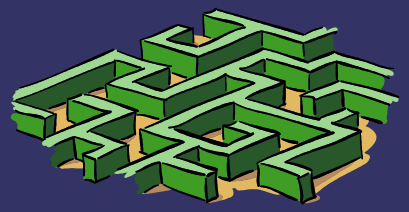
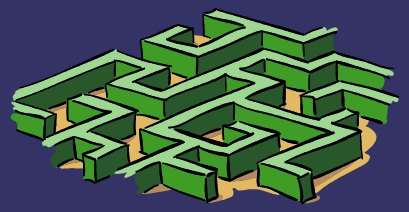
PENETRATION TEST ON METASPOLITABLE 2

W12 D4 PROJECT



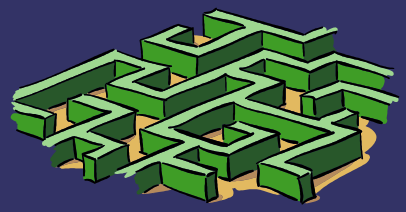
OVERVIEW

- Execute a full scan on virtual machine Metasploitable 2
- Focus on critical vulnerabilities
- Let's see how to fix them; remediation actions
- New full scan on the Machine

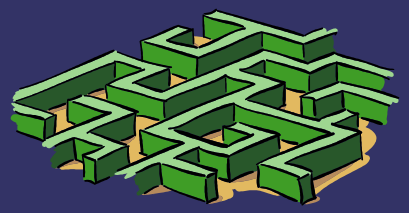


PENETRATION TEST: INTRODUCTION

In this first scan we are going to check the whole situation about the machine connected to the IP 192.168.1.101.
To do this, the Ethical Hackers can have access to a an amount of useful tools which are created to specific ethical purposes; in this case the tool used is Tenable's Nessus Essentials, the trial version of the full app Nessus, wich can allow us to use a very big range of scanners to check the vulnerabilities related to a specific IP.



PENETRATION TEST: FIRST SCAN



192.168.1.101

25	10	27	10	93
CRITICAL	HIGH	MEDIUM	LOW	INFO

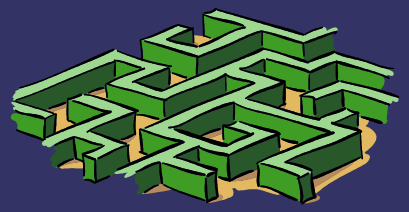
Vulnerabilities Total: 165

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	6.7	184080	PyTorch TorchServe SSRF (CVE-2023-43654)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	9.7	159375	Spring Cloud Function SPEL Expression Injection (direct check)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	9.0	8.1	156164	Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution
CRITICAL	10.0	10.0	156016	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
CRITICAL	10.0	10.0	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
CRITICAL	10.0	10.0	156257	Apache Log4Shell RCE detection via callback correlation (Direct Check DNS)
CRITICAL	10.0	10.0	156115	Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)
CRITICAL	10.0	10.0	156014	Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)
CRITICAL	10.0	10.0	156669	Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC)
CRITICAL	10.0	10.0	156197	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)

CRITICAL	10.0	10.0	156559	Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND)
CRITICAL	10.0	10.0	156232	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)
CRITICAL	10.0	10.0	156132	Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP)
CRITICAL	10.0	10.0	156166	Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)
CRITICAL	10.0	10.0	156162	Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

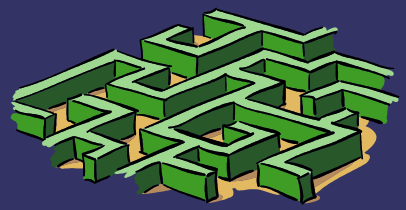
PENETRATION TEST: CRITICAL VULNERABILITIES

Our First Scan on Metsasploitable displayed us a lot of different leveled vulnerabilities, From the most dangerous Critical to the armless Info vulnerabilities, so we are going to focus on the most harmful warnings. As we can see we found 25 Critical vulnerabilities that we have to check and promptly fix.



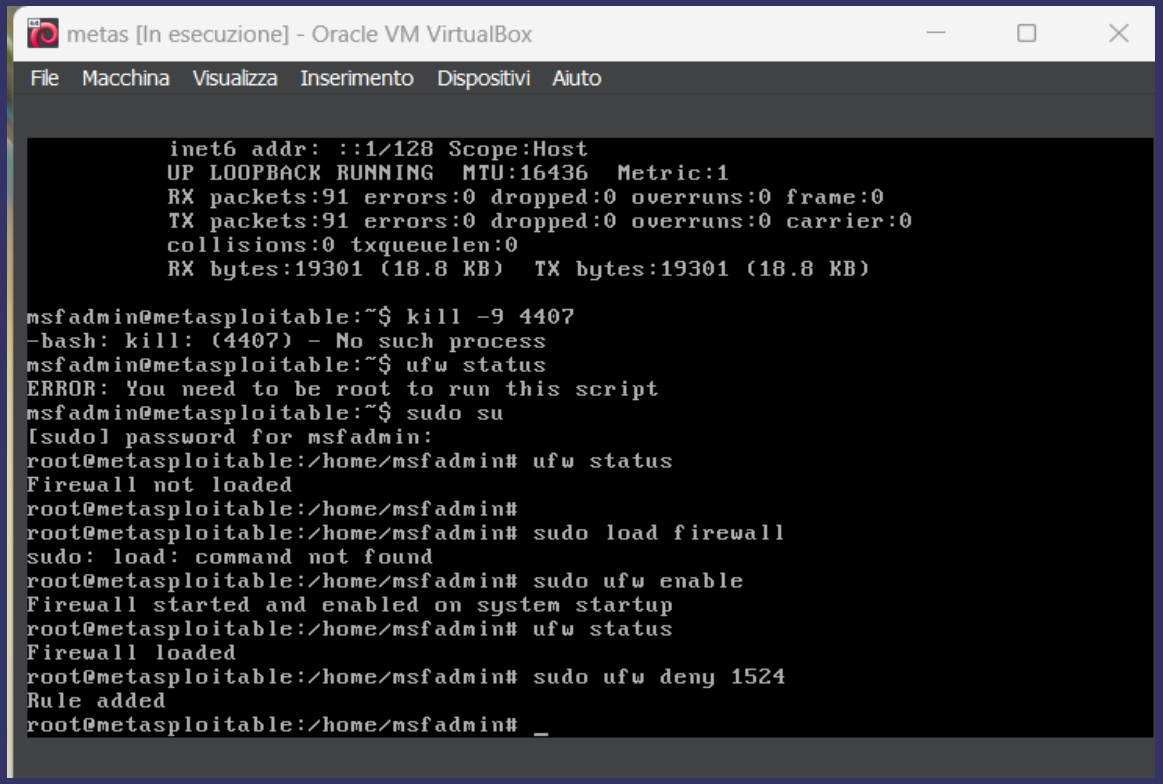
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

This shell is listening on port 1524 without any kind or appro-priated permission or authenticayion required, so an intruder could use it as a shell to put commands from remote



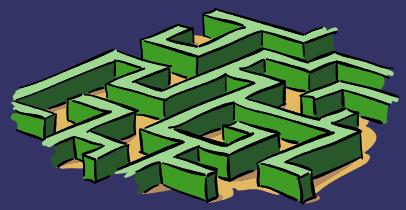
REMEDIATION ACTION FOR BIND SHELL BACKDOOR DETENCTION

To prevent intruders to get in the machine we should check wich is/are the ports open, than got to be sure if we have a firewall or specific rule to block and secure them spots.
Let's enable the firewall rule to deny the access on port 1524.



CRITICAL	10.0*	-	61708	VNC Server 'password' Password

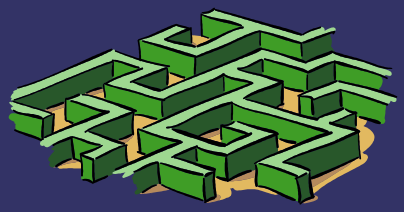
This vulnerabilty show us that the host is secured with a very weak password, very easy to discover and exploitable, so we must check and change this specific server passoword



REMEDIATION ACTION FOR VNC PASSWORD

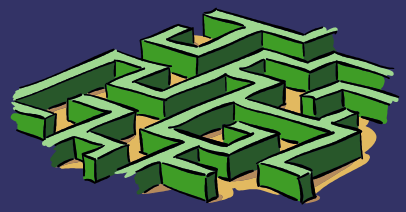
```
root@metasploitable:/home/msfadmin# sudo su
root@metasploitable:/home/msfadmin# sudo password for <user>
bash: syntax error near unexpected token `newline'
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# _
```

We changed the password for VNC server from the root mode on our Metasploiable Machine



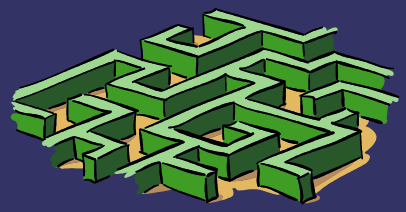
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

We can also notice that trough this vulnerability there an easy acces to port 5900, so it's wise to set a firewall rule even for this one.



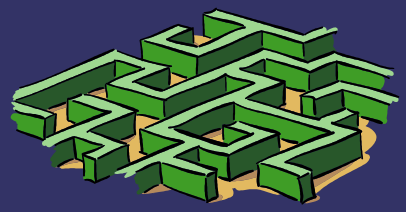
```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
root@metasploitable:/home/msfadmin# sudo ufw deny 5900_
```

So now we have deny the access for port 5900 trough function UFW



OUR MACHINE METASPLOITABLE 2

Our machine, in this specific case a virtual machine, Meta-sploitable2 is programmed to be exploited to let new etichal hackers to practice with tools and tests so whenever we are going to scan it trough any scannig tool we are going to find several flaws and vulnerabilities that needs fixings, even tough Metasploitable 2 don't let us do every task a normal machine would, like most of upgrades of internal apps and tools for example.



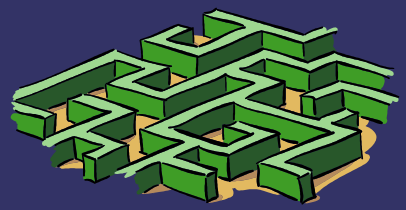
CRITICAL	10.0	10.0	156016	Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)
CRITICAL	10.0	10.0	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
CRITICAL	10.0	10.0	156257	Apache Log4Shell RCE detection via callback correlation (Direct Check DNS)

We can see a lot of flaws with the apache Log4shell; this means that the the webserver is affected by a remotecode execution vulnerability via a flaw in the apachelog4j library. The vulnerability is due to the processing of an unsanitized input sent to a logging function.An attacker could easily get trough with a java process via web request!

To solve the Apache Log4 Shell vulnerabilities we gonset an update so the function will be sanitazed and the flaws will be erased

```
Last login: Fri Mar  8 11:22:19 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo apt update
[sudo] password for msfadmin:
sudo: apt: command not found
msfadmin@metasploitable:~$ dpkg -l grep liblog4j
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Installed/Config-f/Unpacked/Failed-cfg/Half-inst/t-aWait/T-pend
|/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=bad)
||/ Name           Version        Description
+++-==============-==============-============================================
ii  grep           2.5.3~dfsg-3   GNU grep, egrep and fgrep
No packages found matching liblog4j.
msfadmin@metasploitable:~$ sudo aptsudo apt-get update_
```

```
  postgresql-common procps python-apt python-central rsync samba samba-common
  sudo sysv-rc sysvutils tasksel tasksel-data tzdata udev ufw
  update-manager-core util-linux util-linux-locales vim-common vim-tiny wget
  whiptail xkb-data
92 upgraded, 0 newly installed, 0 to remove and 13 not upgraded.
Need to get 69.7MB of archives.
After this operation, 4637kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  libpam-modules base-files bash dash dpkg gzip login mount sysvutils lsb-base
  tzdata util-linux bsdutils mysql-common mysql-server libmysqlclient15off
  mysql-client-5.0 passwd mysql-server-5.0 apt libpam-runtime sysv-rc
  apt-utils xkb-data klibc-utils libklibc module-init-tools libvolume-id0
  procps udev initramfs-tools console-setup cron dhcp3-client dhcp3-common
  eject iproute libgnutls13 libnewt0.52 libssl0.9.8 libsasl2-2
  libsasl2-modules lsb-release pciutils tasksel-data tasksel
  util-linux-locales vim-tiny vim-common wget whiptail initscripts apparmor
  apparmor-utils file libmagic1 friendly-recovery libkrb53 liblwres30
  libntfs-3g23 libparted1.7-1 logrotate lshw parted python-central python-apt
  rsync ufw update-manager-core apache2 fuse-utils libfuse2
  installation-report libapr1 libexpat1 libpq5 libaprutil1 libcurl3-gnutls
  libdbus-1-3 libhtml-parser-perl libpcre3 libxml2 ntpdate openssl postfix
  postgresql-client-common postgresql-client-8.3 postgresql-common
  postgresql-8.3 samba samba-common sudo
Install these packages without verification [y/N]?
```

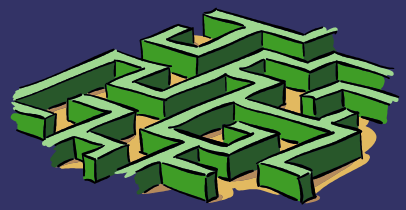


In the end, to be sure to block ost f vulnerabilities on our machine we can enable an appropriate firewall; to do this on metasploitable we a have multiple choises like setting a PFSense rule, an IPTable rule or an UFW Firewall.

metas [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ kill -9 4407
-bash: kill: (4407) - No such process
msfadmin@metasploitable:~$ ufw status
ERROR: You need to be root to run this script
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# ufw status
Firewall not loaded
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# sudo load firewall
sudo: load: command not found
root@metasploitable:/home/msfadmin# sudo ufw enable
Firewall started and enabled on system startup
root@metasploitable:/home/msfadmin#
```



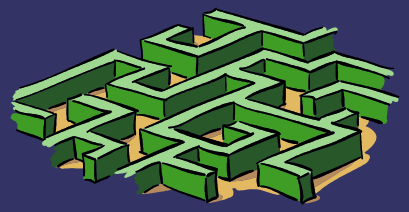
PENETRATION TEST: NEW SCAN

192.168.1.101

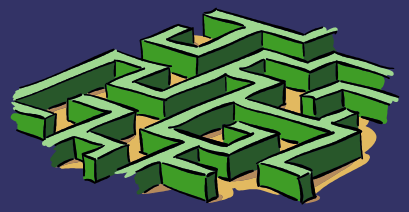
0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10287	Traceroute Information



After all the remediation actions we applied to the machine connected to the 192.168.1.101 IP, executing a new scan with same parameters, the scanners displays us no Critical or High vulnerabilities, so can assume that for now the host is properly protected and secured, even though it is better to always check for new treats.



THANK YOU FOR THE KIND ATTENTION