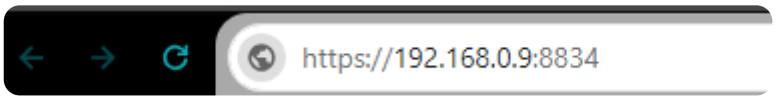
```
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
{"pid":2146,"time":1713163159761,"tid":1,"msg":"Warning: Long rDNS lookup.  Took 10018ms for 192.168.1.220 (failed)",
"severity":"INFO"}
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://ubuntu-nessus:8834/ to configure your scanner

rec0nrat@ubuntu-nessus:~$
```

All the setup processes should read pass, especially INSTALL. If that is true then you have successfully installed Nessus. At the bottom of the output you see that the Nessus service needs to be started. Also to configure and run Nessus you will need to navigate to the serving IP specifying port '8834'.

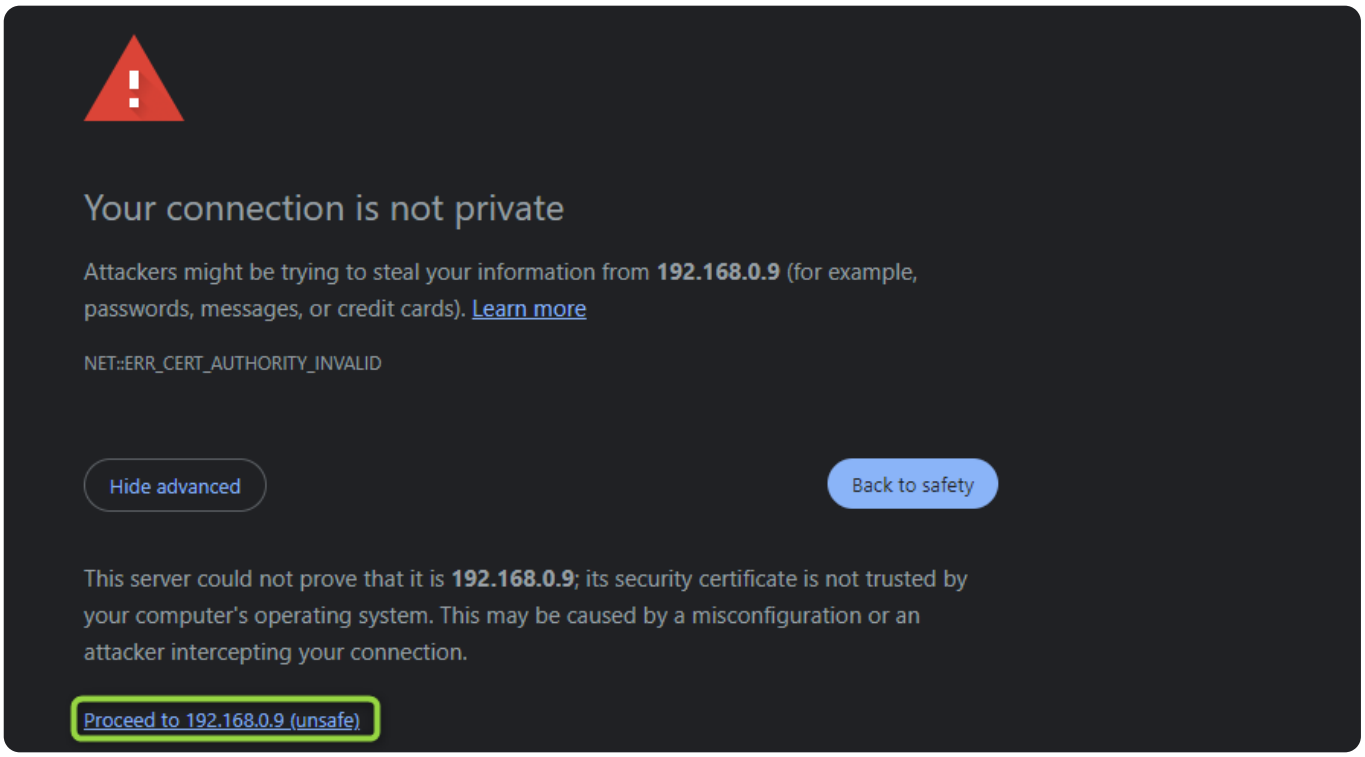
In order to start the service we need to use 'systemctl'. Use the 'start' option to begin the 'nessus' service. You will need to use root permissions to start the service. Check the status of the service after starting it to confirm that the nessus service is running.

```
rec0nrat@ubuntu-nessus:~$ sudo systemctl start nessusd.service
rec0nrat@ubuntu-nessus:~$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-04-15 06:50:45 UTC; 8s ago
   Main PID: 2259 (nessus-service)
      Tasks: 12 (limit: 9389)
     Memory: 46.0M
        CPU: 2.594s
     CGroup: /system.slice/nessusd.service
             ├─2259 /opt/nessus/sbin/nessus-service -q
             └─2260 nessusd -q

Apr 15 06:50:45 ubuntu-nessus systemd[1]: Started The Nessus Vulnerability Scanner.
Apr 15 06:50:52 ubuntu-nessus nessus-service[2260]: Cached 0 plugin libs in 0msec
Apr 15 06:50:52 ubuntu-nessus nessus-service[2260]: Cached 0 plugin libs in 0msec
rec0nrat@ubuntu-nessus:~$
```

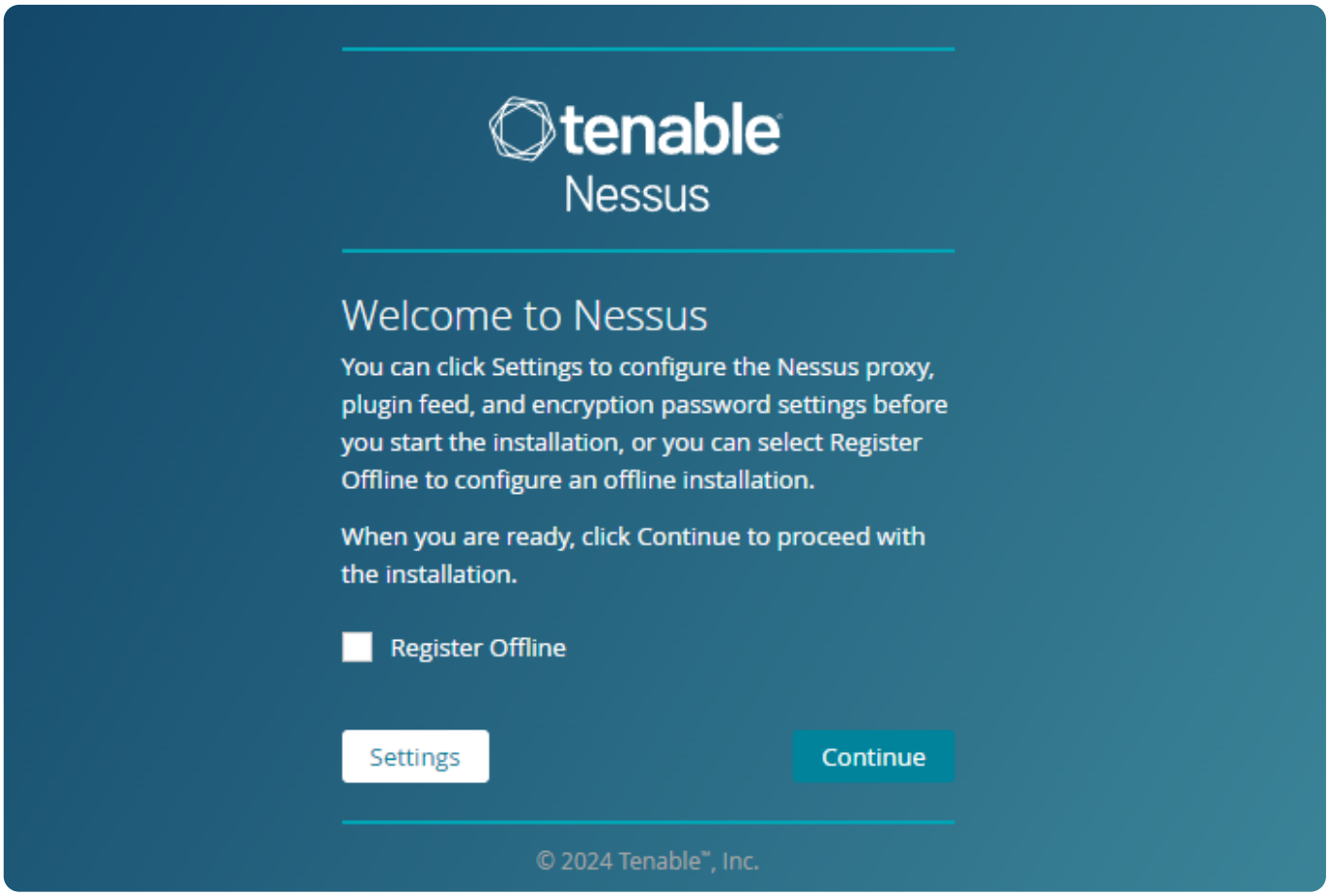
It appears that nessus is active and running. We need to navigate to the nessus browser interface over https on port 8834. Open the browser and navigate to 'https://<server ip>:8834'.



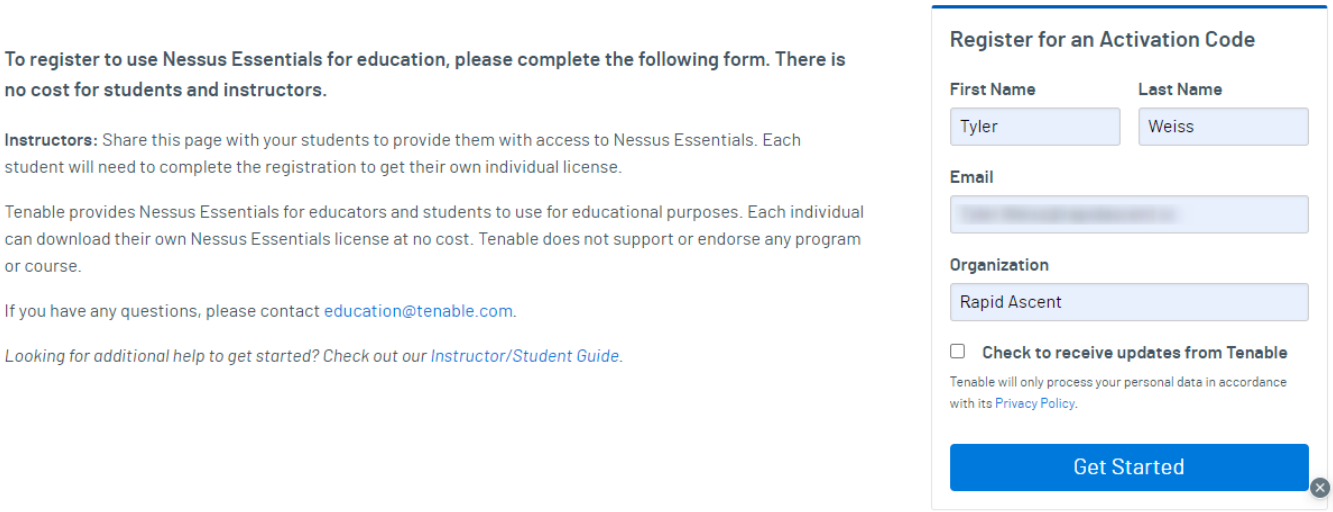
You should see a page that says 'Your connection is not private'. All this means is that we do not have a valid digital certificate. This is just a warning and since we are no going to go through the trouble of validating a cert for the local server we can ignore this. Click the 'Advanced' button and then click the link 'Proceed to <IP> (unsafe)' .



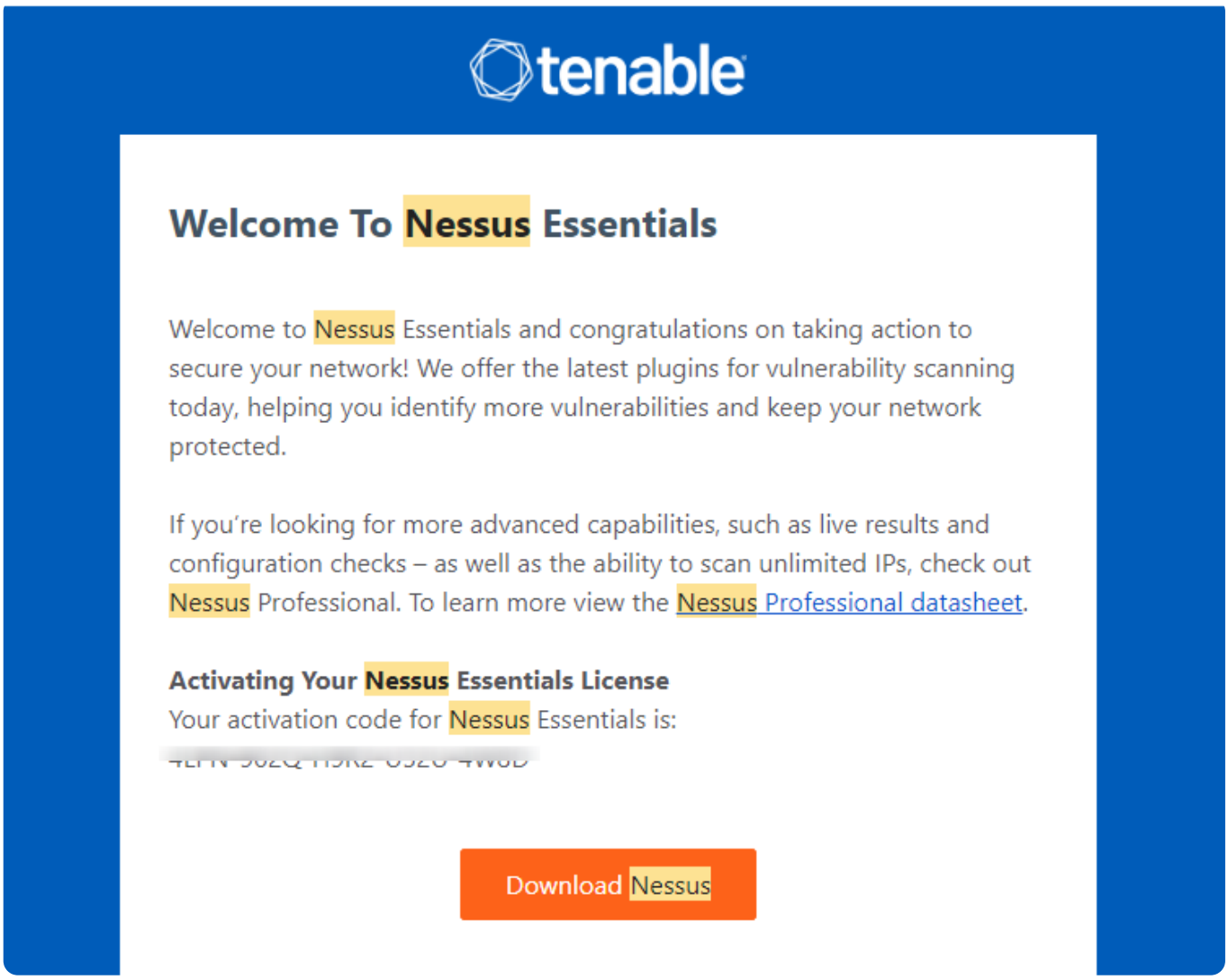
You should see a welcome screen like the one below. But before you continue you need to register an account with tenable for a an "Essentials Edition" of Nessus so that you can obtain a product key. This license can not be used for commercially by the way, it's just for educational purposes.



Register an educational account here:
https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true



You should recieve an email from Tennable that has your activation code.



tenable

Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

Activating Your Nessus Essentials License

Your activation code for Nessus Essentials is:

Download Nessus

Go back to the nessus web interface and click 'Next'. Select the radio button that says 'Nessus Essentials' and click 'Next'. Register if you have not already and click 'Next'. Enter you activation code and click 'Continue'.

tenable
Nessus

Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ○ Nessus Expert
- ○ Nessus Professional
- ○ Nessus Manager
- ◉ Nessus Essentials
- ○ Managed Scanner

Back Continue

tenable
Nessus Essentials

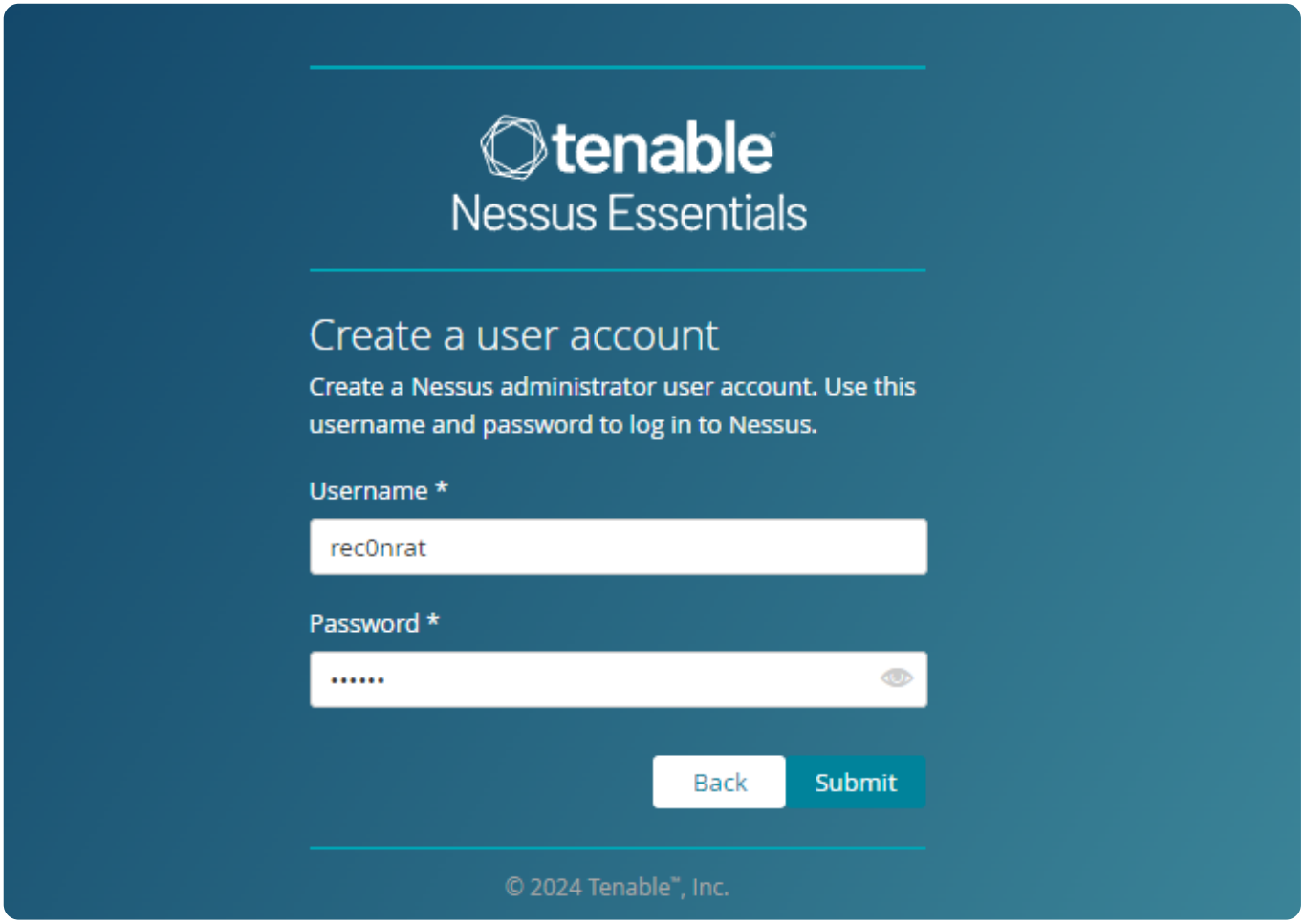
Register Nessus

Enter your activation code.

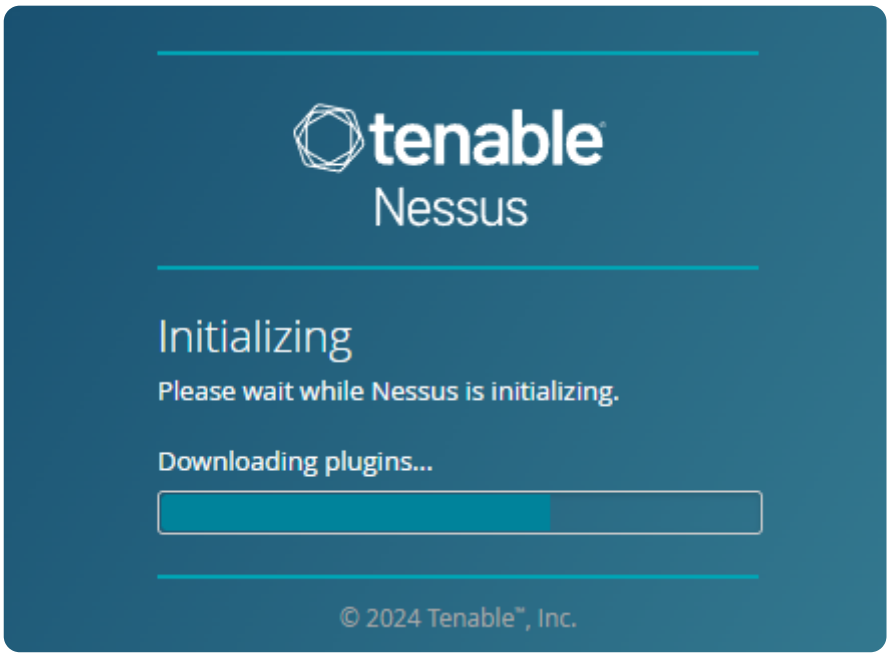
Activation Code *

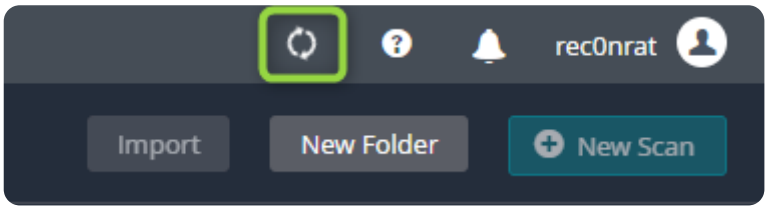
Back Continue

Create a local user account by filling in the account information and click 'Submit'. These are the credentials you will use to sign in to your Nessus interface in the browser.

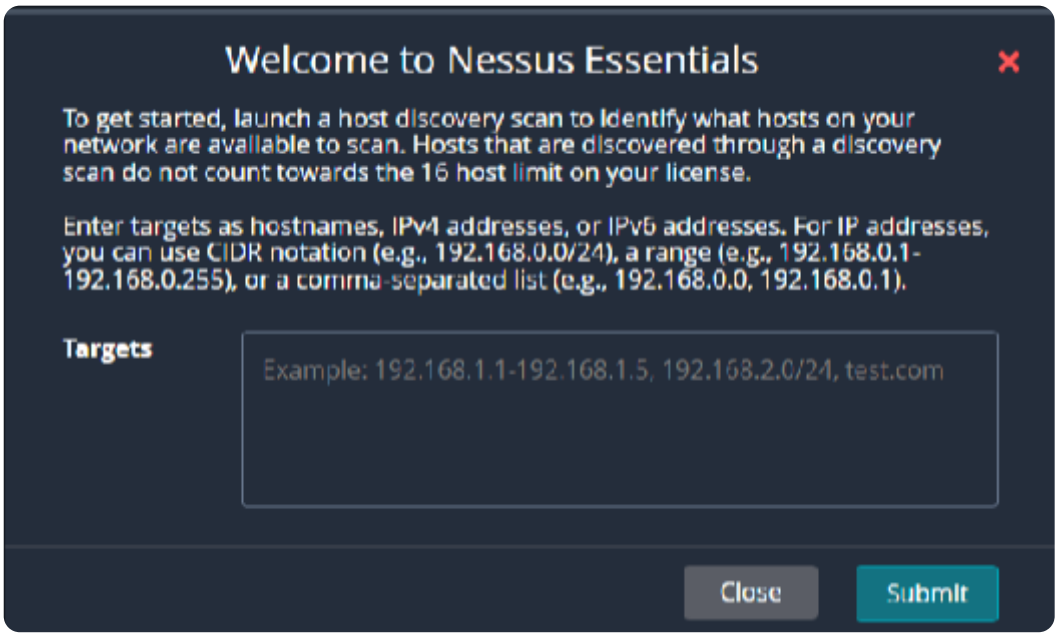


Nessus will begin initializing and starting the setup process. After it is done the dashboard will appear. You should notice a couple rotating arrows in the upper right corner the dashboard. This is because plugins for Nessus are downloading and installing. This may take roughly 30 minutes or so depending on your internet connection. You will have restricted functionality during the install process and can not yet run scans.





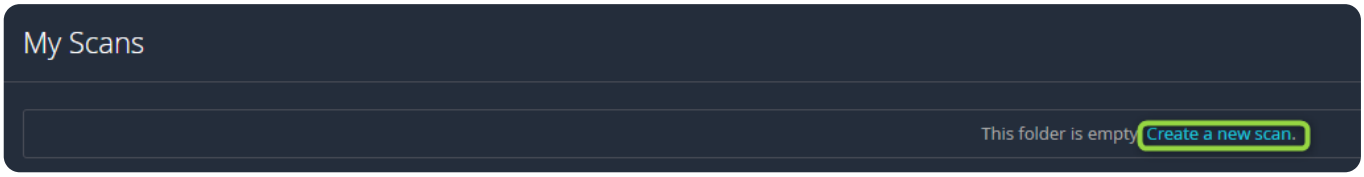
When the initial install is finished a popup, like the one below, will appear. This is telling you that setup has completed and you are now able to use Nessus. Also 16 host scan limit for the license. Do not go and scan everything because you will reach this limit very quickly.

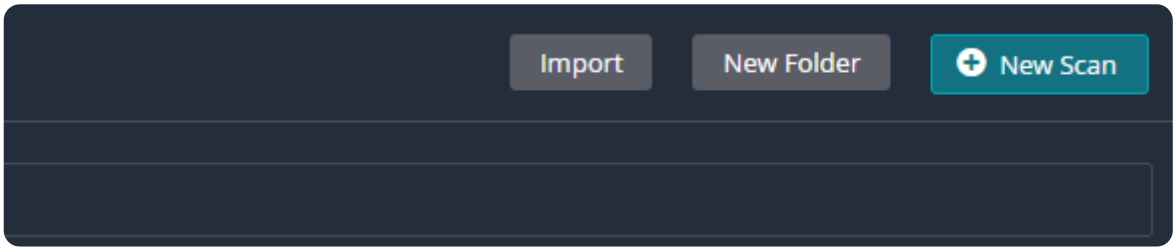


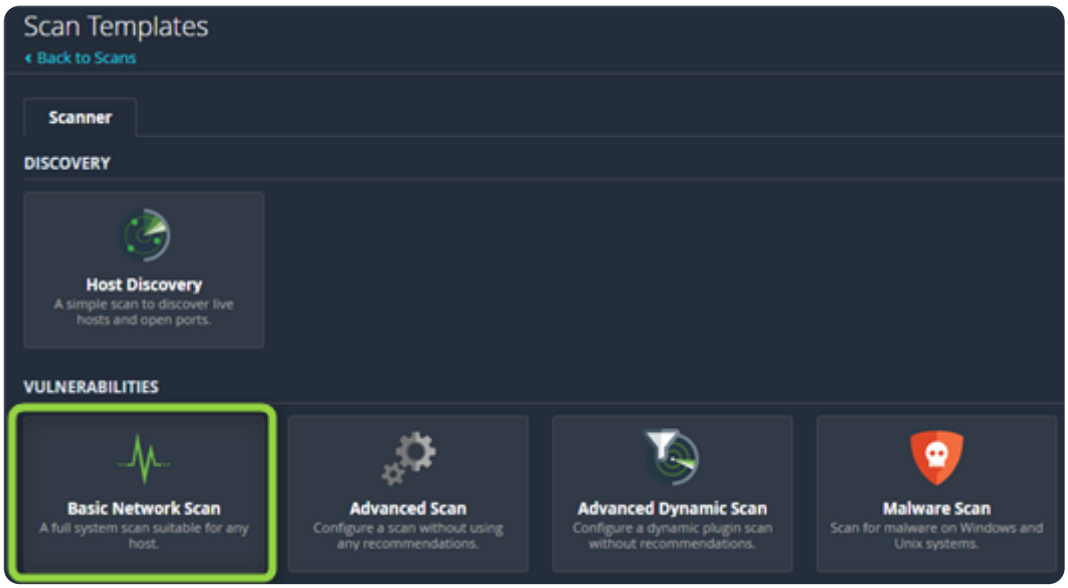
Exercise 3 - Perform a Basic Scan with Nessus

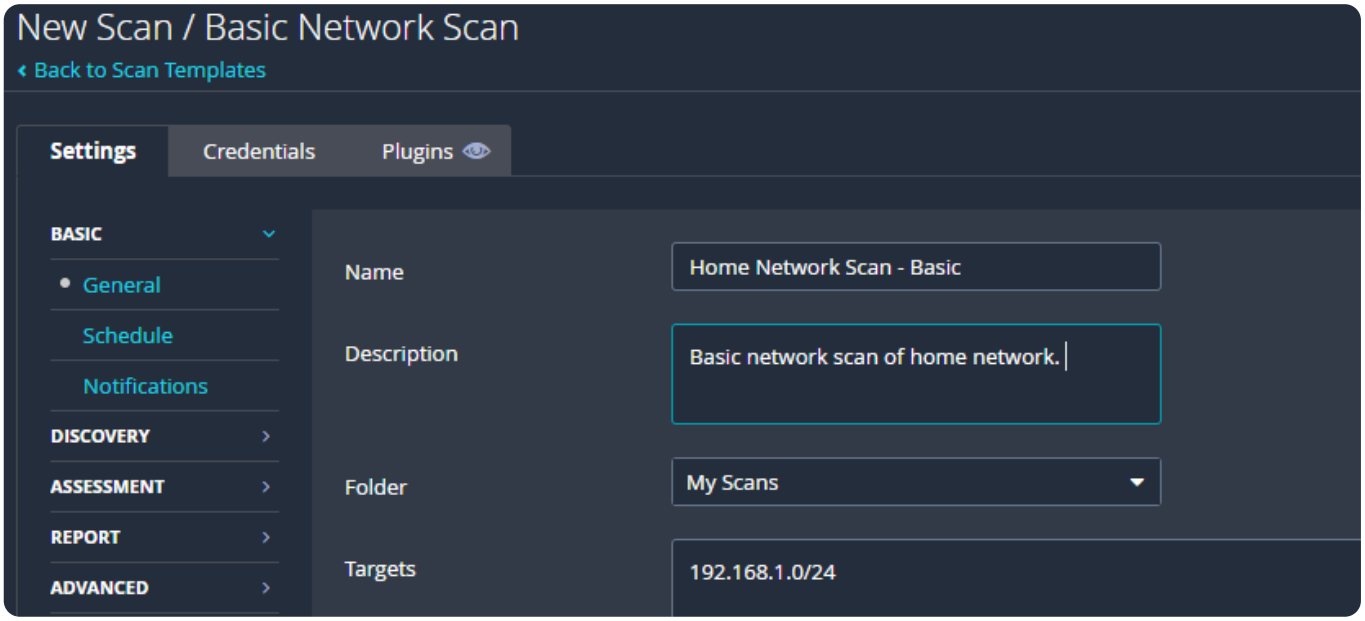
Task 1 - Conduct your first Vulnerability Scan (Home Network)

The first scan we'll conduct of our home network. Click the highlighted text 'Create new scan' under the my scans tab or use the 'New Scan' button. There are many different scans to choose from to include host discovery, basic, advanced, malware, specific vulnerability, and compliance scans. We will you the basic scan in this exercise. Click the 'Basic Network Scan' button and fill out the name of the scan along with the target IP range and description. You can use a list, range or CIDR notation to specify the target IP address. There is also an option to use a file for target input. After you are finished filling out the fields click the 'Save' button.

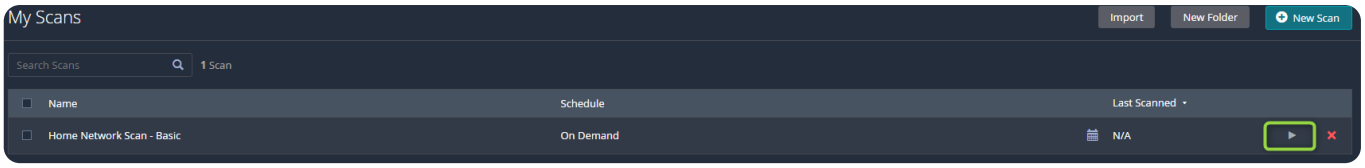








You should now see the newly created scan under the 'My Scans' folder. The scan object shows the scan name, scheduling, the last time the scan was run, the start on demand button and the delete option. you can schedule a scan to run weekly, daily, monthly, and so on. Automating scans can be very advantageous and a big time saver. Click the play button on the far right to begin the scan.



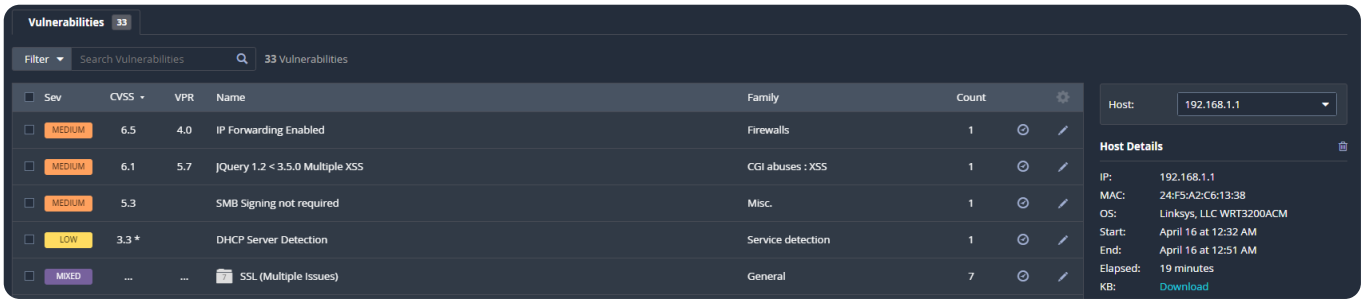
Here is the output of 'htop' run from the server CLI. You'll notice all the processes and threads from 'nessusd' running while the scan is being performed.

```
  0[||||||                                   9.5%]   Tasks: 32, 88 thr; 1 running
  1[|||||                                    9.5%]   Load average: 0.75 0.18 0.06
  2[||||                                     6.1%]   Uptime: 07:01:53
  3[||||                                     6.7%]
Mem[|||||||||||||||||||||||||||||||||||542M/7.75G]
Swp[                                        0K/0K]

  PID USER      PRI  NI  VIRT   RES   SHR S CPU%▽MEM%   TIME+  Command
 3693 root       20   0 1070M  238M 15496 S 34.0  3.0 37:04.53 nessusd -q
 3936 root       20   0 1070M  238M 15496 S  4.8  3.0  0:00.46 nessusd -q
 3938 root       20   0 1070M  238M 15496 S  4.1  3.0  0:00.45 nessusd -q
 3941 root       20   0 1070M  238M 15496 S  4.1  3.0  0:00.45 nessusd -q
 3943 root       20   0 1070M  238M 15496 S  4.1  3.0  0:00.47 nessusd -q
 3934 root       20   0 1070M  238M 15496 S  3.4  3.0  0:00.45 nessusd -q
 3935 root       20   0 1070M  238M 15496 S  3.4  3.0  0:00.42 nessusd -q
 3937 root       20   0 1070M  238M 15496 S  3.4  3.0  0:00.44 nessusd -q
 3933 root       20   0 1070M  238M 15496 S  2.7  3.0  0:01.12 nessusd -q
 3699 root       20   0 1070M  238M 15496 S  0.7  3.0  0:04.08 nessusd -q
 3713 root       20   0 1070M  238M 15496 S  0.7  3.0  0:44.77 nessusd -q
 3932 root       20   0 1070M  238M 15496 S  0.7  3.0  0:00.19 nessusd -q
 3944 root       20   0 1070M  238M 15496 D  0.7  3.0  0:00.03 nessusd -q
 3945 root       20   0 1070M  238M 15496 S  0.7  3.0  0:00.03 nessusd -q
```

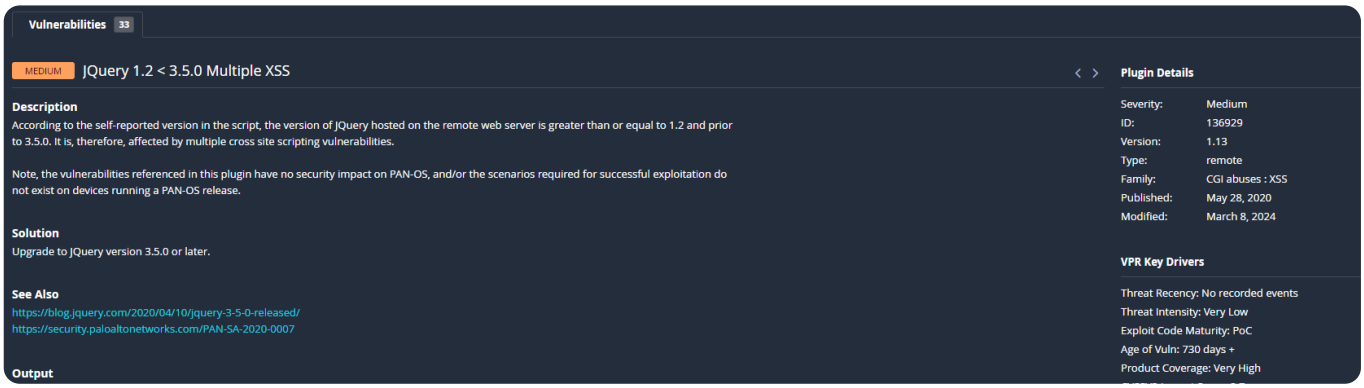
When the scan is complete a checkmark will appear under the 'Last Scanned' column of the scan object. Click on the scan object to review the results. Under the 'Hosts' tab the vulnerabilities per host are displayed. To the right of the screen you can see the scan details. If you click on a host a list of the list vulnerabilities will be presented specific to that host. The 'vulnerabilities' tab is a list of all vulnerabilities found during the scan.

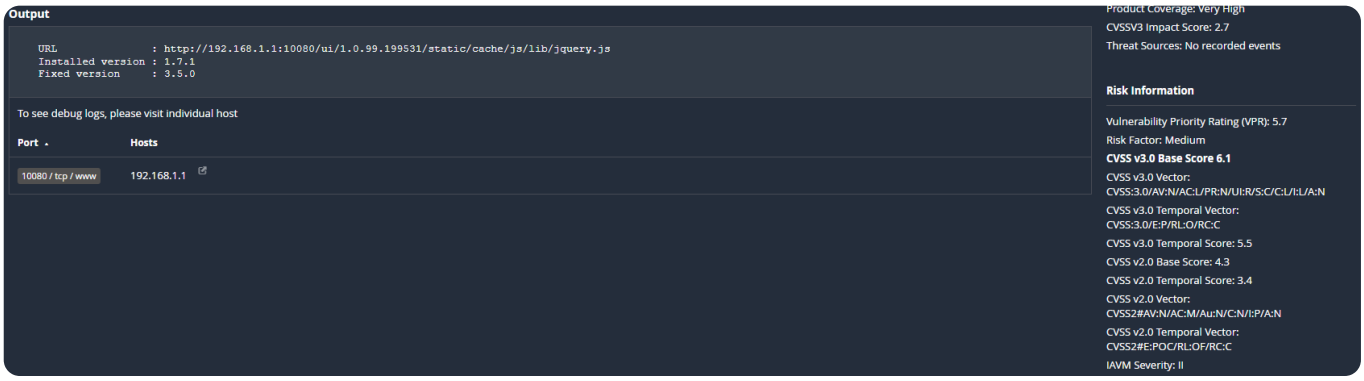
Vulnerabilities are listed showing severity, common vulnerability scoring system (CVSS) score, vulnerability priority rating (VPR), the plugin family associated with the vulnerability, and the count. The vulnerability object has edit and snooze buttons. To the right is a the host and small breakdown of its addressing and OS. You can click the column headers to sort the list. CVSS provides the severity rating of the vulnerability and VPR that represent the risk/urgency of a vulnerability considering the current virtual landscape. These two

rating can help prioritize fixing vulnerable issues.



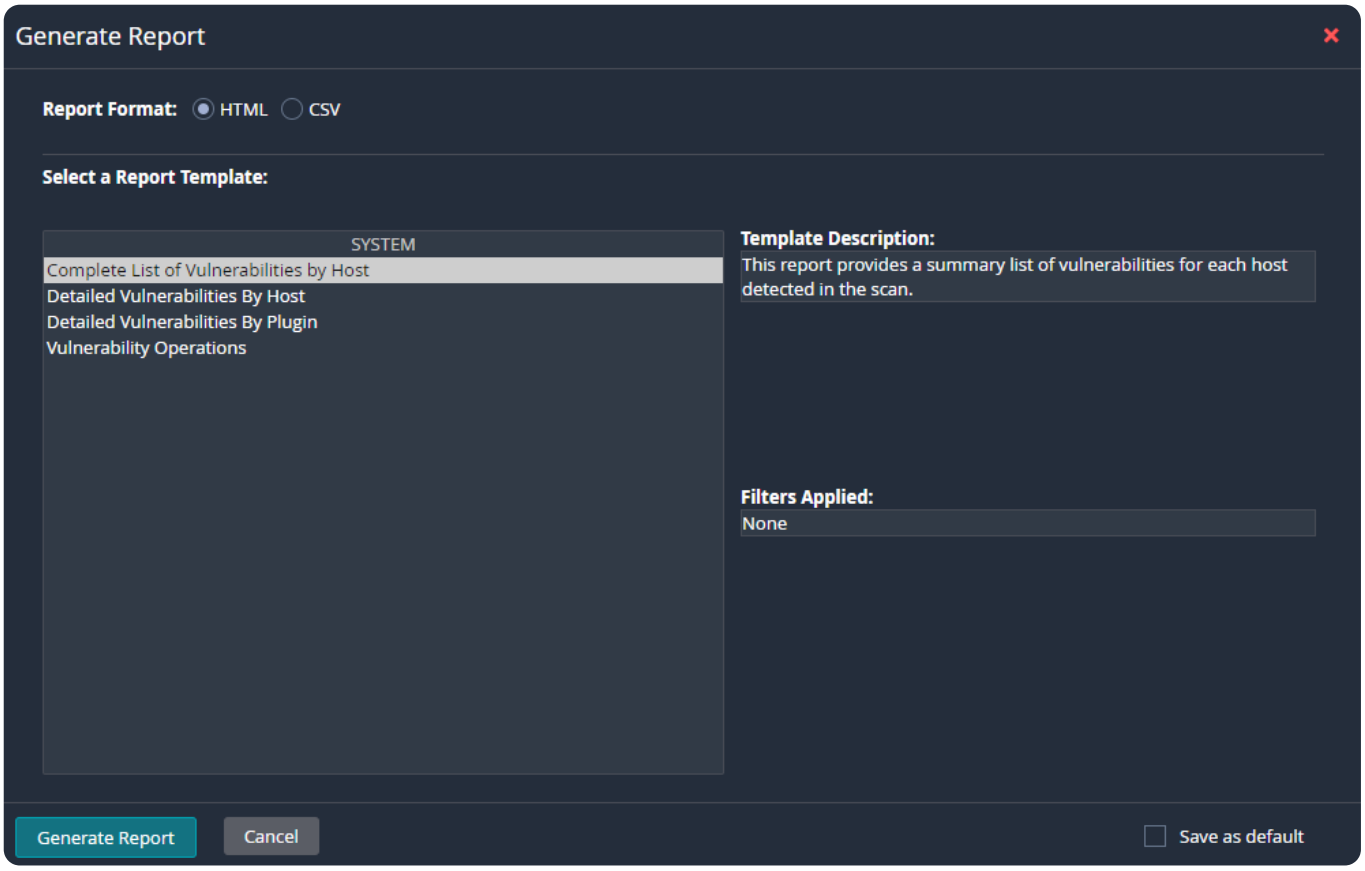
If you drill down further by clicking on a vulnerability object the first thing you'll notice is the description and solution along with some reference links. Below that is the output from the plugin that found the vulnerability and some more specifics about the vulnerable vector. To the right details for the plugin that found the vulnerability, the key factors in VPR calculation, the risk information related to CVSS calculation, vulnerability information related to exploitation, and a collection of reference links to related issues. Exploring some the reference links may also be smart move at this point to gain a better understanding of the vulnerability. This may also include tracking down exploits and proof-of-concepts to become fully aware of how the vulnerability is abused.





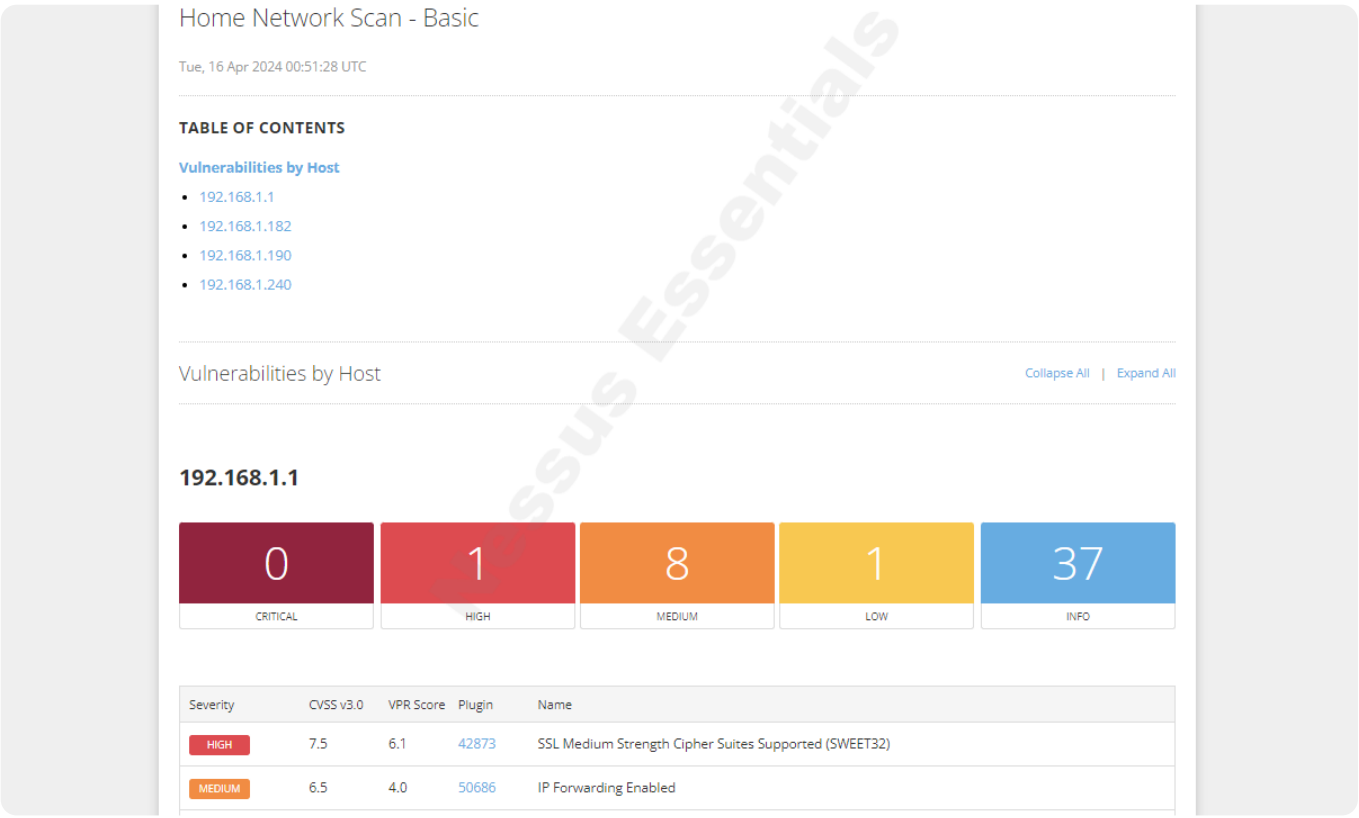
Navigate back to the hosts tab and generate a report of the scan scan. To do this click the report button at the top right of the page. Select the 'HTML' radio button for the format. The CVS format is for passing data between programs. Select the report template you want. I'll use the default selection for this exercise. When you are done click 'Generate

report'. Save the report file to somewhere that makes sense.



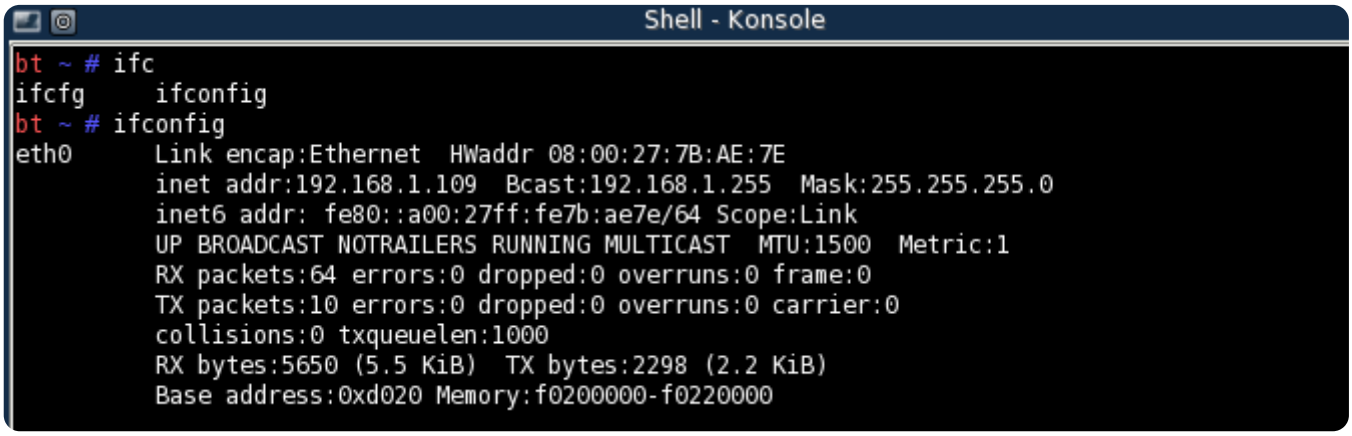
The report can opened in the browser for review. This report displays a basic breakdown of vulnerabilities by host. Clicking on the show button under a host displays the vulnerability object list. For more information on a vulnerability, to include all the details previously found in the Nessus interface, click on the plugin link. This will take you to the associated Nessus plugin page where you can find all the information the vulnerability. This is not the only report template though so perform some scans and generate reports to gain better insight into report generation for specific purposes. For example, you may

want to generate different reports for different departments.



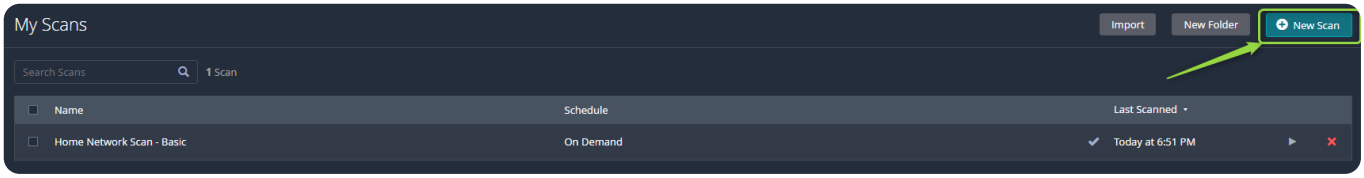
Task 2 - Conduct your first Vulnerability Scan – DVL

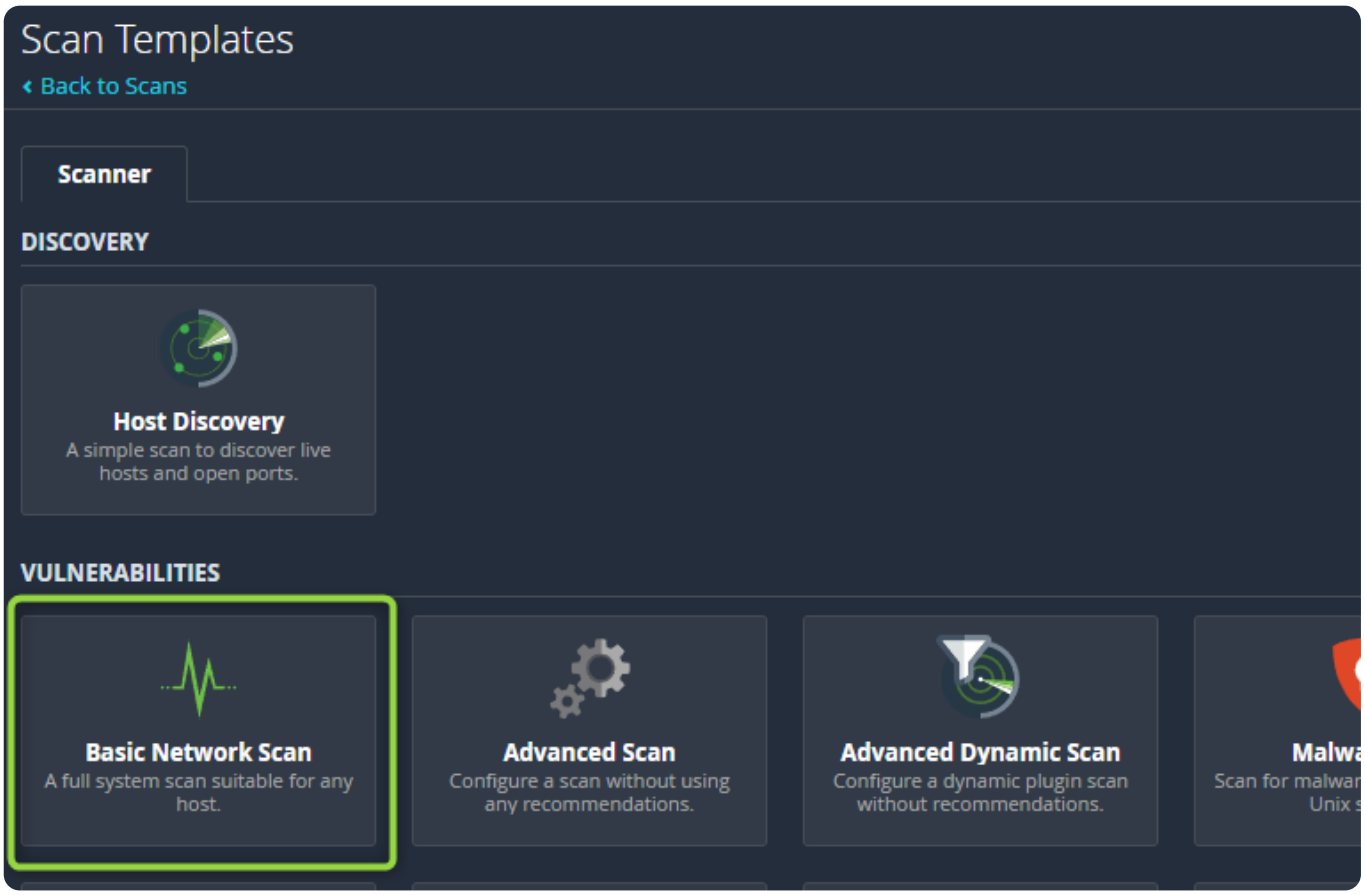
This scan will target a Damn Vulnerable Linux version 1.5 (DVL). Make sure you have a VM deployed of DVL and start it up. I purposely went logged into my DVL instance and started a bunch of services to make the scan more interesting. Use 'ifconfig' to find the local IP address of the DVL VM and make a note of it. We are going to use this IP address as the target for the scan.

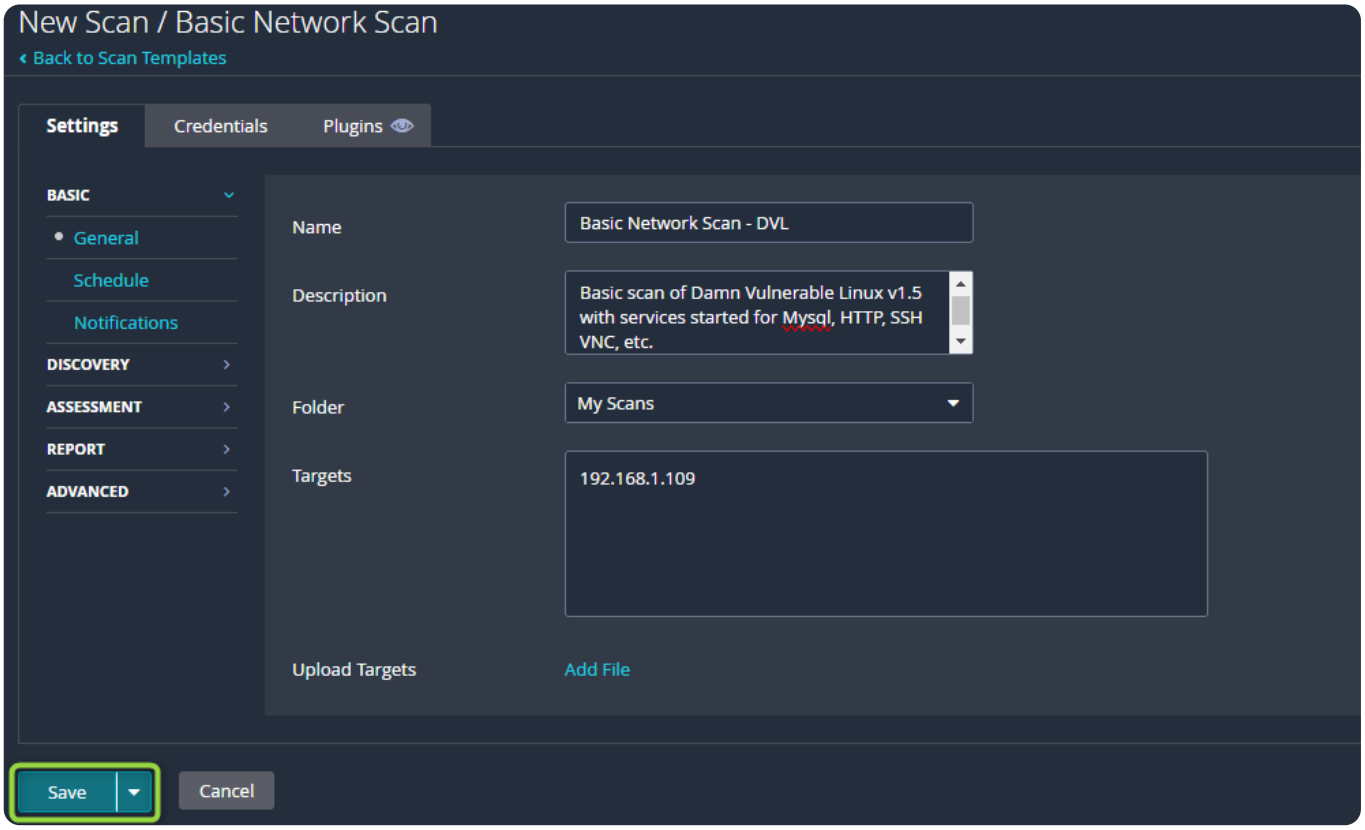


Open up the Nessus interface in the browser by navigating to the server's IP address on port 8834. Click on the 'New Scan' button in the 'My Scans' folder. Select the 'Basic

Network Scan' option and fill out the required fields. The target is the DVL IP address that you recorded earlier. Once you are done, click the 'Save' button to create the scan.

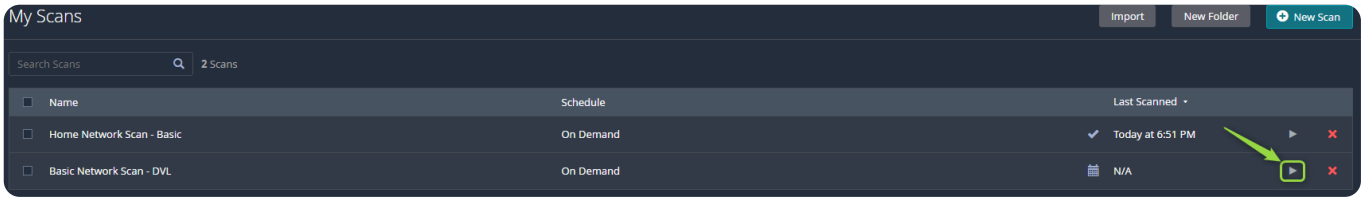




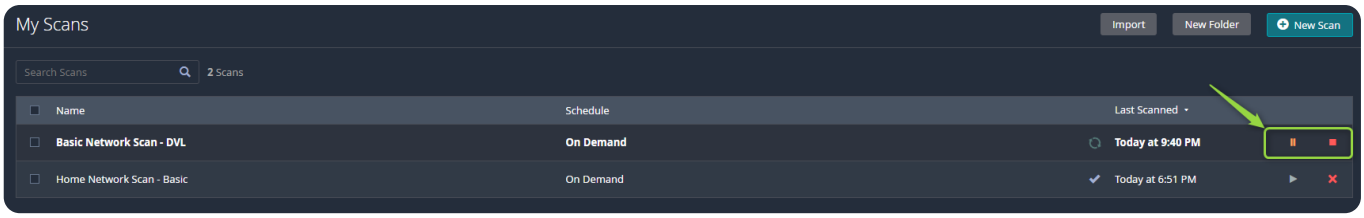


The new scan should now appear in the 'My Scans' folder. Click the play button on in the scan object to begin the scan. This is going to take some time so be patient and wait for

the checkmark to appear next to the 'Last Scanned' DTG of the scan object.

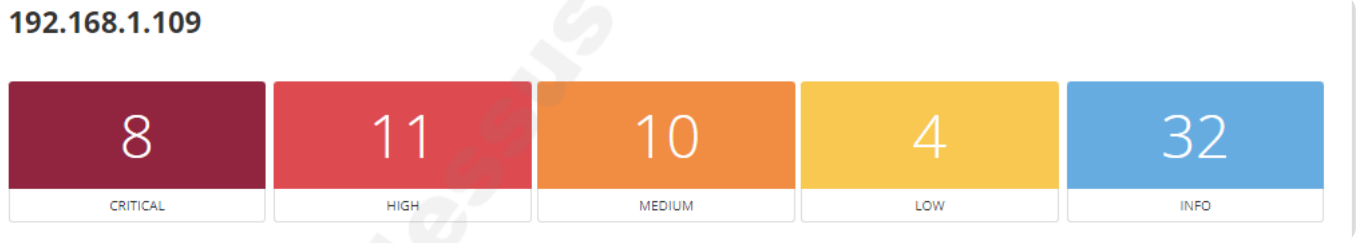


Remember that you can pause or stop the scan at anytime. Once paused there is an option to resume the scan as well.



Scan results:

Below are some snapshots of the scan results. We can observe that there are quite a few vulnerabilities present on the DVL VM. Upon deeper inspection it becomes obvious that many of the services running on the system are out of date. The recommended remediation for most of the these higher severity issues is to update the services to the latest version. In the scan results page of Nessus you'll see that a large amount of vulnerabilities are grouped by service and have a severity label of 'MIXED'. If you drill down into these entries you'll find many critical or high severity issues relating to the same core problem; the service being out of date or not supported. I believe it is fair to say that the DVL instance would be easily exploitable. I spent quite a while digging into each of these issues and found countless available exploits or proof-of-concept write-ups regarding each; far too many to list here.



Basic Network Scan - DVL / 192.168.1.109

‹ Back to Hosts

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 28

Filter | Search Vulnerabilities | 28 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
LOW	2.6 *		X Server Detection	Service detection	2
MIXED	...	...	PHP (Multiple Issues)	CGI abuses	15
MIXED	...	...	Apache Httpd (Multiple Issues)	Web Servers	8
MIXED	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	4
MIXED	...	...	SSH (Multiple Issues)	General	3
MIXED	...	...	HTTP (Multiple Issues)	Web Servers	6
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
INFO	...	...	VNC (Multiple Issues)	Service detection	3
INFO	...	...	SSH (Multiple Issues)	Service detection	2

Host Details

IP: 192.168.1.109
MAC: 08:00:27:7B:AE:7E
OS: Linux Kernel 2.6
Start: Today at 3:37 AM
End: Today at 3:51 AM
Elapsed: 13 minutes
KB: Download

Vulnerabilities

Critical
High
Medium
Low
Info

Basic Network Scan - DVL / 192.168.1.109 / Apache Httpd (Multiple Issues)

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Vulnerabilities 28

Search Vulnerabilities | 8 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.8	6.7	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.8	6.7	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.8	6.7	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.8	5.9	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.0	8.1	Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1
CRITICAL	9.0	6.5	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	1
HIGH	7.5	4.4	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Web Servers	1
HIGH	7.5	4.4	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Web Servers	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: April 15 at 9:37 PM
End: April 15 at 9:51 PM
Elapsed: 13 minutes

Vulnerabilities

Critical
High
Medium
Low
Info

Severity	CVSS v3.0	VPR Score	Plugin	Name
CRITICAL	9.8	6.7	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	5.9	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	6.7	172186	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL	9.8	6.7	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.0	6.5	170113	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities
CRITICAL	9.0	8.1	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	-	171347	Apache HTTP Server SEoL (<= 1.3.x)
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	7.5	4.4	183391	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities
HIGH	7.5	4.4	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.3	6.3	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	7.5*	7.3	24906	PHP < 4.4.5 Multiple Vulnerabilities
HIGH	7.5*	6.7	29833	PHP < 4.4.8 Multiple Vulnerabilities
HIGH	7.5*	6.7	33849	PHP < 4.4.9 Multiple Vulnerabilities
HIGH	7.5*	6.7	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5*	6.3	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5*	8.9	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5*	6.3	57537	PHP < 5.3.9 Multiple Vulnerabilities