Title: Vulnerability Scanning

The tool used to identify the network port and vulnerability scanning.

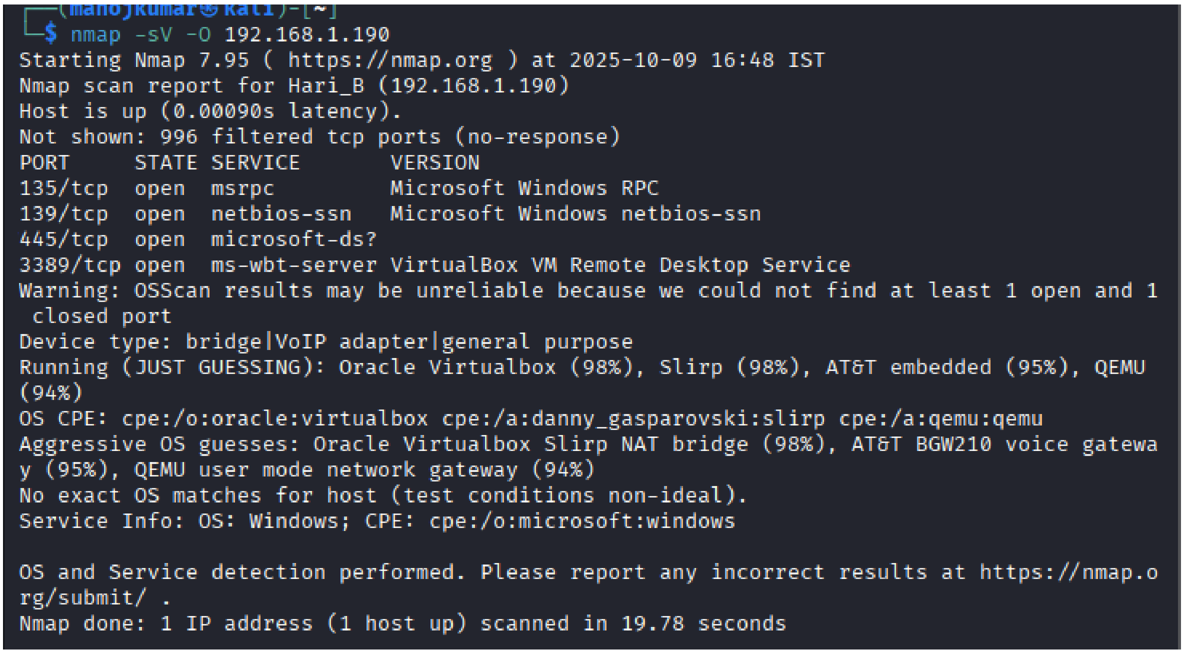
- Nmap
- OpenVAS
- Nikto

Task:

- **Nmap**

  Detect open ports and service versions.

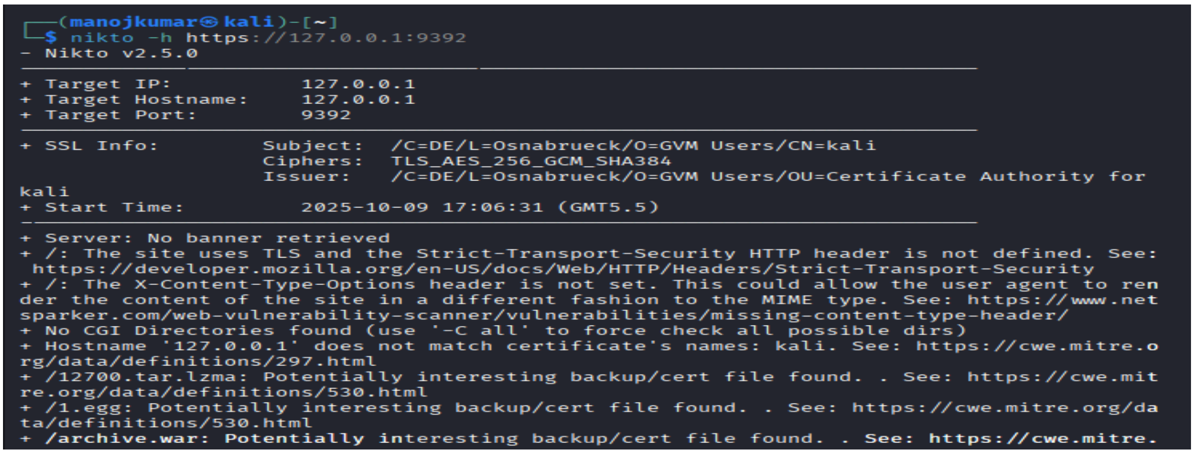
  nmap -sV -O 192.168.1.190



```
┌──(manojkumar㉿kali)-[~]
└─$ nmap -sV -O 192.168.1.190
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 16:48 IST
Nmap scan report for Hari_B (192.168.1.190)
Host is up (0.00090s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server VirtualBox VM Remote Desktop Service
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU
(94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gatewa
y (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.78 seconds
```

- **Nikto**

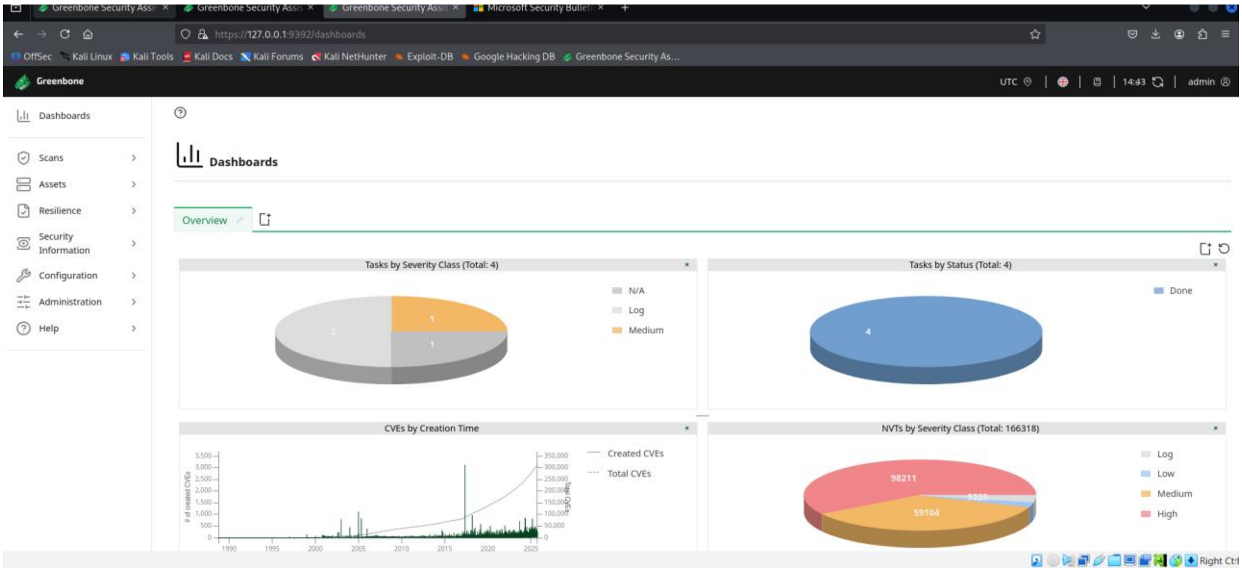
  Find web application / service issues.



```
┌──(manojkumar㉿kali)-[~]
└─$ nikto -h https://127.0.0.1:9392
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        9392
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=DE/L=Osnabrueck/O=GVM Users/CN=kali
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=DE/L=Osnabrueck/O=GVM Users/OU=Certificate Authority for
kali
+ Start Time:         2025-10-09 17:06:31 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See:
 https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to ren
der the content of the site in a different fashion to the MIME type. See: https://www.net
sparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '127.0.0.1' does not match certificate's names: kali. See: https://cwe.mitre.o
rg/data/definitions/297.html
+ /12700.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mit
re.org/data/definitions/530.html
+ /1.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/da
ta/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.
```

➢ OpenVAS

- Scan target from web UI (https://127.0.0.1:9392)
- Full vulnerability assessment with CVSS Scores.



➢ Analyse and Prioritize Vulnerabilities

Use CVSS Calculator to determine.

Severity	CVSS Range	Action
Critical	9.0 - 10.0	Immediate Action Required
High	7.0 - 8.9	Fix as soon as possible
Medium	4.0 - 6.9	Fix based on business impact
Low	0.1 - 3.9	Acceptable Risk Not required the immediate remediation

➢ Document Result

Record findings in a excel.

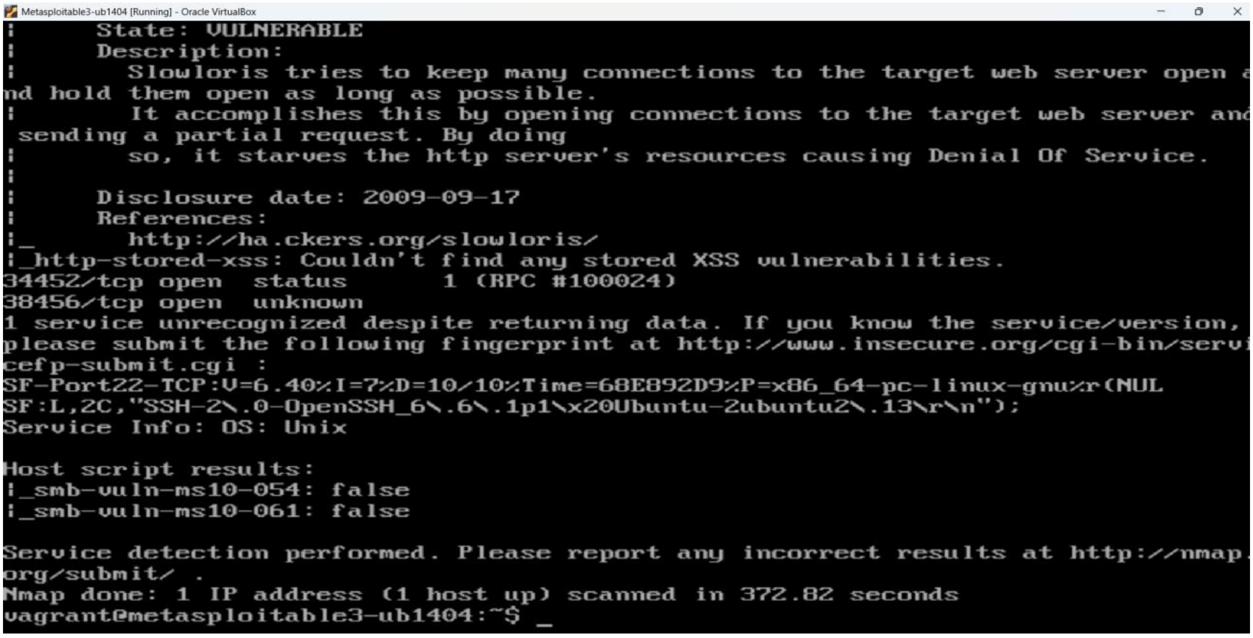
Scan ID	Vulnerability Name	CVSS Score	Priority	Host
1	Adobe Acrobat 9 PDF Document Encryption Weakness Vulnerability - Windows	7.5	High	192.168.1.190
2	Adobe AIR < 1.5 JavaScript Code Execution Vulnerability	6.8	Medium	192.168.1.190
3	ASP.NET Core 3.0.x < 3.0.2, 3.1.0 Multiple Vulnerabilities (Jan 2020)	8.8	High	192.168.1.190

Test: Scan a Metasploitable2 VM with Nmap (nmap -sV 192.168.1.100) and OpenVAS.

Nmap

Quick full surface scan.

nmap -p- -T4 -sV -sC --script vuln -oA nmap_full 10.0.2.15



Metasploitable3-ub1404 [Running] - Oracle VirtualBox

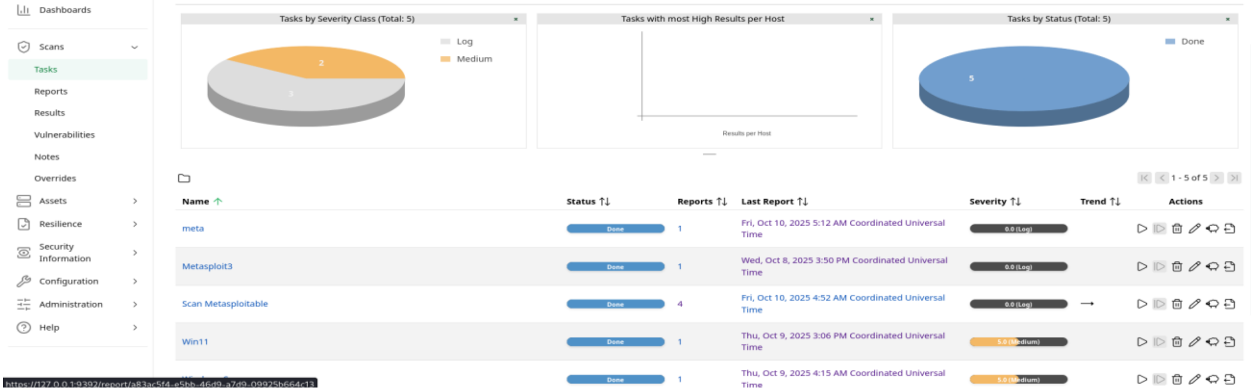
```
|       State: VULNERABLE
|       Description:
|         Slowloris tries to keep many connections to the target web server open a
nd hold them open as long as possible.
|         It accomplishes this by opening connections to the target web server and
 sending a partial request. By doing
|         so, it starves the http server's resources causing Denial Of Service.
|
|       Disclosure date: 2009-09-17
|       References:
|_        http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
34452/tcp open  status      1 (RPC #100024)
38456/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port22-TCP:V=6.40%I=7%D=10/10%Time=68E892D9%P=x86_64-pc-linux-gnu%r(NUL
SF:L,2C,"SSH-2\.0-OpenSSH_6\.6\.1p1\x20Ubuntu-2ubuntu2\.13\r\n");
Service Info: OS: Unix

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 372.82 seconds
vagrant@metasploitable3-ub1404:~$ _
```

OpenVAS

- ➢ Open browser to https://127.0.0.1:9392
- ➢ Login with your GVM Credential

- ➢ Create target and scan

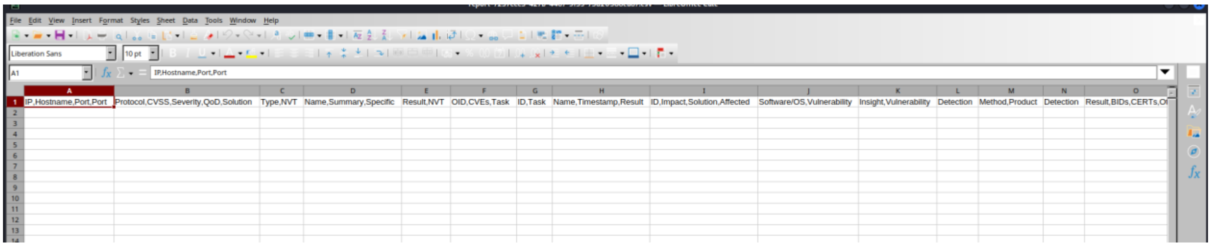
  - Create a target → set host (10.0.2.15)
  - Create task → select the target and a relevant scan config (like full and fast / full and deep)
  - Run task



Name	Status	Reports	Last Report	Severity	Trend	Actions
meta	Done	1	Fri, Oct 10, 2025 5:12 AM Coordinated Universal Time	0.0 (Log)		▷ ▯▷ 🗑 ✎
Metasploit3	Done	1	Wed, Oct 8, 2025 3:50 PM Coordinated Universal Time	0.0 (Log)		▷ ▯▷ 🗑 ✎
Scan Metasploitable	Done	4	Fri, Oct 10, 2025 4:52 AM Coordinated Universal Time	0.0 (Log)	→	▷ ▯▷ 🗑 ✎
Win11	Done	1	Thu, Oct 9, 2025 3:06 PM Coordinated Universal Time	5.0 (Medium)		▷ ▯▷ 🗑 ✎
[illegible]	Done	1	Thu, Oct 9, 2025 4:15 AM Coordinated Universal Time	5.0 (Medium)		▷ ▯▷ 🗑 ✎

https://127.0.0.1:9392/report/a83ac5f4-e5bb-46d9-a7d9-09925b664c13

- Export Report
    - After completion, export and XML, CSV, and PDF.



File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
A1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	IP,Hostname,Port,Port	Protocol,CVSS,Severity,QoD,Solution	Type,NVT	Name,Summary,Specific	Result,NVT	OID,CVEs,Task	ID,Task	Name,Timestamp,Result	ID,Impact,Solution,Affected	Software/OS,Vulnerability	Insight,Vulnerability	Detection	Method,Product	Detection	Result,BIDs,CERTs,O

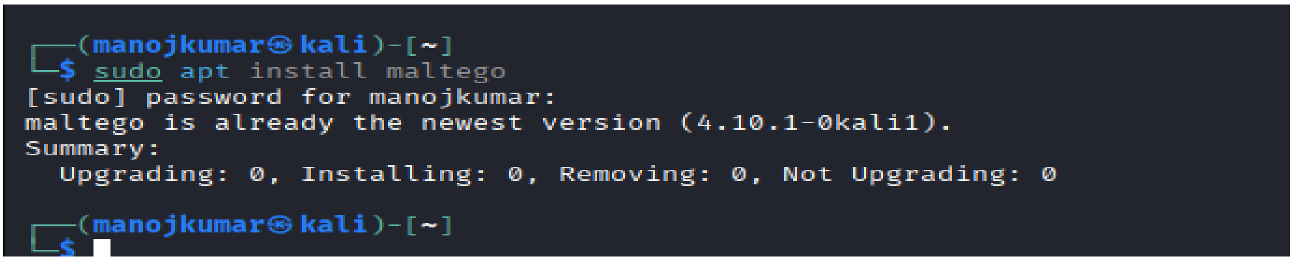
Done — the document now focuses on your titled case **"Critical Web Vulnerabilities"**, with there is no findings for **CVE** on **10.0.2.15** detailed technical info, and remediation steps.

Title: Reconnaissance Practice

Maltego

- Visualize and correlate information.
- Install maltego in kali

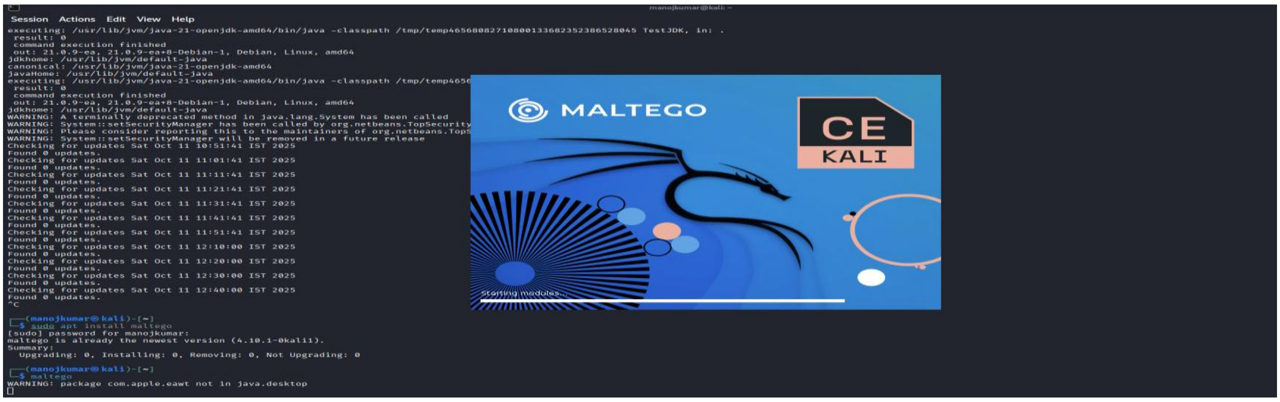
sudo apt install maltego



```
┌──(manojkumar㉿kali)-[~]
└─$ sudo apt install maltego
[sudo] password for manojkumar:
maltego is already the newest version (4.10.1-0kali1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(manojkumar㉿kali)-[~]
└─$ 
```

- Then open maltego through terminal

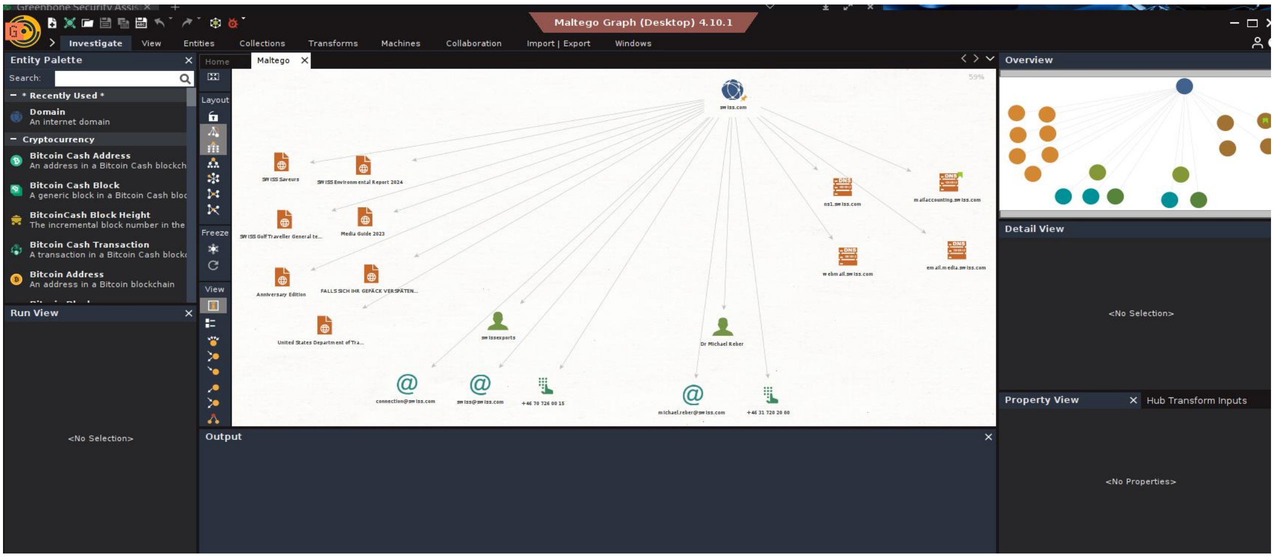
maltego



```
executing: /usr/lib/jvm/java-21-openjdk-amd64/bin/java -classpath /tmp/temp4656808271080013368235238652804S TestJDK, in: .
 result: 0
 command execution finished
 out: 21.0.9-ea, 21.0.9-ea+8-Debian-1, Debian, Linux, amd64
jdkhome: /usr/lib/jvm/default-java
canonical: /usr/lib/jvm/java-21-openjdk-amd64
javaHome: /usr/lib/jvm/default-java
executing: /usr/lib/jvm/java-21-openjdk-amd64/bin/java -classpath /tmp/temp4656
 result: 0
 command execution finished
 out: 21.0.9-ea, 21.0.9-ea+8-Debian-1, Debian, Linux, amd64
jdkhome: /usr/lib/jvm/default-java
WARNING: A terminally deprecated method in java.lang.System has been called
WARNING: System::setSecurityManager has been called by org.netbeans.TopSecurity
WARNING: Please consider reporting this to the maintainers of org.netbeans.TopS
WARNING: System::setSecurityManager will be removed in a future release
Checking for updates Sat Oct 11 10:51:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:01:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:11:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:21:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:31:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:41:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 11:51:41 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 12:10:00 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 12:20:00 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 12:30:00 IST 2025
Found 0 updates.
Checking for updates Sat Oct 11 12:40:00 IST 2025
Found 0 updates.
^C

┌──(manojkumar㉿kali)-[~]
└─$ sudo apt install maltego
[sudo] password for manojkumar:
maltego is already the newest version (4.10.1-0kali1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(manojkumar㉿kali)-[~]
└─$ maltego
WARNING: package com.apple.eawt not in java.desktop
```

Step:

- Open Maltego → Choose a transform set
- Start with Domain (swiss)
- Run transforms
  - ✓ **DNS Name (swiss.com)**
  - ✓ **MX Record (webmail.swiss.com)**
  - ✓ **To WHOIS information (swiss export, Michael Reber)**
- Analyze relationship and visualize results.



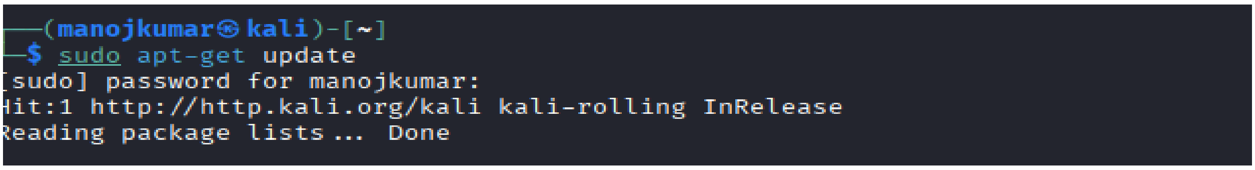
- Export the graph PNG or PDF.

Title: Exploitation Lab

Burp Suite

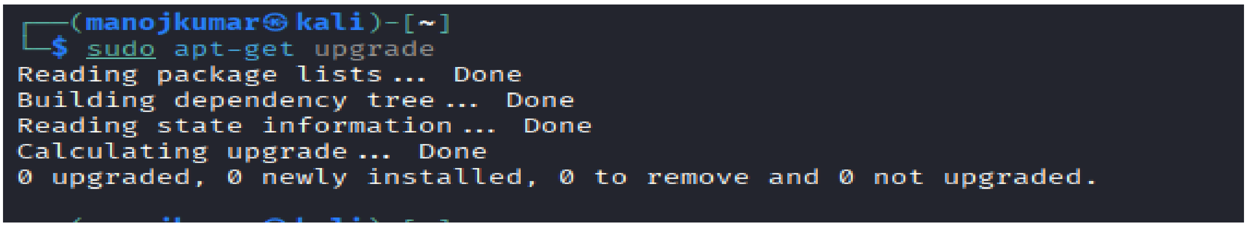
- ➢ Burpsuite is installed on kali linux by default
- ➢ However, if for whatever reason you don't have burp installed.

sudo apt-get update



```
──(manojkumar㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for manojkumar:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
```

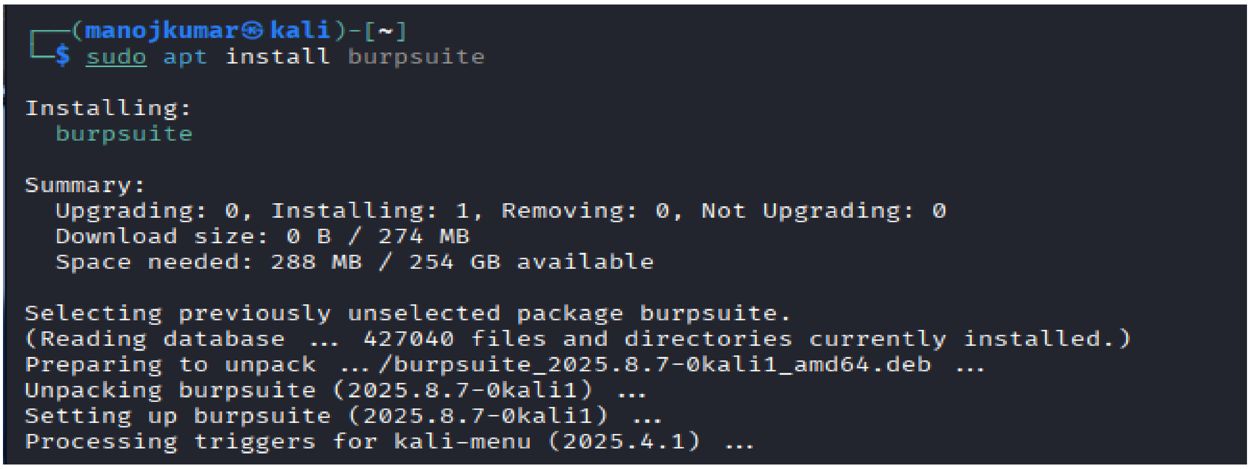
sudo apt-get upgrade



```
┌──(manojkumar㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- ➢ Then install burpsuite

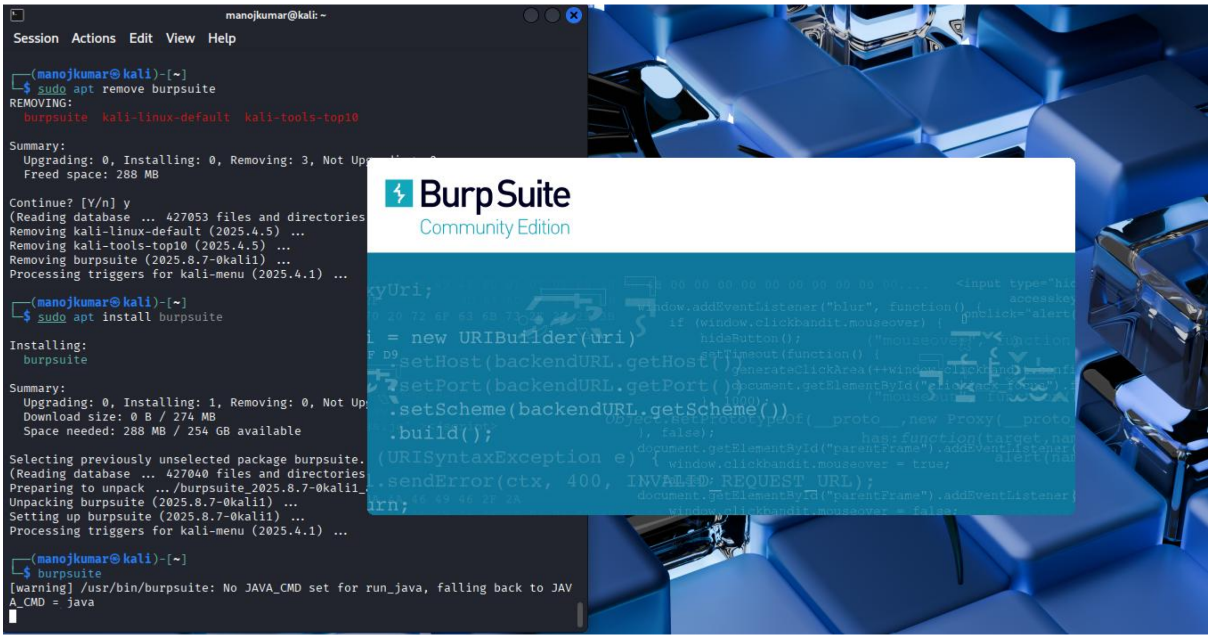
sudo apt install burpsuite



```
┌──(manojkumar㉿kali)-[~]
└─$ sudo apt install burpsuite

Installing:
  burpsuite

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 0
  Download size: 0 B / 274 MB
  Space needed: 288 MB / 254 GB available

Selecting previously unselected package burpsuite.
(Reading database ... 427040 files and directories currently installed.)
Preparing to unpack .../burpsuite_2025.8.7-0kali1_amd64.deb ...
Unpacking burpsuite (2025.8.7-0kali1) ...
Setting up burpsuite (2025.8.7-0kali1) ...
Processing triggers for kali-menu (2025.4.1) ...
```

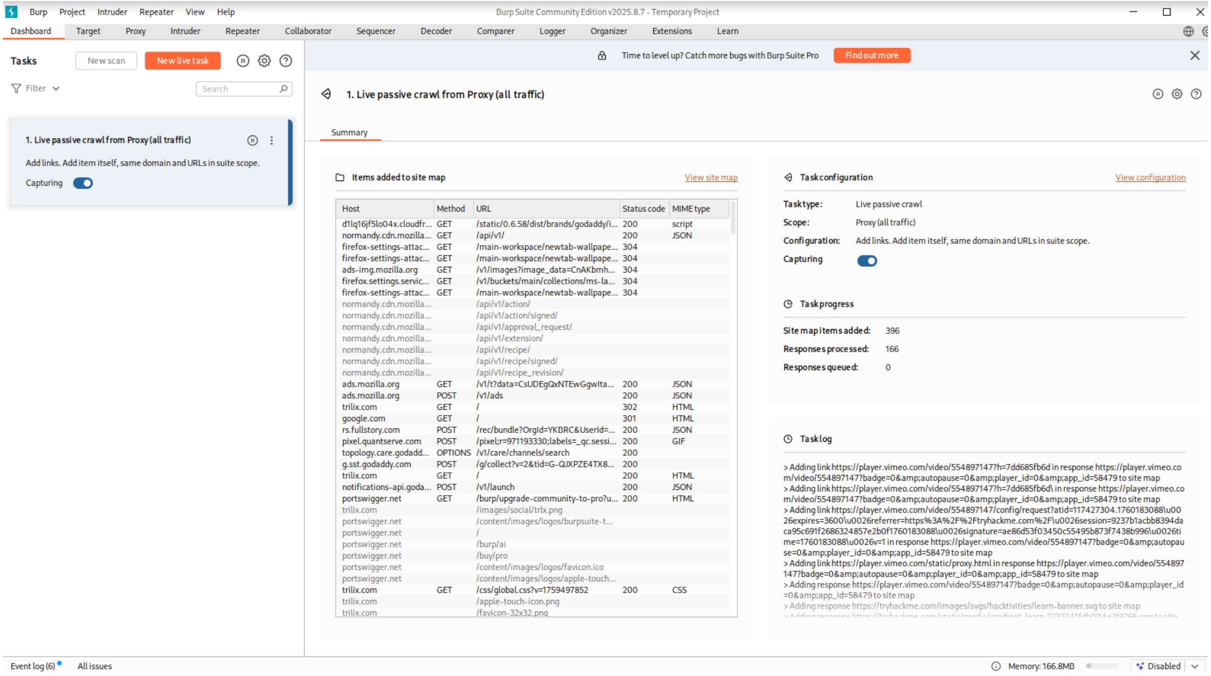
- ➢ **Open terminal and run burpsuite.**

burpsuite



```
┌──(manojkumar㉿kali)-[~]
└─$ sudo apt remove burpsuite
REMOVING:
  burpsuite  kali-linux-default  kali-tools-top10

Summary:
  Upgrading: 0, Installing: 0, Removing: 3, Not Up
  Freed space: 288 MB

Continue? [Y/n] y
(Reading database ... 427053 files and directories
Removing kali-linux-default (2025.4.5) ...
Removing kali-tools-top10 (2025.4.5) ...
Removing burpsuite (2025.8.7-0kali1) ...
Processing triggers for kali-menu (2025.4.1) ...

┌──(manojkumar㉿kali)-[~]
└─$ sudo apt install burpsuite

Installing:
  burpsuite

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Up
  Download size: 0 B / 274 MB
  Space needed: 288 MB / 254 GB available

Selecting previously unselected package burpsuite.
(Reading database ... 427040 files and directories
Preparing to unpack .../burpsuite_2025.8.7-0kali1_
Unpacking burpsuite (2025.8.7-0kali1) ...
Setting up burpsuite (2025.8.7-0kali1) ...
Processing triggers for kali-menu (2025.4.1) ...

┌──(manojkumar㉿kali)-[~]
└─$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAV
A_CMD = java
```

- Live passive crawl from proxy all traffic


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.7 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Tasks
New scan
New live task
Filter
Search
Time to level up? Catch more bugs with Burp Suite Pro
Find out more
Summary
View site map
View configuration
Event log (6)
All issues
Memory: 166.8MB
Disabled

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

1. Live passive crawl from Proxy (all traffic)

Items added to site map

Host	Method	URL	Status code	MIME type
d1lq16jf5lo04x.cloudfr...	GET	/static/0.6.58/dist/brands/godaddy/i...	200	script
normandy.cdn.mozilla...	GET	/api/v1/	200	JSON
firefox-settings-attac...	GET	/main-workspace/newtab-wallpape...	304	
firefox-settings-attac...	GET	/main-workspace/newtab-wallpape...	304	
ads-img.mozilla.org	GET	/v1/images?image_data=CnAKbmh...	304	
firefox.settings.servic...	GET	/v1/buckets/main/collections/ms-la...	304	
firefox-settings-attac...	GET	/main-workspace/newtab-wallpape...	304	
normandy.cdn.mozilla...		/api/v1/action/		
normandy.cdn.mozilla...		/api/v1/action/signed/		
normandy.cdn.mozilla...		/api/v1/approval_request/		
normandy.cdn.mozilla...		/api/v1/extension/		
normandy.cdn.mozilla...		/api/v1/recipe/		
normandy.cdn.mozilla...		/api/v1/recipe/signed/		
normandy.cdn.mozilla...		/api/v1/recipe_revision/		
ads.mozilla.org	GET	/v1/t?data=CsUDEgQxNTEwGgwIta...	200	JSON
ads.mozilla.org	POST	/v1/ads	200	JSON
trilix.com	GET	/	302	HTML
google.com	GET	/	301	HTML
rs.fullstory.com	POST	/rec/bundle?OrgId=YKBRC&UserId=...	200	JSON
pixel.quantserve.com	POST	/pixel;r=971193330;labels=_qc.sessi...	200	GIF
topology.care.godadd...	OPTIONS	/v1/care/channels/search	200	
g.sst.godaddy.com	POST	/g/collect?v=2&tid=G-QJXPZE4TX8...	200	
trilix.com	GET	/	200	HTML
notifications-api.goda...	POST	/v1/launch	200	JSON
portswigger.net	GET	/burp/upgrade-community-to-pro?u...	200	HTML
trilix.com		/images/social/trlx.png		
portswigger.net		/content/images/logos/burpsuite-t...		
portswigger.net		/		
portswigger.net		/burp/ai		
portswigger.net		/buy/pro		
portswigger.net		/content/images/logos/favicon.ico		
portswigger.net		/content/images/logos/apple-touch...		
trilix.com	GET	/css/global.css?v=1759497852	200	CSS
trilix.com		/apple-touch-icon.png		
trilix.com		/favicon-32x32.png		

Task configuration

Task type: Live passive crawl
Scope: Proxy (all traffic)
Configuration: Add links. Add item itself, same domain and URLs in suite scope.
Capturing

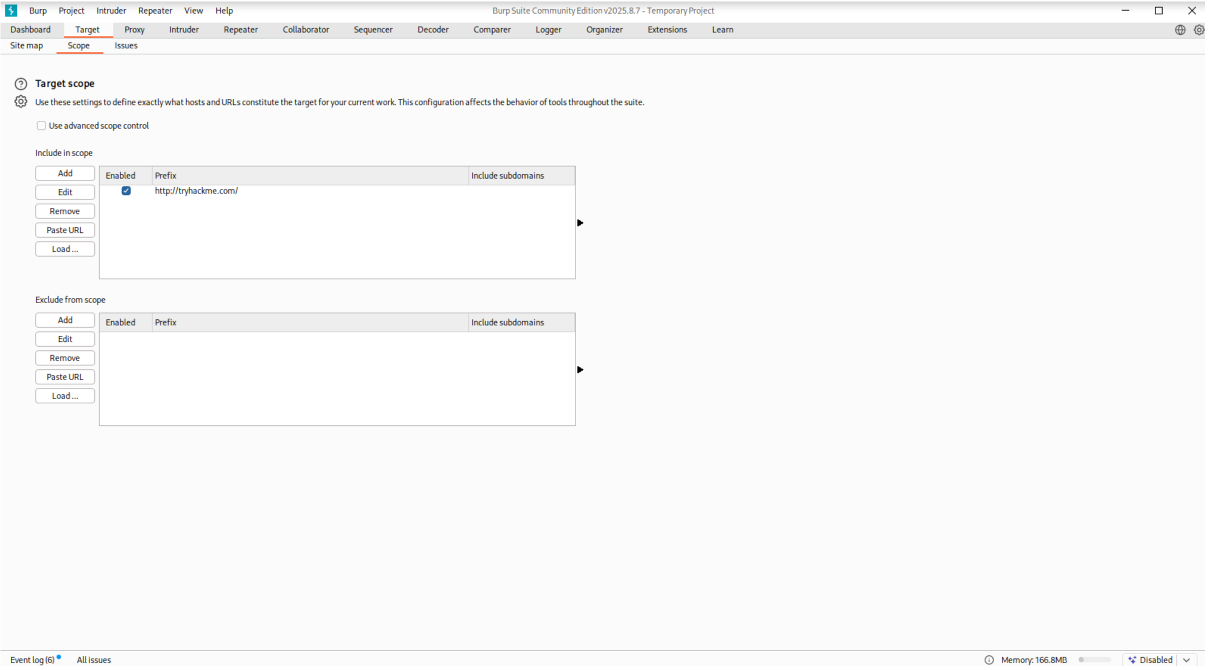
Task progress

Site map items added:	396
Responses processed:	166
Responses queued:	0

Task log

```
> Adding link https://player.vimeo.com/video/554897147?h=7dd685fb6d in response https://player.vimeo.com/video/554897147?badge=0&amp;autopause=0&amp;player_id=0&amp;app_id=58479 to site map
> Adding link https://player.vimeo.com/video/554897147?h=7dd685fb6d\ in response https://player.vimeo.com/video/554897147?badge=0&amp;autopause=0&amp;player_id=0&amp;app_id=58479 to site map
> Adding link https://player.vimeo.com/video/554897147/config/request?atid=117427304.1760183088\u0026expires=3600\u0026referrer=https%3A%2F%2Ftryhackme.com%2F\u0026session=9237b1acbb8394daca95c691f2686324857e2b0f1760183088\u0026signature=ae86d53f03450c55495b873f7438b996\u0026time=1760183088\u0026v=1 in response https://player.vimeo.com/video/554897147?badge=0&amp;autopause=0&amp;player_id=0&amp;app_id=58479 to site map
> Adding link https://player.vimeo.com/static/proxy.html in response https://player.vimeo.com/video/554897147?badge=0&amp;autopause=0&amp;player_id=0&amp;app_id=58479 to site map
> Adding response https://player.vimeo.com/video/554897147?badge=0&amp;autopause=0&amp;player_id=0&amp;app_id=58479 to site map
> Adding response https://tryhackme.com/images/svgs/hacktivities/learn-banner.svg to site map
> Adding response https://tryhackme.com/static/media/gradient_learn.2233241fdb004e2f9266.png to site
```

- Target Scope use these setting to define exactly what hosts and URLs constitute the target for your current network.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.7 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Site map Scope Issues
Add
Edit
Remove
Paste URL
Load ...
Add
Edit
Remove
Paste URL
Load ...
Event log (6)
All issues
Memory: 166.8MB
Disabled

Target scope

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools throughout the suite.

☐ Use advanced scope control

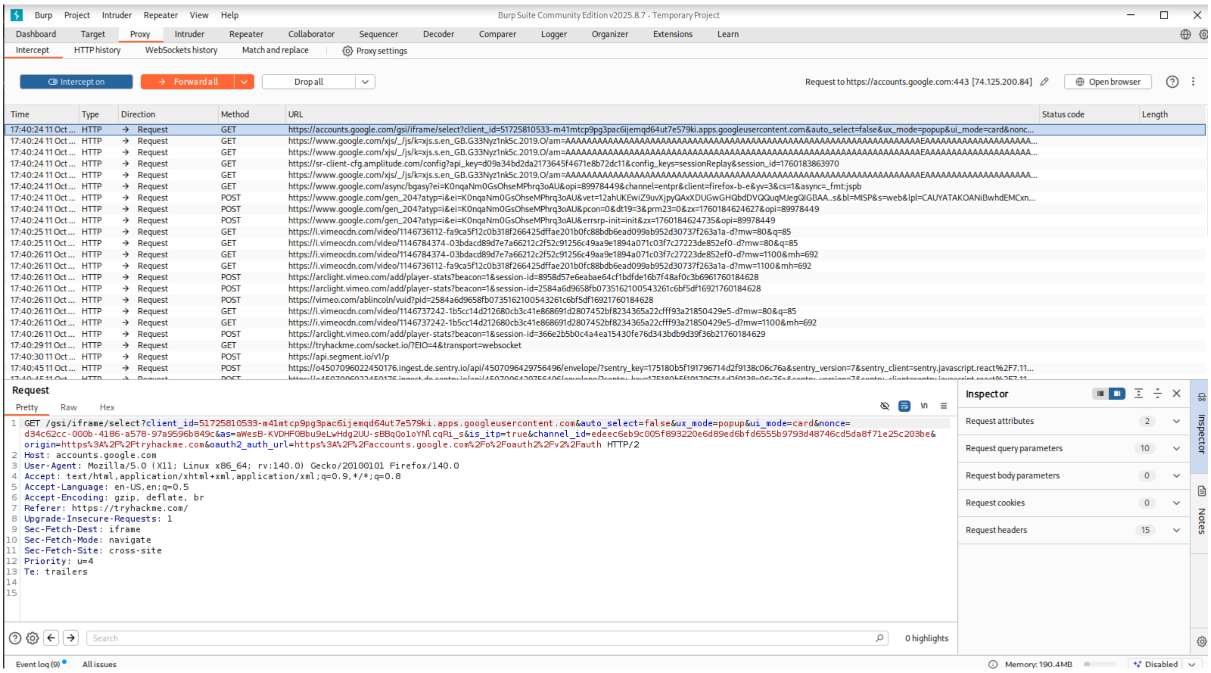
Include in scope

Enabled	Prefix	Include subdomains
☑	http://tryhackme.com/	

Exclude from scope

Enabled	Prefix	Include subdomains

Proxy route browser traffic through burp to capture full request and response. Use scope rules to avoid crawling out of target scope and save http history and tag interesting items.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.7 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward all
Drop all
Open browser

Request to https://accounts.google.com:443 [74.125.200.84]

Time	Type	Direction	Method	URL	Status code	Length
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://accounts.google.com/gsi/iframe/select?client_id=51725810533-m41mtcp9pg3pac6ijemqd64ut7e579ki.apps.googleusercontent.com&auto_select=false&ux_mode=popup&ui_mode=card&nonc...		
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_GB.G33Nyz1nk5c.2019.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAA...		
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_GB.G33Nyz1nk5c.2019.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAA...		
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://sr-client-cfg.amplitude.com/config?api_key=d09a34bd2da2173645f4671e8b72dc11&config_keys=sessionReplay&session_id=1760183863970		
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://www.google.com/xjs/_/js/k=xjs.s.en_GB.G33Nyz1nk5c.2019.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAA...		
17:40:24 11 Oct ...	HTTP	→ Request	GET	https://www.google.com/async/bgasy?ei=K0nqaNm0GsOhseMPhrq3oAU&opi=89978449&channel=entpr&client=firefox-b-e&yv=3&cs=1&async=_fmt:jspb		
17:40:24 11 Oct ...	HTTP	→ Request	POST	https://www.google.com/gen_204?atyp=i&ei=K0nqaNm0GsOhseMPhrq3oAU&vet=12ahUKEwiZ9uvXjpyQAxXDUGwGHQbdDVQQuqMJegQIGBAA..s&bl=MISP&s=web&lpl=CAUYATAKOANiBwhdEMCxn...		
17:40:24 11 Oct ...	HTTP	→ Request	POST	https://www.google.com/gen_204?atyp=i&ei=K0nqaNm0GsOhseMPhrq3oAU&pcon=0&dt19=3&prm23=0&zx=1760184624627&opi=89978449		
17:40:24 11 Oct ...	HTTP	→ Request	POST	https://www.google.com/gen_204?atyp=i&ei=K0nqaNm0GsOhseMPhrq3oAU&errsrp-init=init&zx=1760184624735&opi=89978449		
17:40:25 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146736112-fa9ca5f12c0b318f266425dffae201b0fc88bdb6ead099ab952d30737f263a1a-d?mw=80&q=85		
17:40:25 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146784374-03bdacd89d7e7a66212c2f52c91256c49aa9e1894a071c03f7c27223de852ef0-d?mw=80&q=85		
17:40:26 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146784374-03bdacd89d7e7a66212c2f52c91256c49aa9e1894a071c03f7c27223de852ef0-d?mw=1100&mh=692		
17:40:26 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146736112-fa9ca5f12c0b318f266425dffae201b0fc88bdb6ead099ab952d30737f263a1a-d?mw=1100&mh=692		
17:40:26 11 Oct ...	HTTP	→ Request	POST	https://arclight.vimeo.com/add/player-stats?beacon=1&session-id=8958d57e6eabae64cf1bdfde16b7f48af0c3b6961760184628		
17:40:26 11 Oct ...	HTTP	→ Request	POST	https://arclight.vimeo.com/add/player-stats?beacon=1&session-id=2584a6d9658fb0735162100543261c6bf5df16921760184628		
17:40:26 11 Oct ...	HTTP	→ Request	POST	https://vimeo.com/ablincoln/vuid?pid=2584a6d9658fb0735162100543261c6bf5df16921760184628		
17:40:26 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146737242-1b5cc14d212680cb3c41e868691d2807452bf8234365a22cfff93a21850429e5-d?mw=80&q=85		
17:40:26 11 Oct ...	HTTP	→ Request	GET	https://i.vimeocdn.com/video/1146737242-1b5cc14d212680cb3c41e868691d2807452bf8234365a22cfff93a21850429e5-d?mw=1100&mh=692		
17:40:26 11 Oct ...	HTTP	→ Request	POST	https://arclight.vimeo.com/add/player-stats?beacon=1&session-id=366e2b5b0c4a4ea15430fe76d343bdb9d39f36b21760184629		
17:40:29 11 Oct ...	HTTP	→ Request	GET	https://tryhackme.com/socket.io/?EIO=4&transport=websocket		
17:40:30 11 Oct ...	HTTP	→ Request	POST	https://api.segment.io/v1/p		
17:40:45 11 Oct ...	HTTP	→ Request	POST	https://o4507096022450176.ingest.de.sentry.io/api/4507096429756496/envelope/?sentry_key=175180b5f191796714d2f9138c06c76a&sentry_version=7&sentry_client=sentry.javascript.react%2F7.11...		

Request

```
GET /gsi/iframe/select?client_id=51725810533-m41mtcp9pg3pac6ijemqd64ut7e579ki.apps.googleusercontent.com&auto_select=false&ux_mode=popup&ui_mode=card&nonce=
d34c62cc-000b-4186-a578-97a9596b849c&as=aWesB-KVDHF0Bbu9eLwHdg2UU-sBBqQoloYNlcqRi_s&is_itp=true&channel_id=edeec6eb9c005f893220e6d89ed6bfd6555b9793d48746cd5da8f71e25c203be&
origin=https%3A%2F%2Ftryhackme.com&oauth2_auth_url=https%3A%2F%2Faccounts.google.com%2Fo%2Foauth2%2Fv2%2Fauth HTTP/2
Host: accounts.google.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://tryhackme.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Priority: u=4
Te: trailers
```

Inspector

Request attributes	2
Request query parameters	10
Request body parameters	0
Request cookies	0
Request headers	15

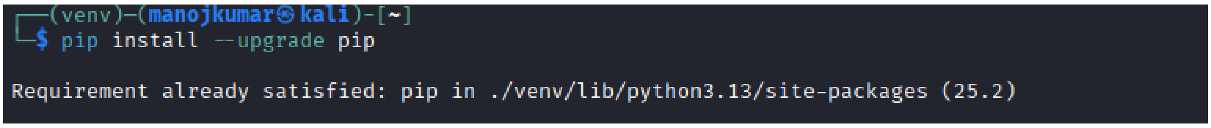
Title: Post-Exploitation Practice

Volatility

Volstility 3 actively developed, python 3, modern plugins and output formats.

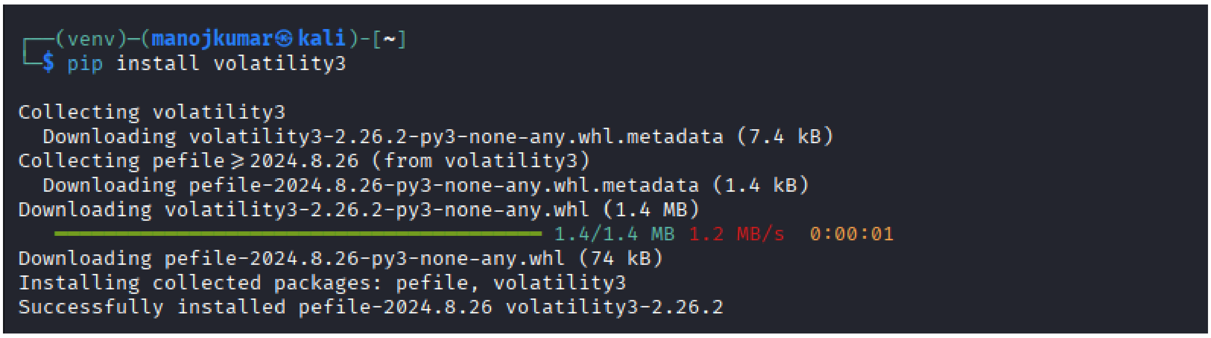
- Install volatility3 from pypi

pip install –upgrade pip



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ pip install --upgrade pip

Requirement already satisfied: pip in ./venv/lib/python3.13/site-packages (25.2)
```

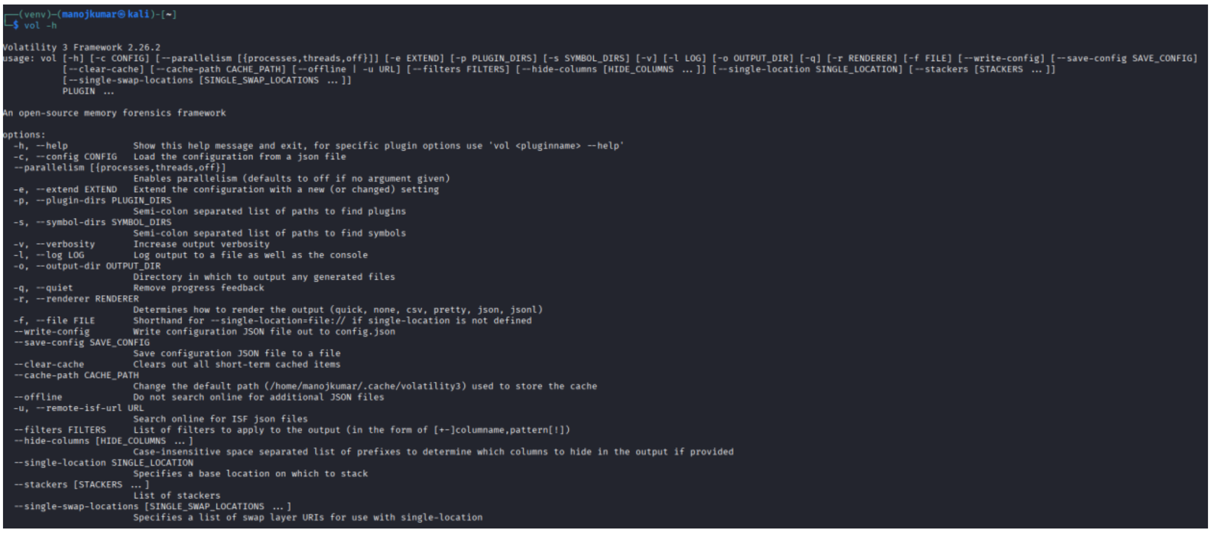
pip install volatility3



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ pip install volatility3

Collecting volatility3
  Downloading volatility3-2.26.2-py3-none-any.whl.metadata (7.4 kB)
Collecting pefile>=2024.8.26 (from volatility3)
  Downloading pefile-2024.8.26-py3-none-any.whl.metadata (1.4 kB)
Downloading volatility3-2.26.2-py3-none-any.whl (1.4 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.4/1.4 MB 1.2 MB/s  0:00:01
Downloading pefile-2024.8.26-py3-none-any.whl (74 kB)
Installing collected packages: pefile, volatility3
Successfully installed pefile-2024.8.26 volatility3-2.26.2
```

- Verify the volatility3 installation

vol -h

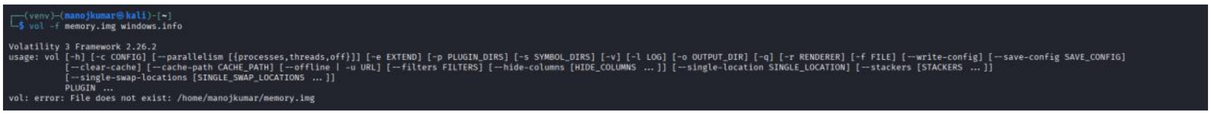


```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -h

Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...

An open-source memory forensics framework

options:
  -h, --help            Show this help message and exit, for specific plugin options use 'vol <pluginname> --help'
  -c, --config CONFIG   Load the configuration from a json file
  --parallelism [{processes,threads,off}]
                        Enables parallelism (defaults to off if no argument given)
  -e, --extend EXTEND   Extend the configuration with a new (or changed) setting
  -p, --plugin-dirs PLUGIN_DIRS
                        Semi-colon separated list of paths to find plugins
  -s, --symbol-dirs SYMBOL_DIRS
                        Semi-colon separated list of paths to find symbols
  -v, --verbosity       Increase output verbosity
  -l, --log LOG         Log output to a file as well as the console
  -o, --output-dir OUTPUT_DIR
                        Directory in which to output any generated files
  -q, --quiet           Remove progress feedback
  -r, --renderer RENDERER
                        Determines how to render the output (quick, none, csv, pretty, json, jsonl)
  -f, --file FILE       Shorthand for --single-location=file:// if single-location is not defined
  --write-config        Write configuration JSON file out to config.json
  --save-config SAVE_CONFIG
                        Save configuration JSON file to a file
  --clear-cache         Clears out all short-term cached items
  --cache-path CACHE_PATH
                        Change the default path (/home/manojkumar/.cache/volatility3) used to store the cache
  --offline             Do not search online for additional JSON files
  -u, --remote-isf-url URL
                        Search online for ISF json files
  --filters FILTERS     List of filters to apply to the output (in the form of [+-]columname,pattern[!])
  --hide-columns [HIDE_COLUMNS ...]
                        Case-insensitive space separated list of prefixes to determine which columns to hide in the output if provided
  --single-location SINGLE_LOCATION
                        Specifies a base location on which to stack
  --stackers [STACKERS ...]
                        List of stackers
  --single-swap-locations [SINGLE_SWAP_LOCATIONS ...]
                        Specifies a list of swap layer URIs for use with single-location
```

Volatility 3 Workflow

- Confirm image type, architecture, suggested plugins

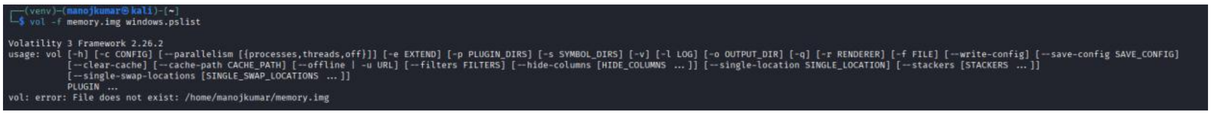
vol -f memory.img windows.info



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -f memory.img windows.info

Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
vol: error: File does not exist: /home/manojkumar/memory.img
```

- List processes

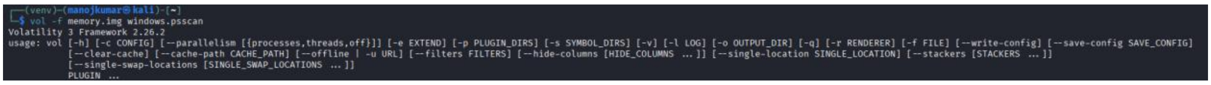
vol -f memory.img windows.pslist



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -f memory.img windows.pslist

Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
vol: error: File does not exist: /home/manojkumar/memory.img
```

- Find hidden

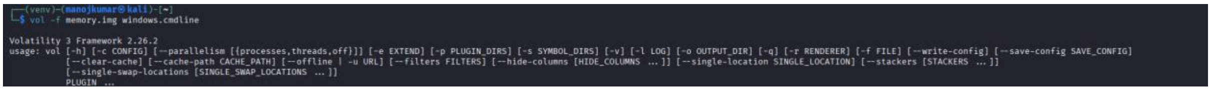
vol -f memory.img windows.psscan



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -f memory.img windows.psscan
Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
```

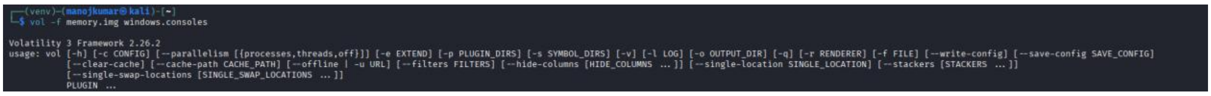
- Show command line

vol -f memory.img windows.cmdline



```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -f memory.img windows.cmdline

Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
```

vol -f memory.img windows.consoles



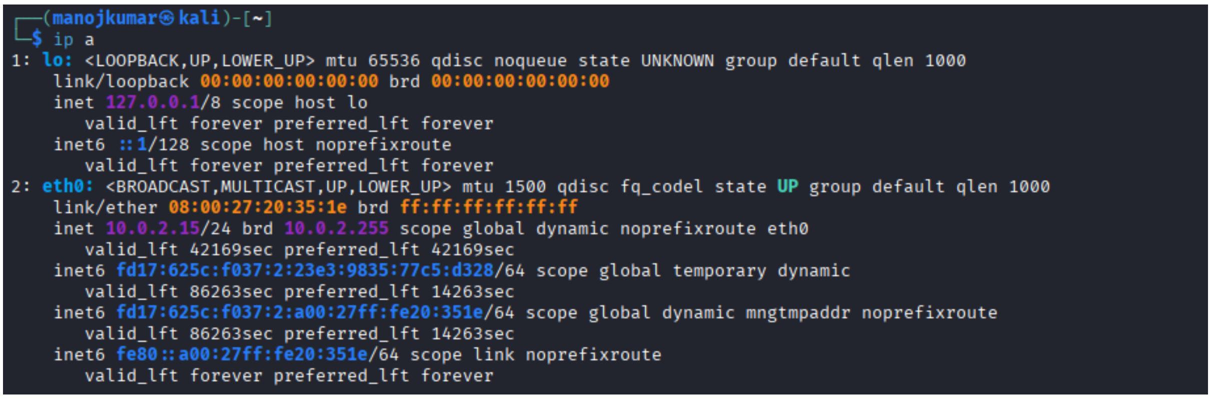
```
┌──(venv)─(manojkumar㉿kali)-[~]
└─$ vol -f memory.img windows.consoles

Volatility 3 Framework 2.26.2
usage: vol [-h] [-c CONFIG] [--parallelism [{processes,threads,off}]] [-e EXTEND] [-p PLUGIN_DIRS] [-s SYMBOL_DIRS] [-v] [-l LOG] [-o OUTPUT_DIR] [-q] [-r RENDERER] [-f FILE] [--write-config] [--save-config SAVE_CONFIG]
           [--clear-cache] [--cache-path CACHE_PATH] [--offline | -u URL] [--filters FILTERS] [--hide-columns [HIDE_COLUMNS ...]] [--single-location SINGLE_LOCATION] [--stackers [STACKERS ...]]
           [--single-swap-locations [SINGLE_SWAP_LOCATIONS ...]]
           PLUGIN ...
```

Title: Capstone Project: Full VAPT Cycle

Only run these steps on machines you own or explicitly have authorization to test.

- Find the target IP in kali

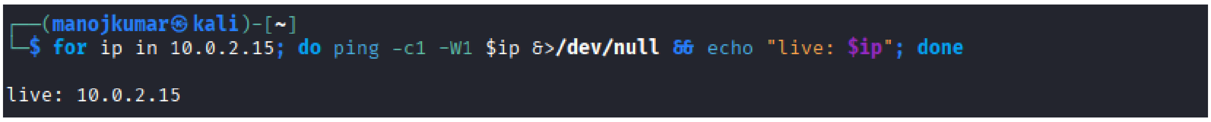
ip a



```
┌──(manojkumar㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:20:35:1e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 42169sec preferred_lft 42169sec
    inet6 fd17:625c:f037:2:23e3:9835:77c5:d328/64 scope global temporary dynamic
       valid_lft 86263sec preferred_lft 14263sec
    inet6 fd17:625c:f037:2:a00:27ff:fe20:351e/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86263sec preferred_lft 14263sec
    inet6 fe80::a00:27ff:fe20:351e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- Ping range to find live hosts

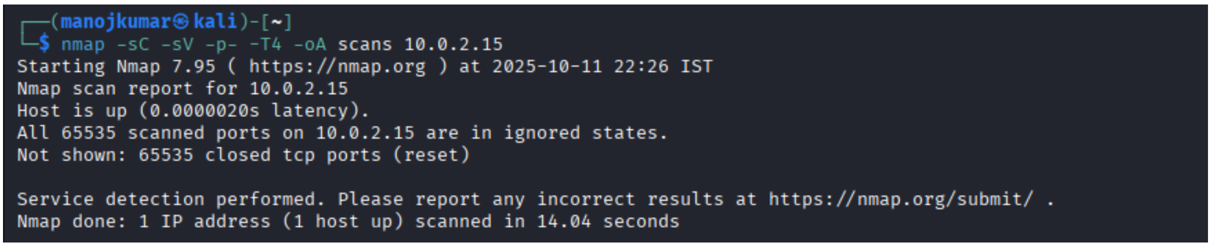
for ip in 10.0.2.15; do ping -c1 -W1 $ip &>/dev/null && echo "live: $ip"; done



```
┌──(manojkumar㉿kali)-[~]
└─$ for ip in 10.0.2.15; do ping -c1 -W1 $ip &>/dev/null && echo "live: $ip"; done

live: 10.0.2.15
```

- Fast port and service scan using nmap

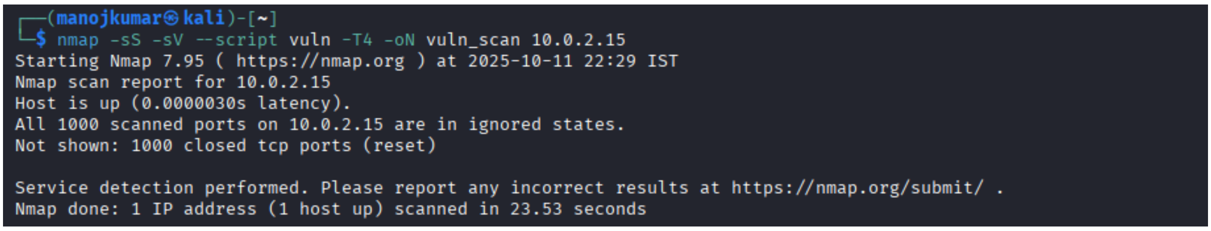
nmap -sC -sV -p- -T4 -oA scans/initial 10.0.2.15



```
┌──(manojkumar㉿kali)-[~]
└─$ nmap -sC -sV -p- -T4 -oA scans 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 22:26 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.04 seconds
```

- Focused scan

nmap -sS -sV --script vuln -T4 -oN vuln_scan 10.0.2.15

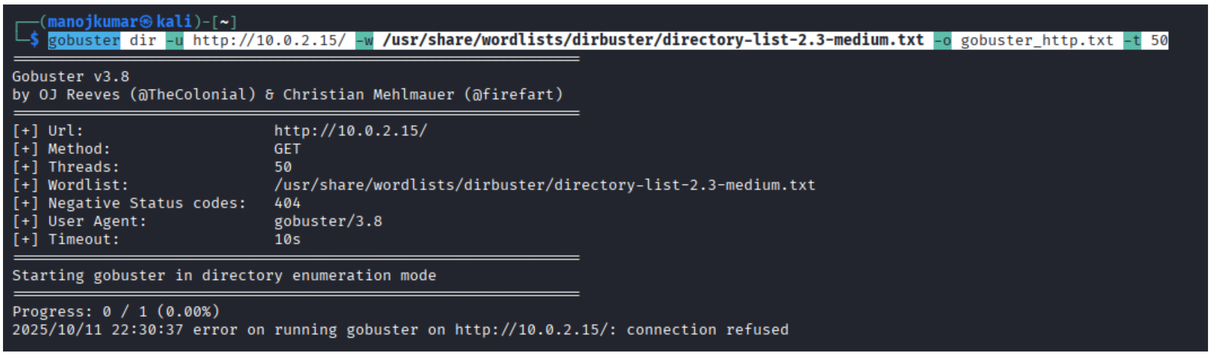


```
┌──(manojkumar㉿kali)-[~]
└─$ nmap -sS -sV --script vuln -T4 -oN vuln_scan 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 22:29 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.53 seconds
```

- ➢ Enumeration pre-service use the result of the nmap scan to enumerate services

HTTP/Web

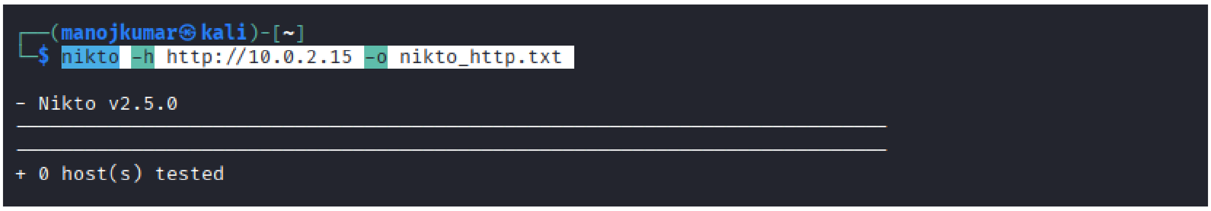
gobuster dir -u http://10.0.2.15/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobuster_http.txt -t 50



```
┌──(manojkumar㉿kali)-[~]
└─$ gobuster dir -u http://10.0.2.15/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobuster_http.txt -t 50
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.15/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 0 / 1 (0.00%)
2025/10/11 22:30:37 error on running gobuster on http://10.0.2.15/: connection refused
```

Nikto scan

nikto -h http://10.0.2.15 -o nikto_http.txt

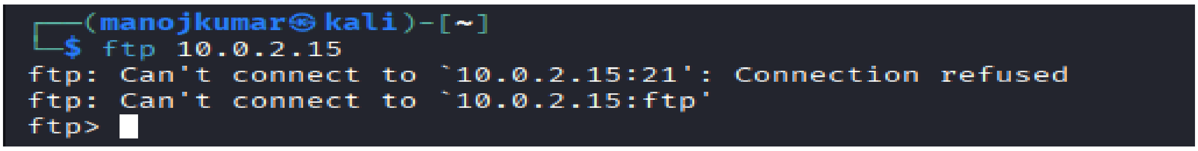


```
┌──(manojkumar㉿kali)-[~]
└─$ nikto -h http://10.0.2.15 -o nikto_http.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested
```

FTP

- ➢ Anonymous login check

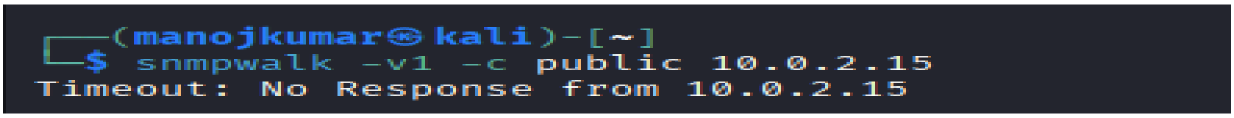
ftp 10.0.2.15



```
┌──(manojkumar㉿kali)-[~]
└─$ ftp 10.0.2.15
ftp: Can't connect to `10.0.2.15:21': Connection refused
ftp: Can't connect to `10.0.2.15:ftp'
ftp> █
```

SNMP

- ➢ SNMP is Check public community

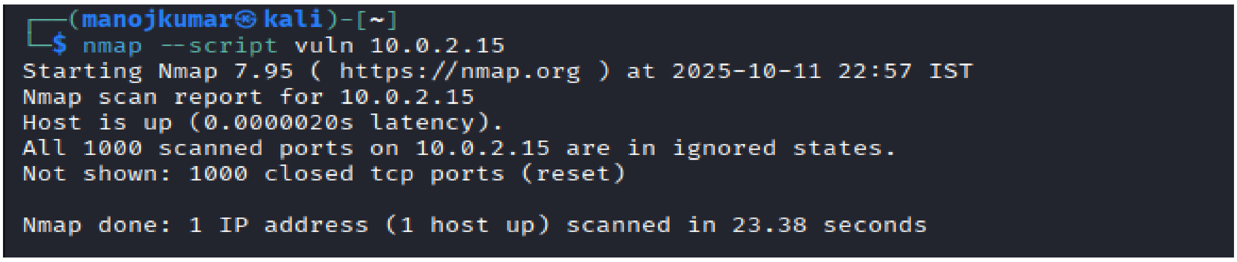


```
┌──(manojkumar㉿kali)-[~]
└─$ snmpwalk -v1 -c public 10.0.2.15
Timeout: No Response from 10.0.2.15
```

Vulnerability discovery

- Map observed versions to known CVEs locally

nmap --script vuln



```
┌──(manojkumar㉿kali)-[~]
└─$ nmap --script vuln 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 22:57 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 23.38 seconds
```