Penetration testing Report on Metaspoiltable 2.

Submitted by :

Name: tenzin yarphel

Email: tenzinyarphel51@gmail.com

Index

1. Execute Summery

1.1 Scope and Duration of work

the penetration test was performed on Metaspolitable2 between 15th June,2022 and 1st July, 2022. Domains and applications were tested for 2 work hours. Reporting took 8 work hours.

The purpose of the test was to Test determine sec vulnerabilities and exploit them.

The scope of the test was limited to IP address listed below.

129.168.88.128

1.2 Findings

Critical: 10%

High: 8%

Medium: 8%

Low: 21%

Info: 59%

2. Methodology

The methodology consisted of 7 of steps beginning with the determination of test scope, and ending with reporting. These tests were performed by security experts using potential attackers' modes of operation while controlling execution to prevent harm to the systems being tested. The approach included but is not limited to manual and automated vulnerability scans, verification of findings (Automated and otherwise). This verification step and manual scanning process eliminated false positives and erroneous outputs, resulting in more efficient tests.

- Determining scope of the test
- Information Gathering / Reconnaissance
- Scanning
- Vulnerability Analysis
- Exploitation
- Reporting

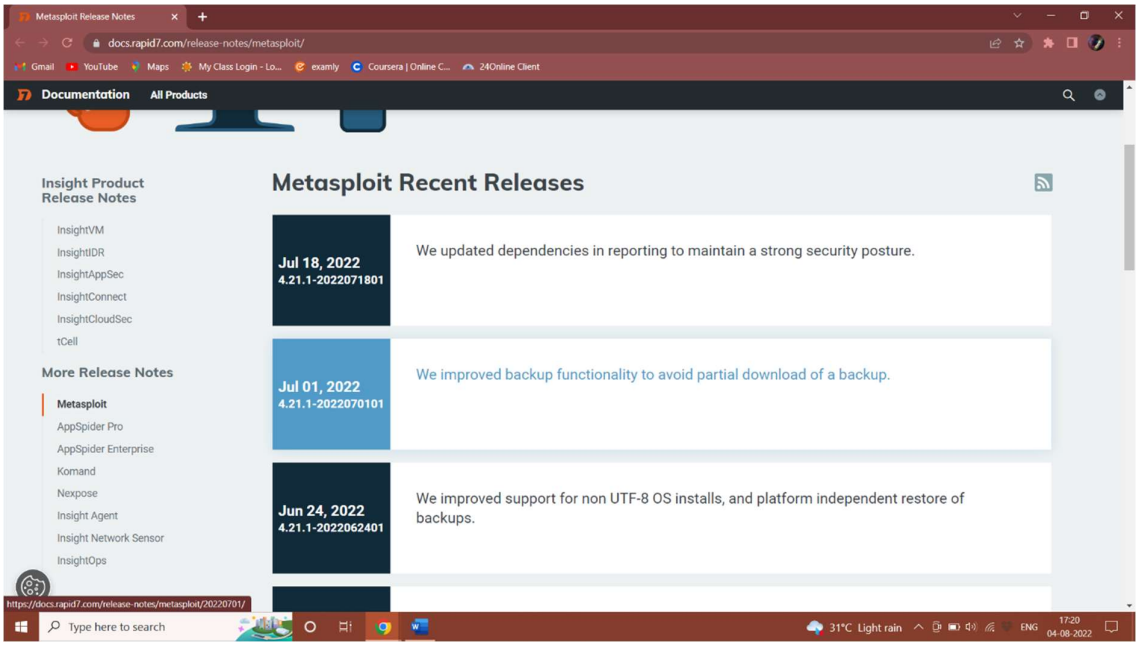
2.1. Determining the Scope

Choose one, delete other

Our first step was determining the scope of the test. Since this was a Blackbox test scope, as given by our teacher. It is an educational test and does not have any ill intent to any organization.

2.2. reconnaissance

Before directly accessing the target, we researched everything we could locate from third party resources. This included google hacking, looking for publisher notes etc. This information was used in later tests

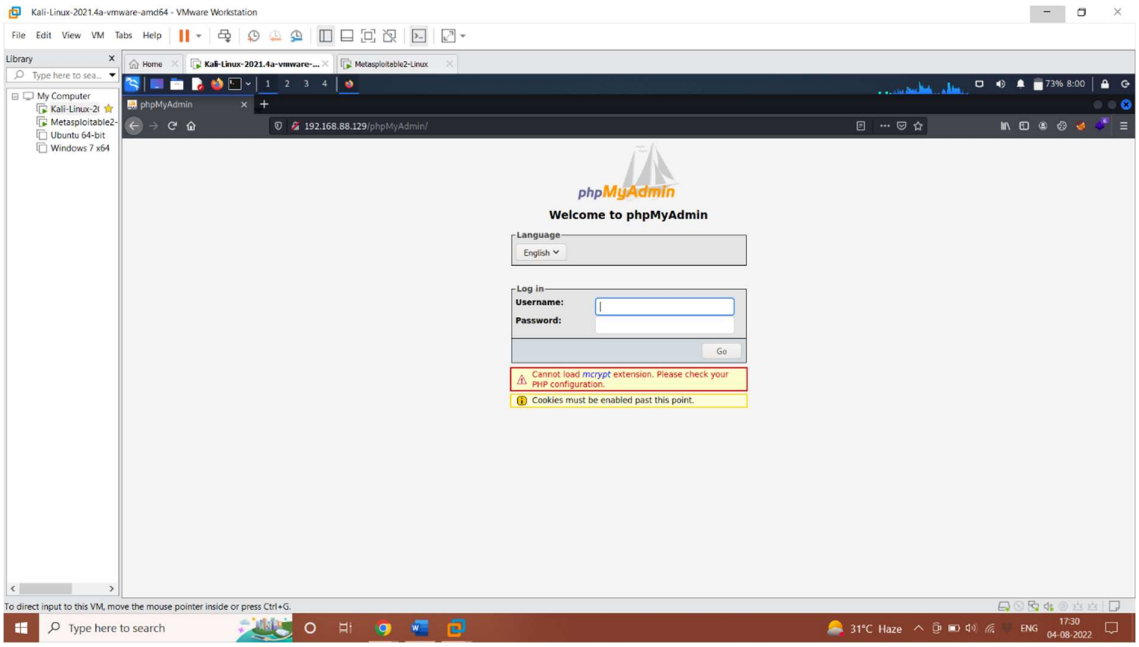


2.2.1. IP Addresses and Domains

Here is a list of the IP addresses and domains gathered using search engines:

192.168.88.129	Metaspoiltable2

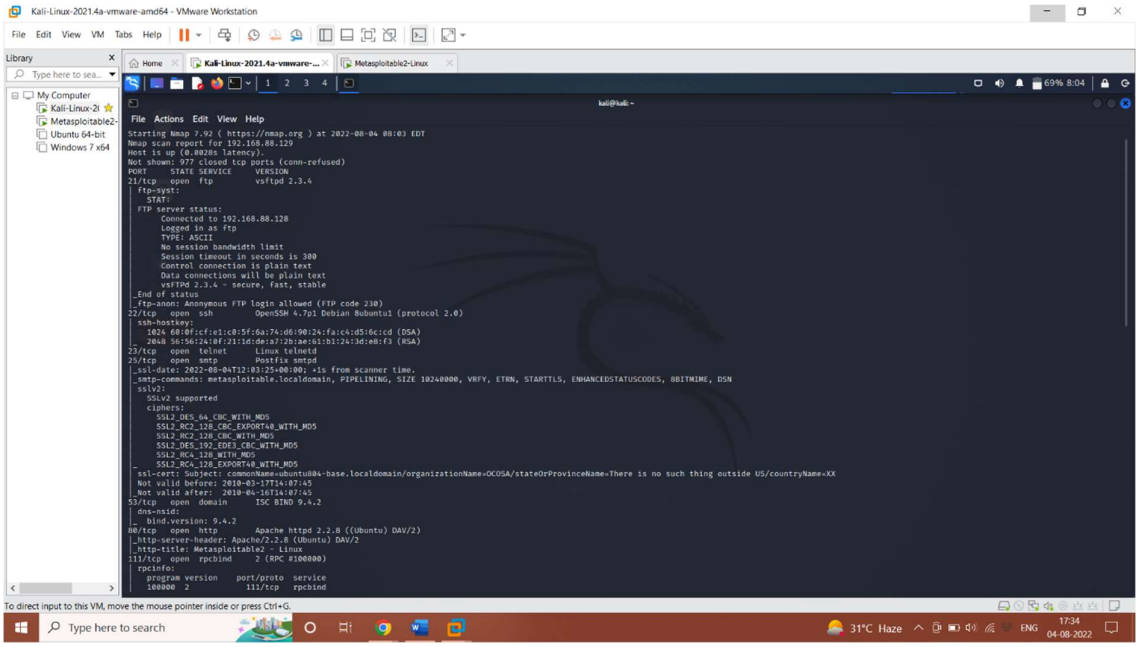
2.2.2. Login Pages Found During Server Analysis Login pages are the front line of an application's defence against unauthorized access. They also present a surface area of interest to attackers who will try to defeat the defences in order to access the functionality and data within the system. This section identifies the URLs and screens of the login pages discovered during analysis.

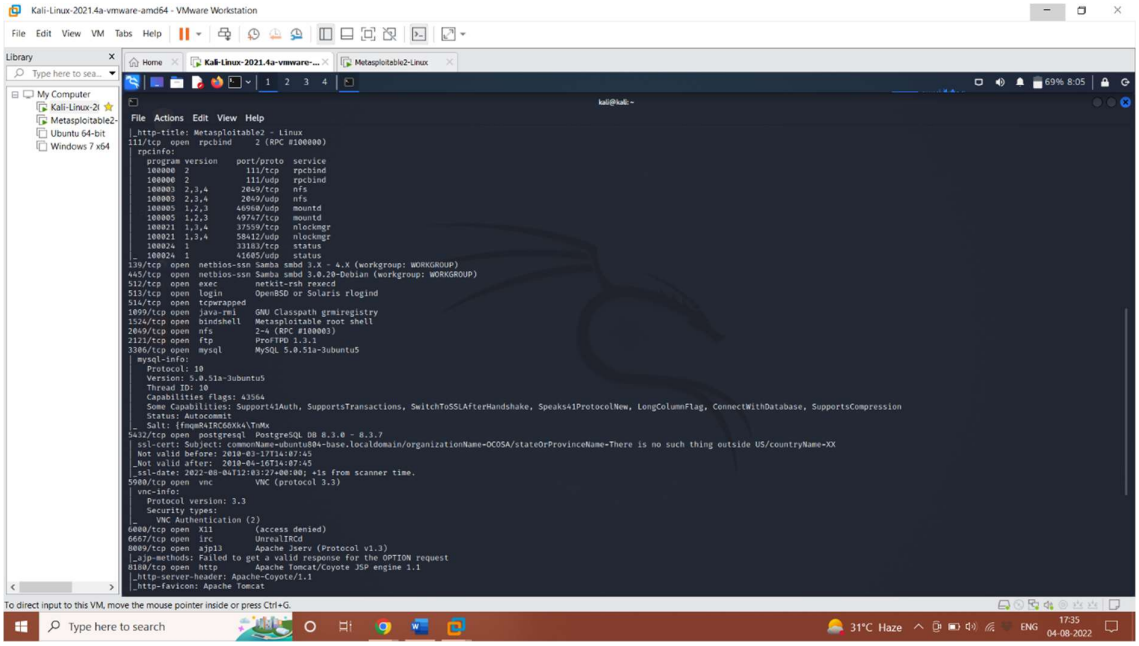


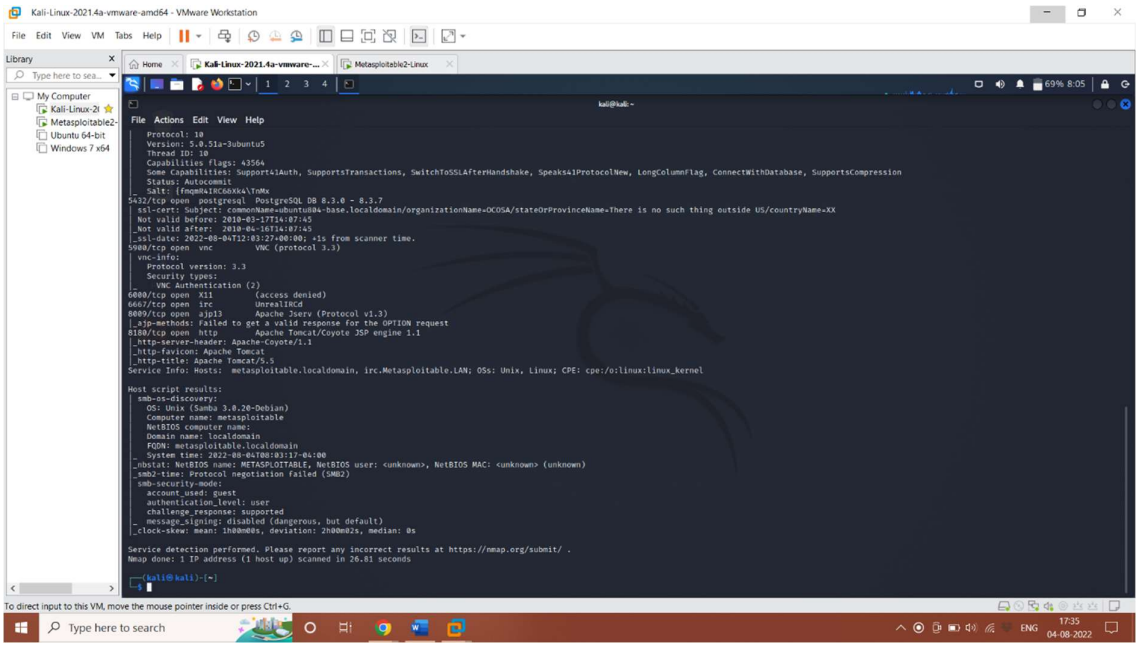
2.3. Scanning

Various scans were performed to determine and verify vulnerabilities in the target systems.

2.3.1 Port Scan







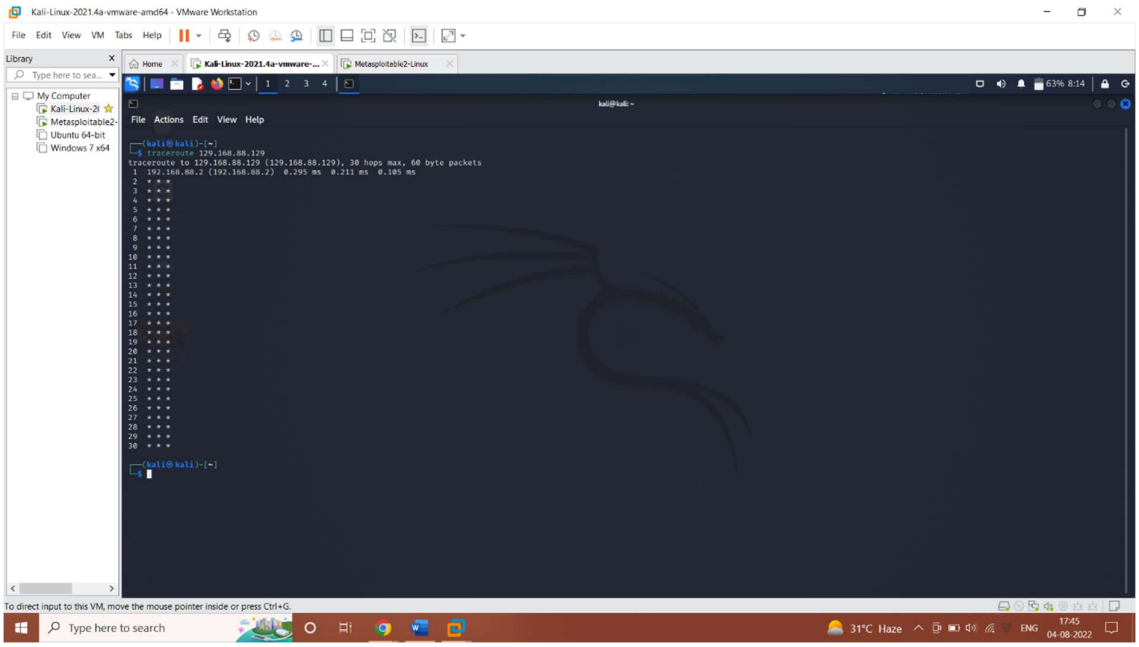
Open ports :

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

2.3.2 Route Scans

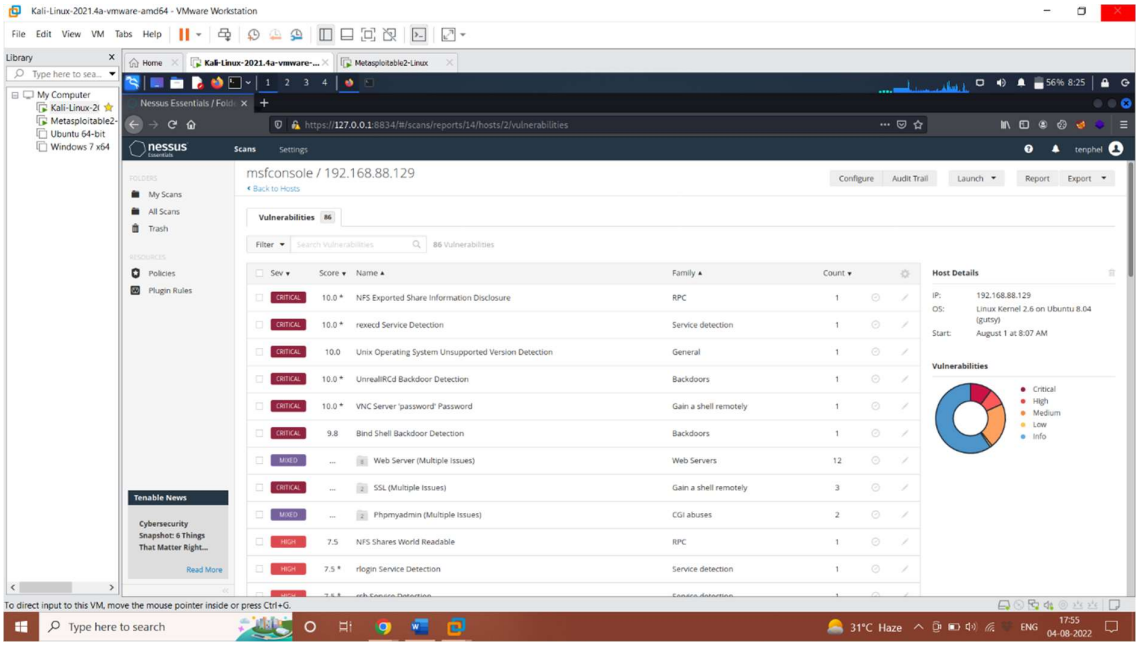
With the help of traceroute we are able to map path between machines.

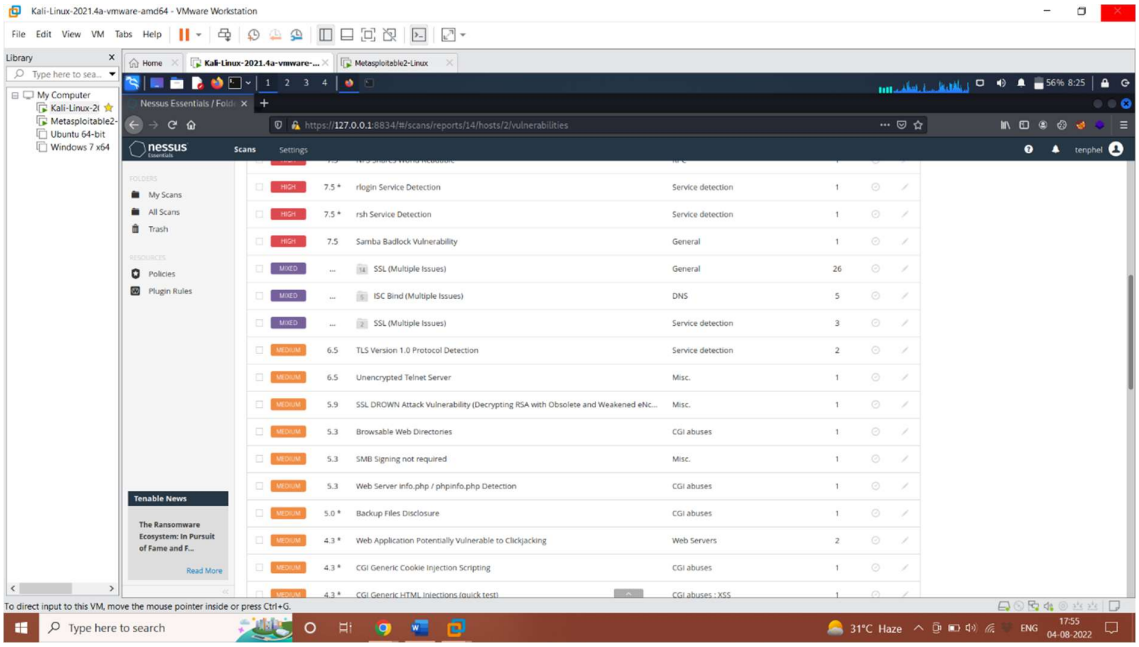


2.4. Vulnerability Analysis

2.4.1. Scanning Target Systems

Using vulnerability scanners like Nessus target systems were crosschecked with up-to date vulnerability databases.





Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to sea...

My Computer

Kali-Linux-2021

Metasploitable2-

Ubuntu 64-bit

Windows 7 x64

Home | Kali-Linux-2021.4a-vmware-... | Metasploitable2-Linux

Nessus Essentials / Folde...

https://127.0.0.1:8834/#/scans/reports/14/hosts/2/vulnerabilities

nessus Essentials | Scans | Settings | tenphel

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules

Tenable News: The Ransomware Ecosystem: In Pursuit of Fame and F... Read More

MEDIUM	4.3 *	CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1
MEDIUM	4.3 *	CGI Generic XSS (quick test)	CGI abuses : XSS	1
MIXED	...	HTTP (Multiple Issues)	Web Servers	7
MIXED	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	DNS (Multiple Issues)	DNS	5
MIXED	...	PHP (Multiple Issues)	Web Servers	3
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	2
MIXED	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	TLS (Multiple Issues)	SMTP problems	2
LOW	2.6 *	X Server Detection	Service detection	1
INFO	...	SMB (Multiple Issues)	Windows	7
INFO	...	HTTP (Multiple Issues)	CGI abuses	4
INFO	...	TLS (Multiple Issues)	General	4
INFO	...	FTP (Multiple Issues)	Service detection	3
INFO	...	VNC (Multiple Issues)	Service detection	3
INFO	...	Apache HTTP Server (Multiple Issues)	Web Servers	2

Apache HTTP Server (Multiple Issues)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search | 31°C Haze | ENG | 17:55 04-08-2022

Kali-Linux-2021.4a-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library

Type here to sea...

My Computer

Kali-Linux-2021

Metasploitable2-

Ubuntu 64-bit

Windows 7 x64

Home | Kali-Linux-2021.4a-vmware-... | Metasploitable2-Linux

Nessus Essentials / Folde...

https://127.0.0.1:8834/#/scans/reports/14/hosts/2/vulnerabilities

nessus Essentials | Scans | Settings | tenphel

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules

Tenable News: The Ransomware Ecosystem: In Pursuit of Fame and F... Read More

INFO	...	HTTP (Multiple Issues)	CGI abuses	4
INFO	...	TLS (Multiple Issues)	General	4
INFO	...	FTP (Multiple Issues)	Service detection	3
INFO	...	VNC (Multiple Issues)	Service detection	3
INFO	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	...	RPC (Multiple Issues)	RPC	2
INFO	...	SSH (Multiple Issues)	Service detection	2
INFO		Nessus SYN scanner	Port scanners	25
INFO		RPC Services Enumeration	Service detection	10
INFO		Service Detection	Service detection	8
INFO		CGI Generic Injectable Parameter	CGI abuses	2
INFO		CGI Generic Tests Load Estimation (all tests)	CGI abuses	2
INFO		External URLs	Web Servers	2
INFO		OpenSSL Detection	Service detection	2

Results per page 50

Showing: 1 to 50 of 86

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Type here to search | 31°C Haze | ENG | 17:55 04-08-2022

2.5 exploitation

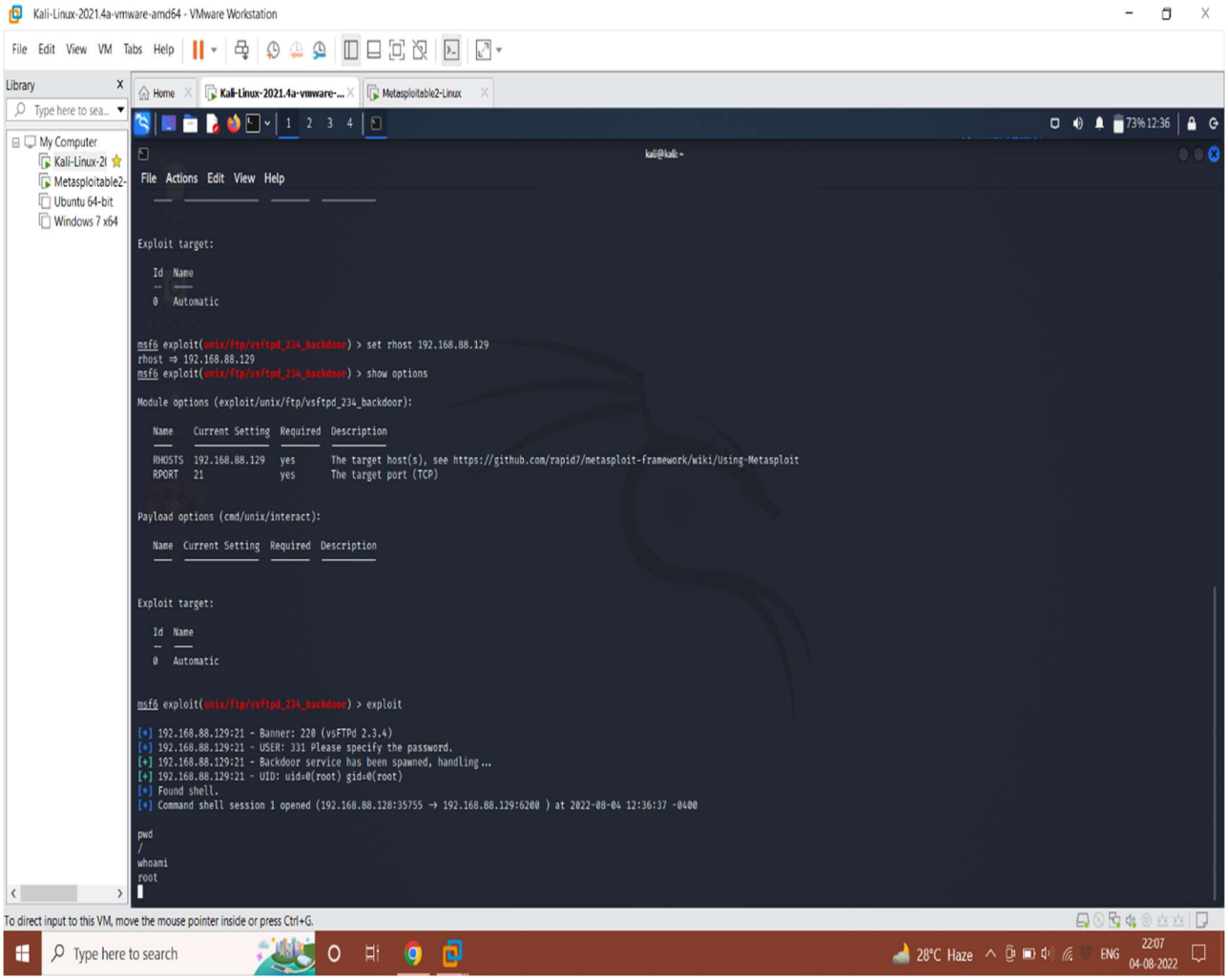
2.5.1. vsftpd 2.3.4 - Backdoor Command Execution

CVE: 2011-2523

CVSS : 10.0

Description: a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011

With this vulnerability a attacker can get root access and it was able to exploit from Metasploit.



2.5.2 unix Operating System Unsupported Version Detection

Risk Factor: Critical

Description : with the help of nmap I was able to found lunix version of this system is no longer supported.

CVSS v3.0 Base Score 10.0

Vulnerability Information

Unsupported by vendor: true

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap  -O  192.168.88.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-05 09:13 EDT
Nmap scan report for 192.168.88.129
Host is up (0.00065s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:A8:65:0A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds

┌──(kali㉿kali)-[~]
└─$
```

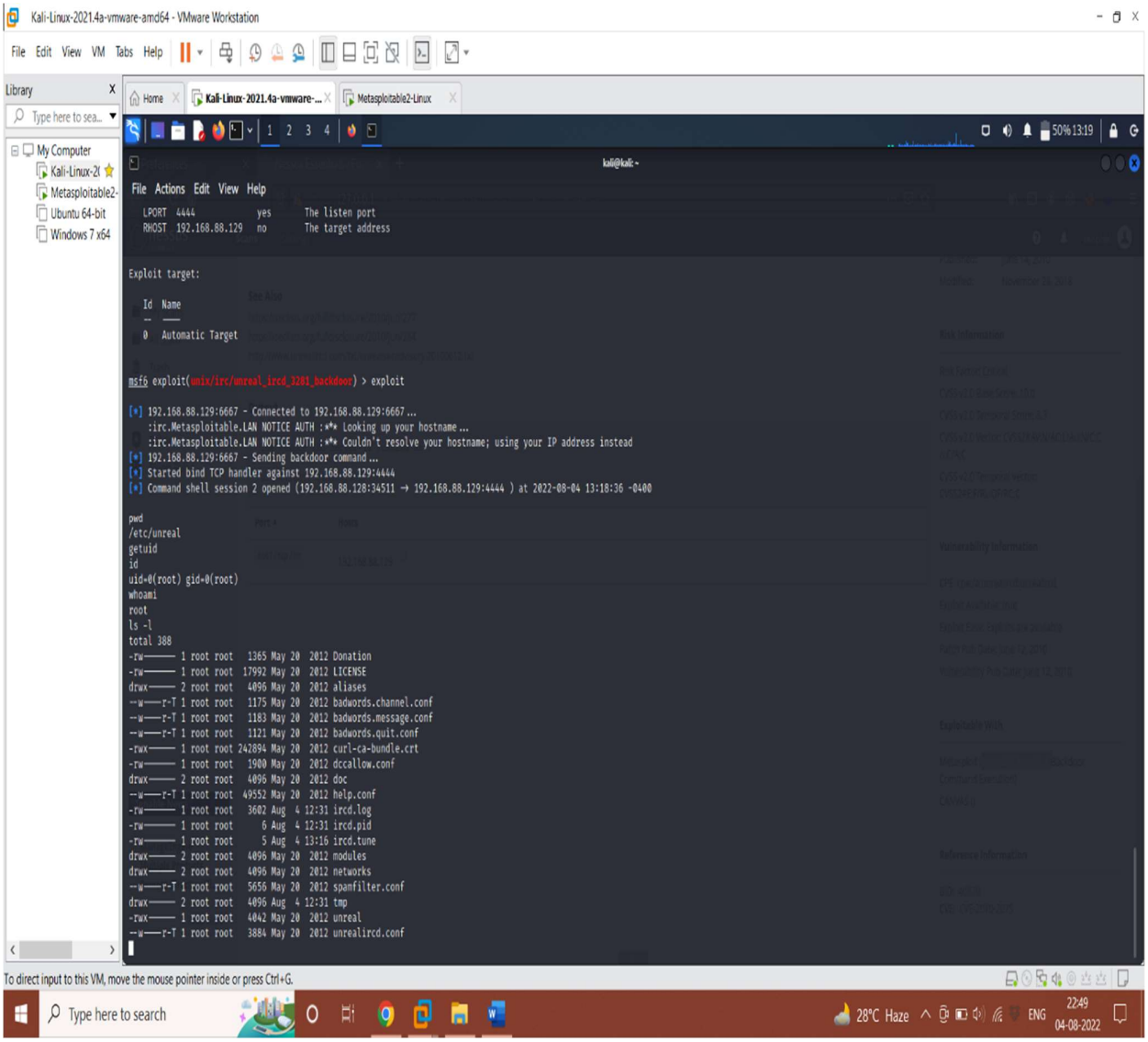
2.5.3. UnrealIRCd Backdoor Detection

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

With this vulnerability a attacker can get root access and it was able to exploit from Metasploit



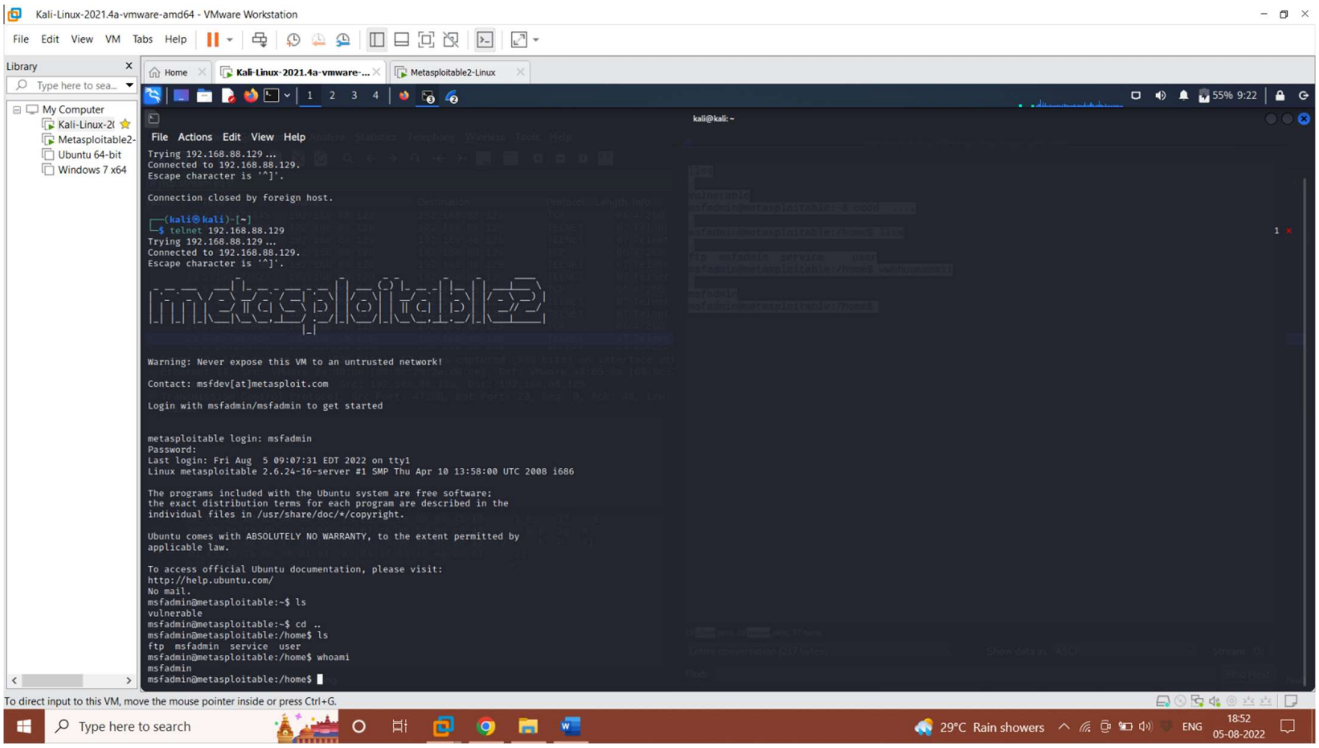
2.5.4 Unencrypted Telnet Server

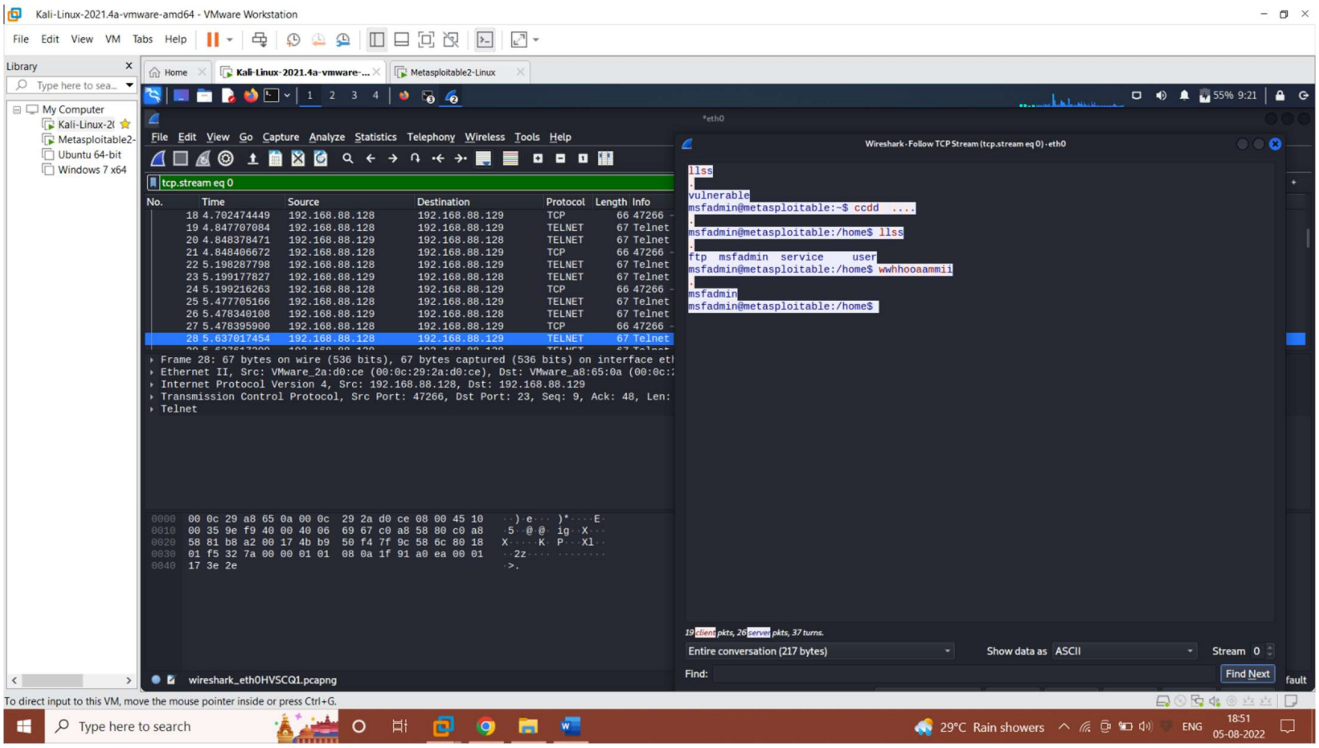
Risk Factor: Medium

CVSS v3.0 Base Score 6.5

CVSS v2.0 Base Score: 5.8

Description : all communication between server and client are unencrypted. Attacker can act as man in middle look at traffic.





2.5.5. NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Output:

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
    - initrd
    - initrd.img
    - lib
    - lost+found
    - media
    - mnt
    - nohup.out
    - opt
    - proc
    - root
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var
    - vmlinuz
less...
```

3. Detected Vulnerabilities and Recommendations.

3.1. Name: vsftpd 2.3.4 - Backdoor Command Execution
recommendation: Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

3.2. Name: NFS Exported Share Information Disclosure
Recommendation: Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

3.3. Name: Unencrypted Telnet Server
Recommendation: close telnet service.

3.4. Name: UnrealIRCd Backdoor Detection
Recommendation: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

3.5. unix Operating System Unsupported Version Detection
recommendation: Upgrade to a version of the Unix operating system that is currently supported.