



GURU NANAK INSTITUTIONS TECHNICAL CAMPUS
(AUTONOMOUS)
SCHOOL OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

ETHICAL HACKING

LAB MANUAL

Subject Code: 18PC0CY08

Regulation: R 18

Class: III Year B. Tech. II Sem CSE (Cyber Security)



GURU NANAK INSTITUTIONS TECHNICAL CAMPUS
(AUTONOMOUS)
SCHOOL OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

ETHICAL HACKING LAB

LIST OF EXPERIMENTS

S. No.	Name of the Experiment
1.	Perform reconnaissance to find all the relevant information on the selected websites site using 10 network information-gathering tools.
2.	Gather information using Social Networking sites and Google Dorks.
3.	(1) Perform active reconnaissance using Angry IP Scanner, Soft perfect Network Scanner, Cain & Able. (2) Perform Network Scanning using NMAP in Windows and ZENMAP in kali Linux Software Based.
4.	(1) Install Wireshark and apply filters to gather different information. (II) Find the link accessed by the victim using Wireshark.
5.	Perform Session hijacking/ find credentials of unsecured real-time websites using Wireshark.
6.	Use the Nessus tool to find all the vulnerabilities with its level and generate a report for an organization
7.	(1) Execute basic commands of Linux. (ii) Use CHMOD command to change the privileges & permissions
8.	Generate Word list from using wordlist generator Crunch.
9.	Exploit windows to gain access of victim's machine using Metasploit framework.
10.	(1) Install Hiren Boot in bootable pen drive. (ii) Perform windows Login Bypass Hiren Boot or active password changer



GURU NANAK INSTITUTIONS TECHNICAL CAMPUS
(AUTONOMOUS)
SCHOOL OF ENGINEERING & TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

11.	Perform Kali Linux Login Bypass in a virtual machine. Perform MAC Login Bypass in a virtual machine.
12.	Create a Trojan and Exploit the victim's machine by taking its complete access.
13.	Track keystrokes of the victim machine using Ardamax Keylogger.
14.	Exploit Windows XP using Metasploit
15.	Exploit Windows 7 using Metasploit

PROGRAM 1

Perform reconnaissance to find all the relevant information on the selected websites site using 10 network information-gathering tools.

AIM: Perform reconnaissance to find all the relevant information on the selected websites site using 10 network information-gathering tools.

System Requirements:

The installation requirements for Kali Linux will vary depending on what you would like to install and your setup. For system requirements:

- On the low end, you can set up Kali Linux as a basic Secure Shell (SSH) server with no desktop, using as little as 128 MB of RAM (512 MB recommended) and 2 GB of disk space.
- On the higher end, if you opt to install the default Xfce4 desktop and the kali-linux-default meta package, you should really aim for at least 2 GB of RAM and 20 GB of disk space.
- When using resource-intensive applications, such as Burp Suite, they recommend at least 8 GB of RAM (and even more if it is a large web application!) or using simultaneous programs at the same time.

Performing reconnaissance to find all the relevant information on the selected websites using 10 network information-gathering tools.

LIST OF TOOLS :

1. Ns lookup
2. Who is
3. Threat cops
4. Wappalyzer
5. way back machine
6. virus total
7. follow that page
8. Reverse Ip lookup
9. IP Geolocation
10. HTTrack

1. Ns lookup

Link: <https://www.nslookup.io/>

Find all DNS records for a domain name using this online tool. For example, try wikipedia.org
Or ww.twitter.com to view their DNS records.

Nslookup.io

Q www.cyberark.comFind DNS records

LearningBrowser extensionAPI

DNS records for **www.cyberark.com**

CloudflareGoogle DNSOpenDNSAuthoritativeLocal DNS


The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 104.17.195.105	5m
> 104.17.194.105	5m
> 104.17.193.105	5m
> 104.17.192.105	5m
> 104.17.196.105	5m

2 Who is

Link : <https://whois.domaintools.com/>

 **DomainTools**

PROFILECONNECTMONITOR SUPPORT

Whois Lookup

Whois Record for **OLX.com**

Domain Profile

Registrant	Domain Administrator
Registrant Org	OLX Global B.V.
Registrant Country	NL
Registrar	CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com , http://cscdbs.com Whois Server: whois.corporatedomains.com domainabuse@cscglobal.com (p) +1.8887802723
Registrar Status	clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited
Dates	8,838 days old Created on 1999-02-08 Expires on 2024-02-08 Updated on 2023-02-21
Name Servers	NS-1474.AWSDNS-56.ORG (has 48,180 domains) NS-1736.AWSDNS-25.CO.UK (has 266 domains) NS-718.AWSDNS-25.NET (has 21 domains) NS-99.AWSDNS-12.COM (has 29,047 domains)
Tech Contact	Domain Administrator OLX Global B.V. Taurusavenue 105, Hoofddorp, Noord-Holland, 2132 LS, NL domains@olx.com (p) +27.112893792 (f) +27.112893792

Tech Contact	Domain Administrator OLX Global B.V. Taurusavenue 105, Hoofddorp, Noord-Holland, 2132 LS, NL domains@olx.com (p) +27.112893792 (f) +27.112893792	
IP Address	23.53.34.8 - 705 other sites hosted on this server	↩
IP Location	 - Washington - Seattle - Akamai Technologies Inc.	
ASN	 AS20940 AKAMAI-ASN1, NL (registered Jul 10, 2001)	
Domain Status	Registered And No Website	
IP History	256 changes on 256 unique IP addresses over 17 years	↩
Registrar History	2 registrars with 2 drops	↩
Hosting History	5 changes on 6 unique name servers over 20 years	↩

Whois Record (last updated on 2023-04-21)

```

Domain Name: olx.com
Registry Domain ID: 3476932_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2023-02-21T06:17:44Z
Creation Date: 1999-02-08T00:00:00Z
Registrar Registration Expiration Date: 2024-02-08T05:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Sponsoring Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited

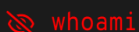
```

3 Threat cops

Link : <https://threatcops.com/>






We get information of –


Threatool is a Investigation platform designed in such a way that someone with no prior knowledge in cybersecurity can easily manage to investigate/gather in-depth intelligence on a person/topic efficiently. Threatool is created with a intention for Cyber crime Investigation, The main goal is to increase security awareness, teach about investigation, information security, countermeasures and give our users information on how to use the tool to test their own security/information on the internet. Threatool cannot be held responsible for any misuse of the given information. Any Malicious use of threatcops.com will not hold the developer/Threatool responsible, The content is solely for educational purposes.



 **How to OSINT ?**

 **USER ANALYSIS**
 **EMAIL INVESTIGATION**
 **PHONE NUMBER SEARCH**
 **DORKS - BUG BOUNTY**
 **IP | DOMAIN TOOLS**
 **SOCK PUPPET**

 **SOCIAL MEDIA INVESTIGATIONS [PRO]**
 **GEOINT - GEOSPATIAL INTELLIGENCE**
 **BREACHED DATA**
 **UNBLUR/CLEAR IMAGES**
 **CRIME INVESTIGATION**
 **RECEIVE SMS/EMAIL**

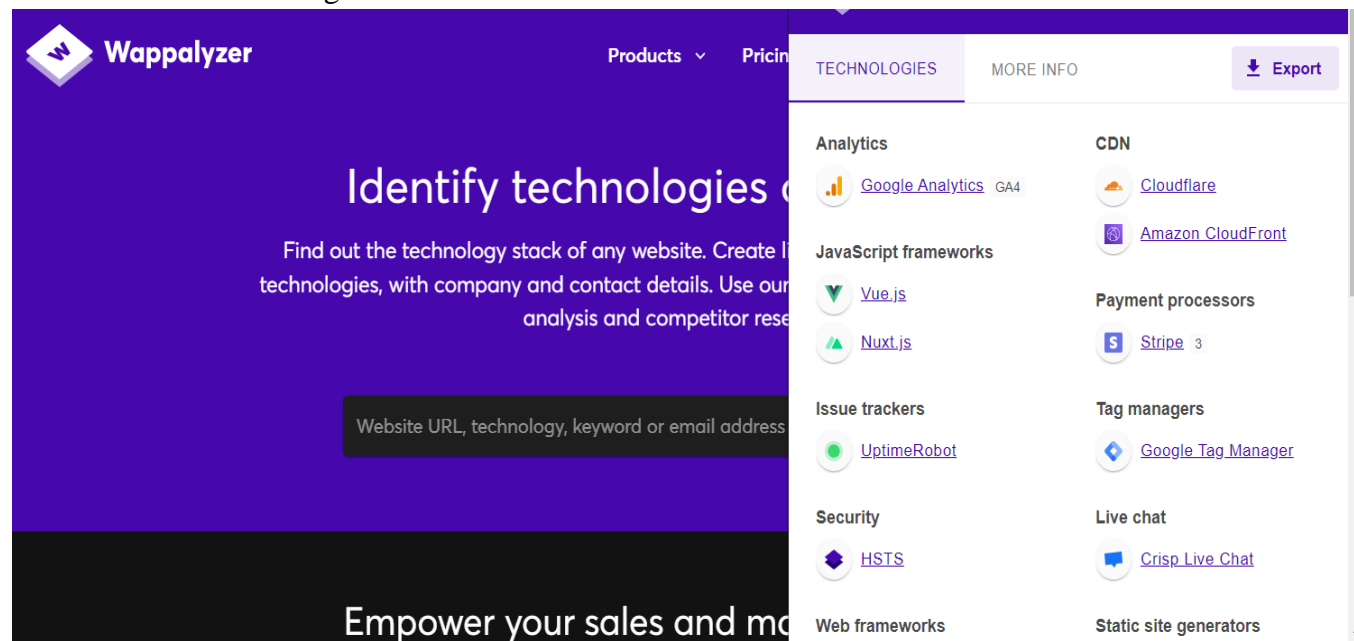
 **NEWS-INFOSEC**
 **PHISHING URL DETECTION**
 **LINKEDIN INVESTIGATION**
 **REVERSE IMAGE LOOKUP**
 **IMAGE FORENSICS**
 **LOCATION LOGGER**

4 Wappalyzer

Link : <https://www.wappalyzer.com/>

Find out the technology stack of any website. Create lists of websites that use certain technologies, with company and contact details. Use our tools for lead generation, market analysis and competitor research.

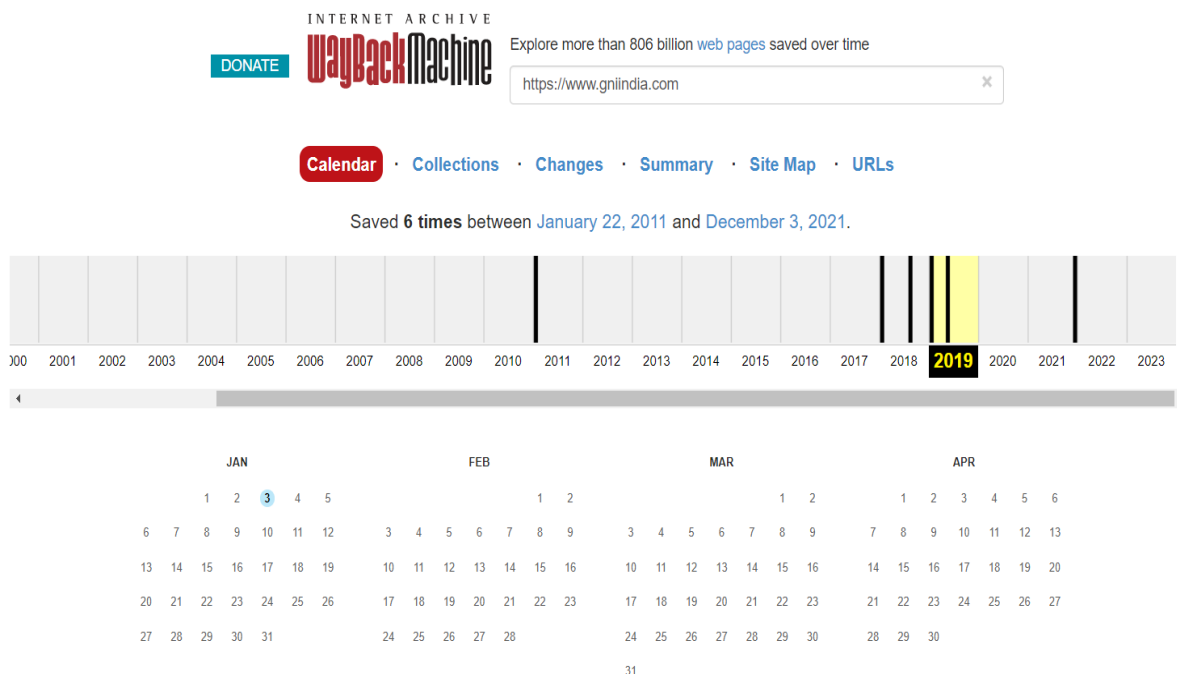
Extinction for search Engines :



5 Way back machine

Link : <https://web.archive.org/>


Explore more than 806 billion web pages saved over time



6 virus total

Link : <https://www.virustotal.com/>

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.


www.hackerrank.com

[Sign in](#)

0

/ 87

At least 10 detected files embedding this domain

www.hackerrank.com

hackerrank.com

[information technology](#)
[job search](#)
[media sharing](#)
[top-1M](#)

Registrar


Name.com, Inc.

Creation Date

11 years ago

Last Analysis Date

7 hours ago



Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
AlphaSOC	✓ Clean	Antiy-AVL	✓ Clean
ArcSight Threat Intelligence	✓ Clean	Avira	✓ Clean
benkow.cc	✓ Clean	Bfore Ai PreCrime	✓ Clean

7 follow that page

Link : <https://www.followthatpage.com/>

Follow That Page is a change detection and notification service that sends you an email when your favourite web pages have changed.



Welcome, mit!

[Home](#)
[Logout](#)
[Your pages](#)
[Your account](#)
[FAQ](#)
[Terms of use](#)
[Contact](#)

New page details

Page address

☐ Ignore numbers
 ☒ Report additions
 ☒ Report removals

Lines of context

Select here how many lines of context you want to see in the reports around the lines of text that have changed. Allowed values: 0 to 30000. If you specify 1 or more, all added and removed text is shown.

Description

You can enter a description of the page, to be used in the subject headers of the emails we send you. If empty, we use the page address (URL).

Report errors

☐ Report all errors, including server connection failures
 ☒ Report HTTP errors (like "page not found")
 ☐ Don't report errors

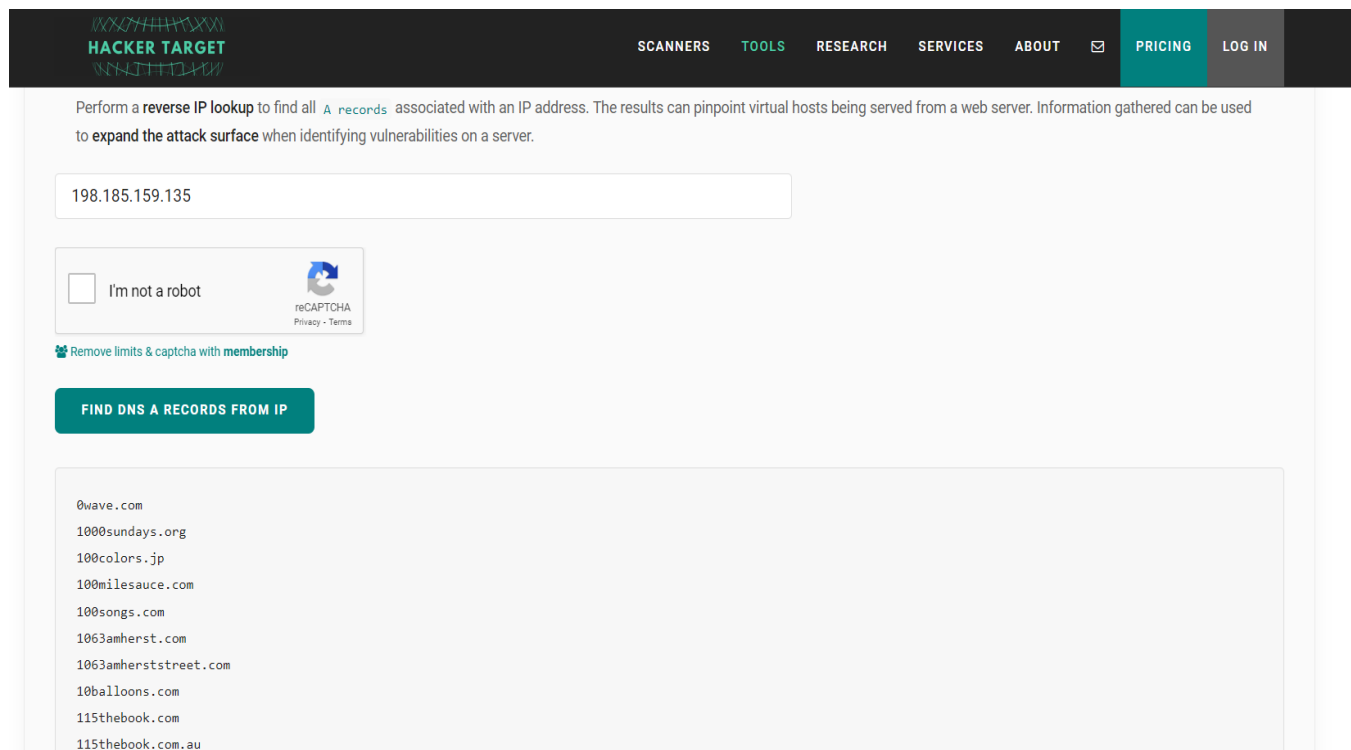
Frequency

☐ Check weekly (max. 20 pages)

8 Reverse Ip lookup

Link : <https://hackertarget.com/reverse-ip-lookup/>

The technique known as Reverse IP Lookup is a way to identify hostnames that have DNS (A) records associated with an IP address.



The screenshot shows the HackerTarget website's Reverse IP Lookup tool. The header is dark with the 'HACKER TARGET' logo on the left and navigation links (SCANNERS, TOOLS, RESEARCH, SERVICES, ABOUT, PRICING, LOG IN) on the right. The main content area has a light background. At the top, a text box explains the tool's purpose: 'Perform a reverse IP lookup to find all A records associated with an IP address. The results can pinpoint virtual hosts being served from a web server. Information gathered can be used to expand the attack surface when identifying vulnerabilities on a server.' Below this is a text input field containing the IP address '198.185.159.135'. Under the input field is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Remove limits & captcha with membership' link. A green button labeled 'FIND DNS A RECORDS FROM IP' is positioned below the reCAPTCHA. The results are displayed in a light gray box at the bottom, listing several domain names: 0wave.com, 1000sundays.org, 100colors.jp, 100milesauce.com, 100songs.com, 1063amherst.com, 1063amherststreet.com, 10balloons.com, 115thebook.com, and 115thebook.com.au.

HACKER TARGET

SCANNERS TOOLS RESEARCH SERVICES ABOUT PRICING LOG IN

Perform a reverse IP lookup to find all A records associated with an IP address. The results can pinpoint virtual hosts being served from a web server. Information gathered can be used to expand the attack surface when identifying vulnerabilities on a server.

198.185.159.135

☐ I'm not a robot

reCAPTCHA
Privacy - Terms

Remove limits & captcha with membership


FIND DNS A RECORDS FROM IP

0wave.com
1000sundays.org
100colors.jp
100milesauce.com
100songs.com
1063amherst.com
1063amherststreet.com
10balloons.com
115thebook.com
115thebook.com.au

9 IP Geolocation

Link : <https://ipgeolocation.io/>

Lookup any IPv4 or IPv6 address with our API to know its physical location, detect TOR, Proxy, VPN, threat, robot and user agent.



[Products](#)
[IP Location](#)
[Pricing](#)
[Documentation](#)
[Blog](#)
[Sign Up](#)
[Sign In](#)


Free IP Geolocation API and Accurate IP Lookup Database

Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.

[Get Free API Access](#)

Enter any IPv4, IPv6 address or domain name:

```

"ip": "103.157.12.220",
"country_name": "India",
"state_prov": "Telangana",
"city": "Farooqnagar",
"latitude": "17.06435",
"longitude": "78.20563",
"time_zone": "Asia/Kolkata",
"isp": "NIXI",
"currency": "Indian Rupee",
"country_flag": 


```

[View More](#)

10 HTTrack

Link : <https://www.httrack.com/>

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure.


Site mirroring in progress [2/10 (+8), 1948738 bytes] - [Hacker rank.whtt]

[File](#)
[Preferences](#)
[Mirror](#)
[Log](#)
[Window](#)
[Help](#)

OS <C:>

DATA <D:>

New Volume <E:>

edge

Hacking Codes

COMMANDS

Hacker rank

hts-cache

supraja

WinHTTrack

backblue.gif

fade.gif

index.html

location hack.txt

sms bomber.txt

supraja.whtt

Temp

VSC

New Volume <F:>

In progress: Transferring data...

Information

Bytes saved:	1.85MiB	Links scanned:	2/10 (+8)
Time:	6s	Files written:	8
Transfer rate:	174.32KiB/s (81.53KiB/s)	Files updated:	0
Active connections:	1	Errors:	0

☒ Actions

scanning	s://www.wa...yzer.com/_nuxt	SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP
		SKIP

< Back

Next >

Cancel

Help

Page 10

PROGRAM 2

Gather information using Social Networking sites and Google Dorks.

AIM: Gather information using Social Networking sites and Google Dorks.

Introduction :

Most of us begin our online searching by merely typing keywords into the search bar, but in doing so, we have already missed an opportunity to optimize our results. Google dorking makes use of commands called Operators that allow users to modify their search results in many ways. For instance, a user searching for information related to private universities in the United States could type Harvard AND Stanford into Google to only return search results that contain both keywords. Note that Google dorks are case-sensitive, so typing Harvard and Stanford would not generate the same results. While this is a very simple Google dorking technique, there are many more that allow users to modify search results in more profound ways.

Many of these techniques are useful on their own. Still, much of their utility is derived from the user's ability to combine them to return very specific results from Google.

By using these Operators in combination with each other (and the many others that exist), users can target specific information more easily.

Let's look at two of these Operators quickly to see how they work together to return specific results.

The site: Operator allows us to perform a Google search that will only return results that are hosted on the designated site. For instance, Harvard site: Wikipedia.org will only return search results related to the keyword Harvard from Wikipedia.org.

The – (minus) Operator allows the user to exclude specific results from their search. By combining these two Operators, we can create the search Harvard -site: Wikipedia.org, which will return search results from Google while excluding any results from Wikipedia. As you become more proficient with each Operator, you will also find more ways to combine these Operators to find useful information regarding your investigations.

To utilize the power of combining Google search Operators, though, we need to learn a few more. In this PDF cheat sheet, we list out all the useful Google dorks (search operators). Download the cheat sheet now to start using them!

Link : <https://www.exploit-db.com/google-hacking-database>

```
# Google Dork: intitle:"webcamXP 5" inurl:admin.html
# Various Online Devices
# Date:14/10/2021
# Exploit Author: César Hernández Obispo
```

Gathering information of WEBCAMXP5

WebcamXP

Webcamxp is a software for recording video stream from webcams, creating a home video surveillance system and recording video broadcast from online cameras. The key features of webcamxp are as follows:

WebcamXP allows you to monitor your home, business from anywhere in the world with Internet access, turning your computer into a video surveillance system. The ability to connect remotely using a computer or mobile phone, make an online video broadcast to your website, perform automatic recording or launch certain actions using a motion detector — and all this is adapted in the Webcamxp 5 and Webcam 7 software.

The screenshot shows the Exploit Database interface with a search for 'Webcamxp'. The results table lists 10 entries, all categorized as 'Various Online Devices'. The entries include details such as the date added, the Google Dork used, and the author. The interface also features a sidebar with navigation icons, a top navigation bar, and a bottom pagination bar.

Date Added	Dork	Category	Author
2021-11-09	intitle:"webcamXP" inurl:8080	Various Online Devices	Krishna Agarwal
2021-10-19	intitle:"webcamXP 5" inurl:admin.html	Various Online Devices	César Hernández Obispo
2021-05-28	intitle:"webcamxp" "Flash JPEG Stream"	Various Online Devices	Anmol K Sachan
2021-05-25	inurl:mobile.html intitle:webcamXP	Various Online Devices	Anmol K Sachan
2021-03-19	intitle:"webcamxp 5" intext:"live stream"	Various Online Devices	Hitesh Parmar
2020-03-30	intitle:"webcamXP 5" inurl:8080 'Live'	Various Online Devices	Siddhesh Thakur
2017-06-05	intitle:"webcamXP 5" -download	Various Online Devices	anonymous
2016-03-24	intext:"powered by webcamXP 5"	Various Online Devices	anonymous
2004-10-11	intitle:"my webcamXP server" inurl:".8080"	Various Online Devices	anonymous
2004-07-16	"powered by webcamXP" "ProBroadcast"	Various Online Devices	anonymous

Showing 1 to 10 of 10 entries (filtered from 7,669 total entries)

Pagination: FIRST PREVIOUS 1 NEXT LAST

Live cameras: WebcamXP

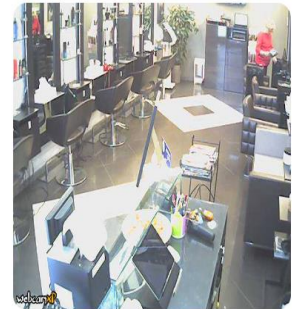
« 1 2 3 4 5 6 »



Live camera in Goppingen, Germany





Live camera in Tromso, Norway



Live camera in Ivrea, Italy

WEBCAMXP 5
WEBCAMS AND IP CAMERAS SERVER FOR WINDOWS ALTERNATIV STREAM LOGIN



Pan, Tilt & Zoom


[Home](#)
[Multi view](#)
[Smartphone](#)
[Gallery](#)
[Administration](#)

Not logged in

Source 1 JavaScript

webcamXP 5
08:51:43
Frame 10764

<http://seccam.mywire.org>

Program 3

- (1) Perform active reconnaissance using Angry IP Scanner, Soft perfect Network Scanner, Cain & Able.
- (2) Perform Network Scanning using NMAP in Windows and ZENMAP in kali Linux Software Based.

AIM: (1) Perform active reconnaissance using Angry IP Scanner, Soft perfect Network Scanner, Cain & Able.

Description:

Angry IP Scanner

Scanning of computer networks (searching for addresses with known properties) is a practice that is often used by both network administrators and crackers. Although it is widely accepted that activity of the latter is often illegal, most of the time they depend on exactly the same tools that can be used for perfectly legitimate network administration – just like a kitchen knife that can be used maliciously. Thanks to the recent activity of mass-media on the subject (that popularized the wrong term for a cracker – a ‘hacker’), nowadays every educated person more or less understands the reasons and goals that stand behind malicious cracking: curiosity, stealing of information, making damage, showing self-importance to the world, etc..

Angry IP Scanner is widely-used open-source and multi-platform network scanner. As a rule, almost all such programs are open-source, because they are developed with the collaboration of many people without having any commercial goals. Secure networks are possible only with the help of open-source systems and tools, possibly reviewed by thousands of independent experts and hackers alike.

SoftPerfect Network Scanner

Powerful multipurpose network administration tool for Windows and macOS

SoftPerfect Network Scanner iconThis fast, highly configurable IPv4/IPv6 scanner can streamline many of your network support procedures. Its well-designed interface, light weight and portability coupled with an extensive range of options and advanced features make SoftPerfect Network Scanner an invaluable tool, whether you are a professional system administrator, someone providing occasional network maintenance, or a general user interested in computer security.

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell. It also scans for remote services, registry, files and performance counters; offers flexible filtering and display options and exports NetScan results to a variety of formats from XML to JSON.

Cain & Able

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

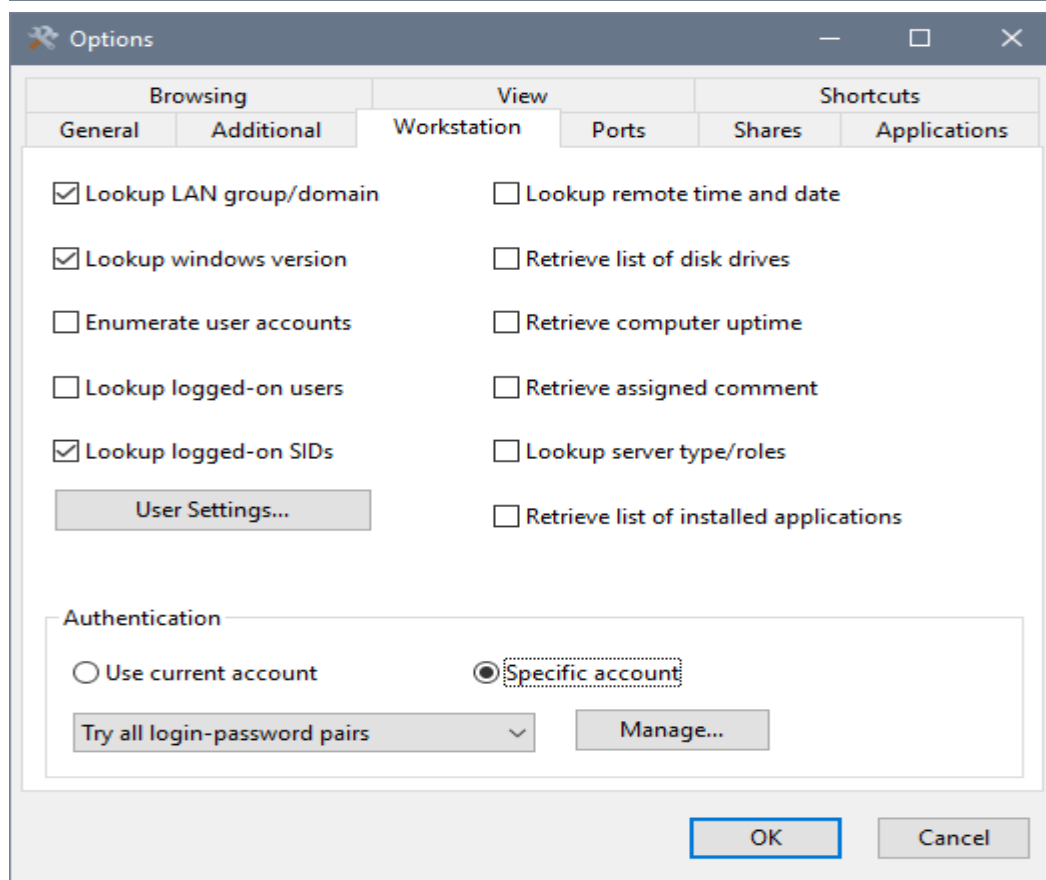
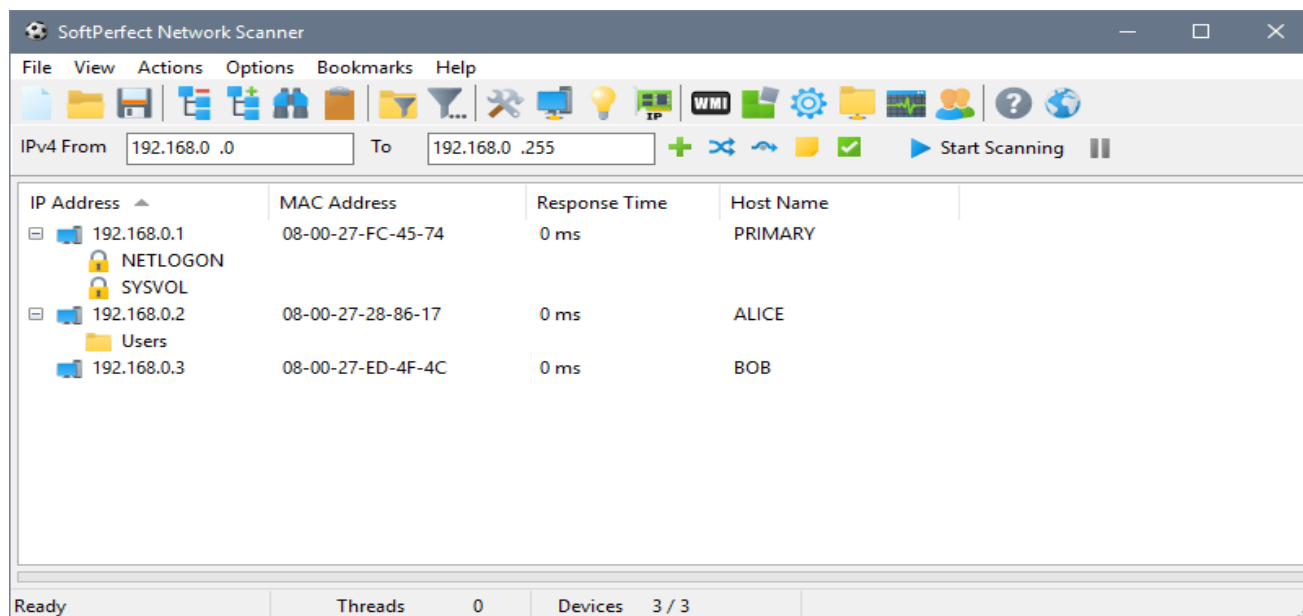
Angry IP Scanner

The screenshot shows the 'IP Range - Angry IP Scanner' window. The IP Range is set to 195.80.116.186 to 195.80.116.186. The Hostname is e-estonia.com. The IP ↑ and Netmask buttons are visible. A green 'Start' button is present. The scan results are displayed in a table with columns: IP, Ping, Hostname, Ports [4+], and Web detect. The IP 195.80.116.184 is highlighted in orange, showing a ping of 22 ms, hostname lists.eas.ee, port 80, and web service Apache.

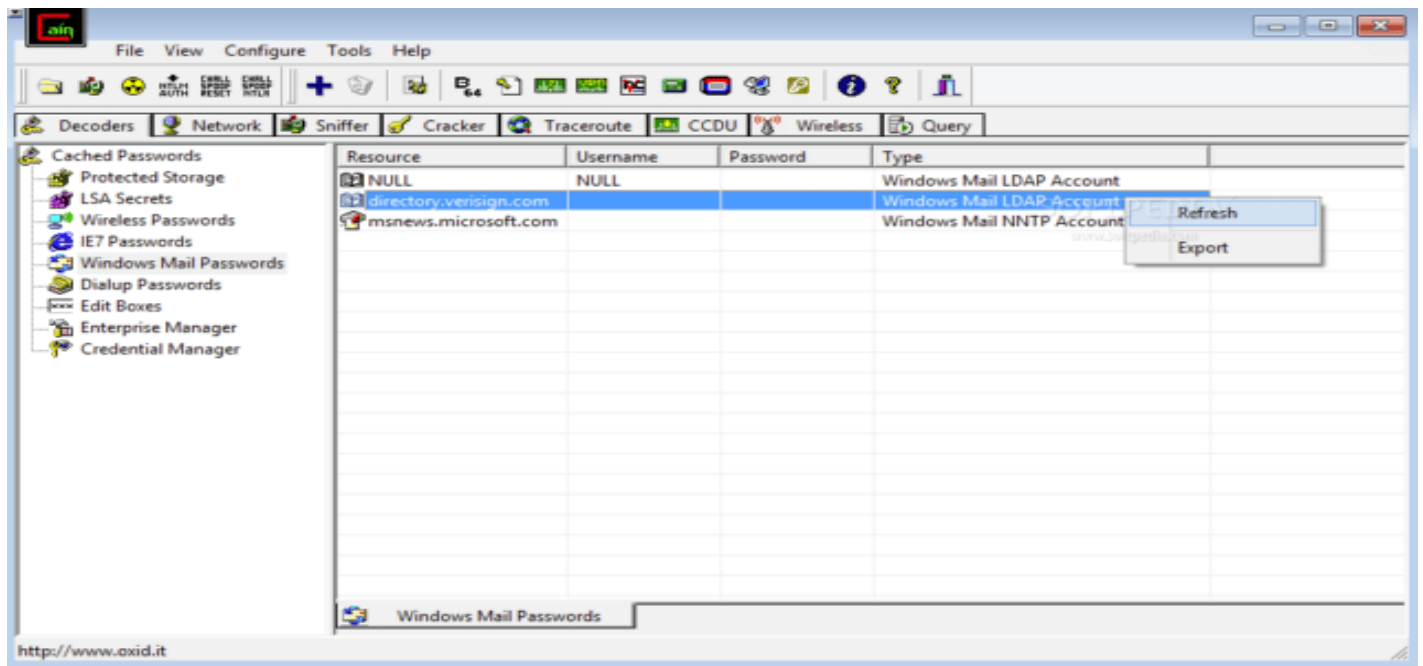
IP	Ping	Hostname	Ports [4+]	Web detect
195.80.116.170	18 ms	[n/a]	[n/a]	[n/a]
195.80.116.171	16 ms	[n/a]	443	[n/a]
195.80.116.172	38 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.173	36 ms	[n/a]	443	[n/a]
195.80.116.174	19 ms	[n/a]	80	[n/a]
195.80.116.175	22 ms	[n/a]	[n/a]	[n/a]
195.80.116.176	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.177	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.178	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.179	688 ms	[n/a]	80,443,8080	Apache/2.2.22 (Debian)
195.80.116.180	358 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.181	22 ms	[n/a]	80,443	Apache
195.80.116.182	18 ms	[n/a]	80	Apache/2.2.16 (Debian)
195.80.116.183	17 ms	[n/a]	443	[n/a]
195.80.116.184	22 ms	lists.eas.ee	80	Apache
195.80.116.185	20 ms	[n/a]	443	[n/a]
195.80.116.186	16 ms	[n/a]	80,443	[n/a]

Ready Display: All Threads: 0

SoftPerfect Network Scanner



Cain & Able



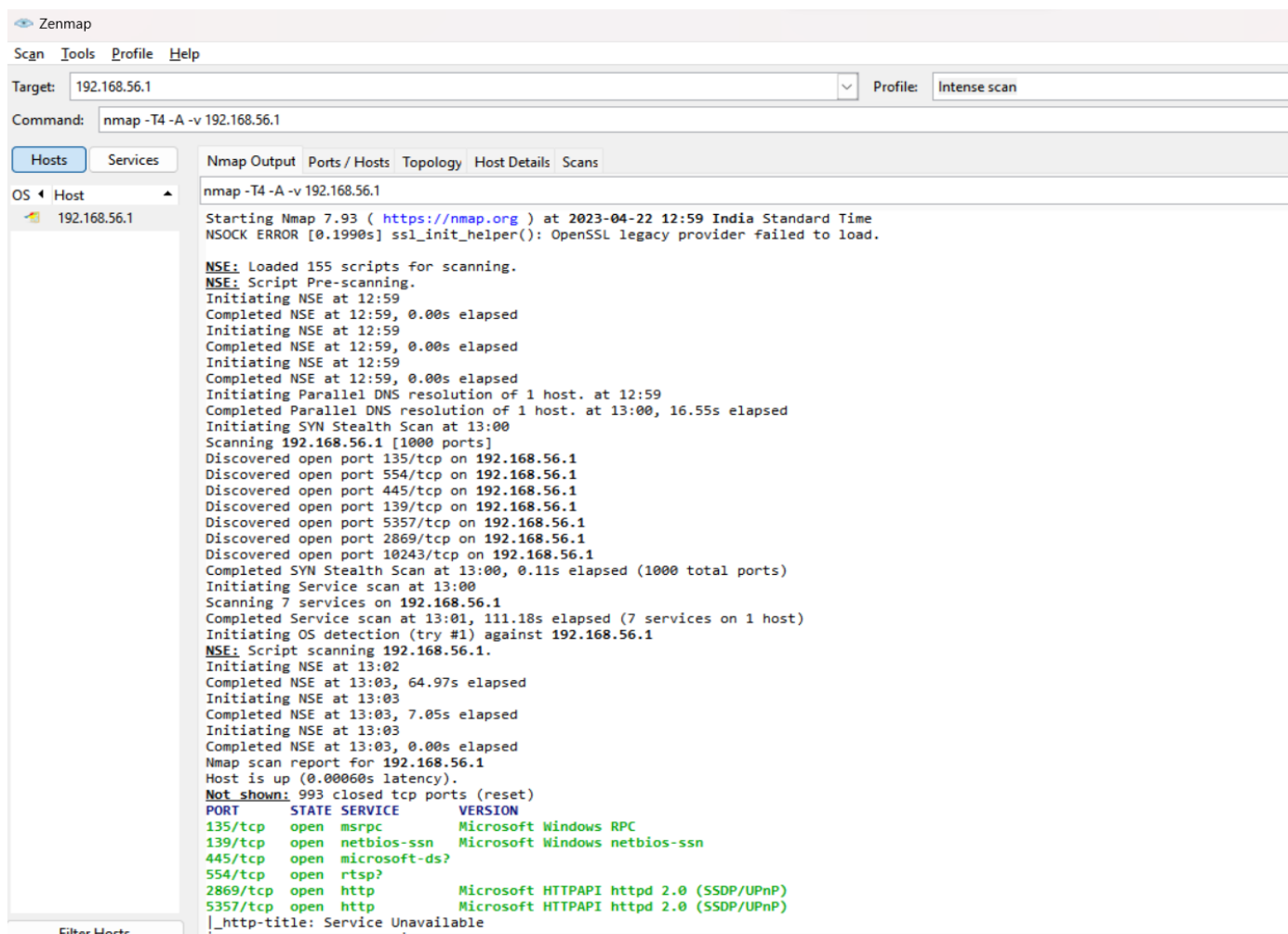
AIM: (2) Perform Network Scanning using NMAP in Windows and ZENMAP in kali Linux Software Based.

Description :

a) Performing Network Scanning using NMAP in Windows

Steps to run NMAP in Windows :

- 1 Download the Nmap installer
- 2 Install Nmap
- 3 Run the “Nmap – Zenmap” GUI program
- 4 Enter in the target for your scan
- 5 Choose your Profile
- 6 Click Scan to start scanning
- 7 Read your results



b) Performing ZENMAP in kali Linux Software Based

Steps and commands in Kali Linux :

Step 1: Download Zenmap

Commands: Sudo apt get install zenmap

Step 2: Download Alien

Commands:sudo apt install alien

Step 3: Convert to Debian format

Commands: sudo alien

Step 4: Installing Python 2

Commands: sudo apt install python2

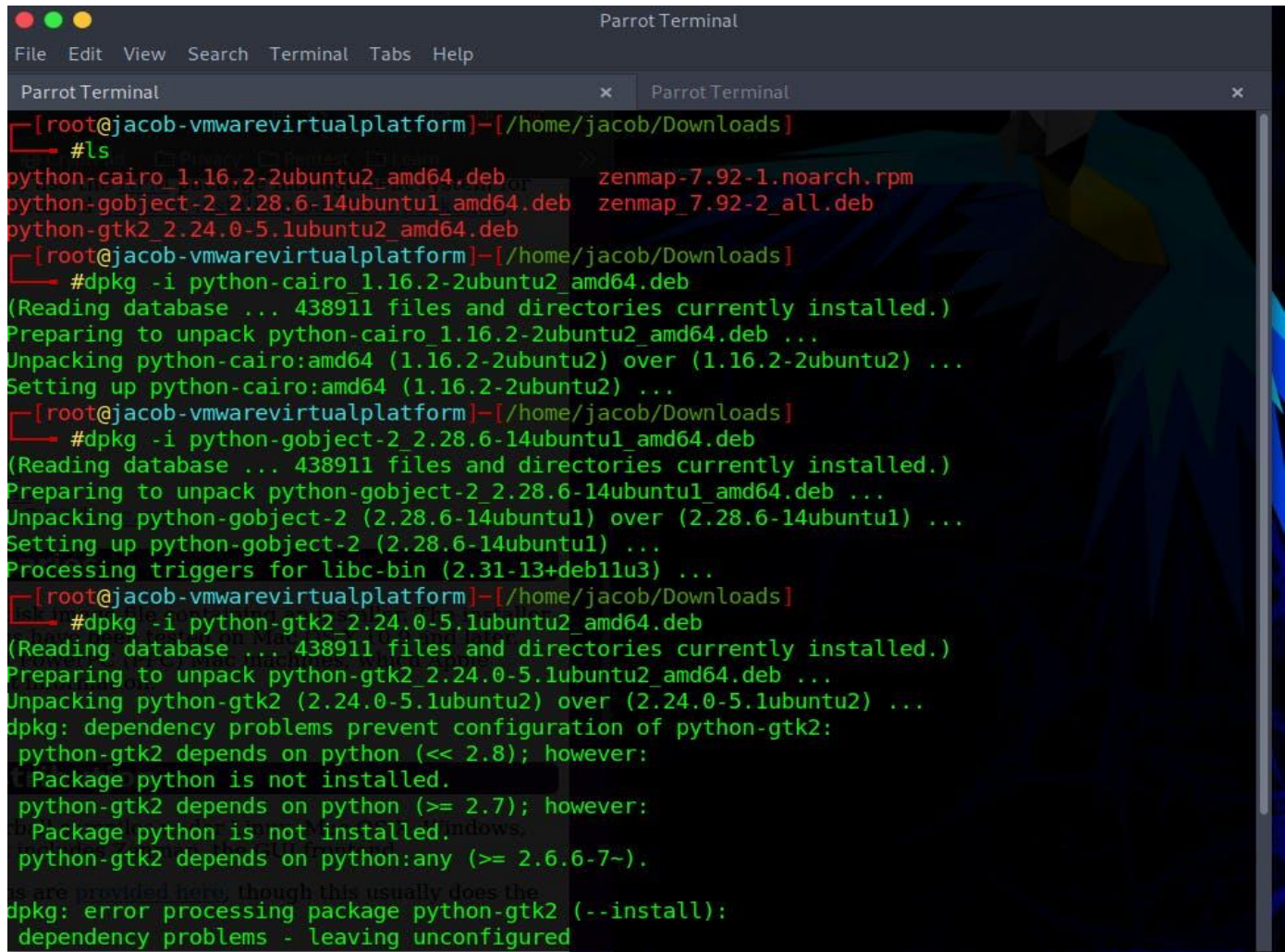
sudo open /usr/bin/env python2

Step 5: Download Dependencies

Commands:wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygtk/python-gtk2_2.24.0-5.1ubuntu2_amd64.deb

wget http://azure.archive.ubuntu.com/ubuntu/pool/universe/p/pygobject-2/python-gobject-2_2.28.6-14ubuntu1_amd64.deb

wget http://security.ubuntu.com/ubuntu/pool/universe/p/pycairo/python-cairo_1.16.2-2ubuntu2_amd64.deb



```
Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

[root@jacob-vmwarevirtualplatform]~/home/jacob/Downloads
#ls
python-cairo_1.16.2-2ubuntu2_amd64.deb      zenmap-7.92-1.noarch.rpm
python-gobject-2_2.28.6-14ubuntu1_amd64.deb  zenmap_7.92-2_all.deb
python-gtk2_2.24.0-5.1ubuntu2_amd64.deb

[root@jacob-vmwarevirtualplatform]~/home/jacob/Downloads
#dpkg -i python-cairo_1.16.2-2ubuntu2_amd64.deb
(Reading database ... 438911 files and directories currently installed.)
Preparing to unpack python-cairo_1.16.2-2ubuntu2_amd64.deb ...
Unpacking python-cairo:amd64 (1.16.2-2ubuntu2) over (1.16.2-2ubuntu2) ...
Setting up python-cairo:amd64 (1.16.2-2ubuntu2) ...

[root@jacob-vmwarevirtualplatform]~/home/jacob/Downloads
#dpkg -i python-gobject-2_2.28.6-14ubuntu1_amd64.deb
(Reading database ... 438911 files and directories currently installed.)
Preparing to unpack python-gobject-2_2.28.6-14ubuntu1_amd64.deb ...
Unpacking python-gobject-2 (2.28.6-14ubuntu1) over (2.28.6-14ubuntu1) ...
Setting up python-gobject-2 (2.28.6-14ubuntu1) ...
Processing triggers for libc-bin (2.31-13+deb11u3) ...

[root@jacob-vmwarevirtualplatform]~/home/jacob/Downloads
#dpkg -i python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
(Reading database ... 438911 files and directories currently installed.)
Preparing to unpack python-gtk2_2.24.0-5.1ubuntu2_amd64.deb ...
Unpacking python-gtk2 (2.24.0-5.1ubuntu2) over (2.24.0-5.1ubuntu2) ...
dpkg: dependency problems prevent configuration of python-gtk2:
 python-gtk2 depends on python (< 2.8); however:
  Package python is not installed.
 python-gtk2 depends on python (>= 2.7); however:
  Package python is not installed.
 python-gtk2 depends on python:any (>= 2.6.6-7~).
As alternatives,
 you can try to install one of these packages:
 python3.9, python3.8, python3.7, python3.6, python3.5, python3.4,
 python3.3, python3.2, python3.1, python3, python2.7, python2.6, python2.5,
 python2.4, python2.3, python2.2, python2.1, python2, python1.5, python1.4,
 python1.3, python1.2, python1.1.
dpkg: error processing package python-gtk2 (--install):
 dependency problems - leaving unconfigured
```

PROGRAM-4

(1) Install Wireshark and apply filters to gather different information.

(II) Find the link accessed by the victim using Wireshark.

AIM:

(1) Install Wireshark and apply filters to gather different information.

Description:

Wireshark is an open-source network protocol analysis software program, widely considered the industry standard. A global organization of network specialists and software developers supports Wireshark and continues to make updates for new network technologies and encryption methods.

Government agencies, corporations, non-profits, and educational institutions use Wireshark for troubleshooting and teaching purposes. There truly isn't a better way to learn low-level networking than to look at traffic under the Wireshark microscope.

You should only use Wireshark on networks where you have permission to inspect network packets. Using Wireshark to look at packets without permission is illegal.

Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.

How to download and install Wireshark

Downloading and installing Wireshark is easy. Step one is to check the official Wireshark download page for the operating system you need. The installation is simple, and the basic version of Wireshark is free.

Wireshark for Windows

Wireshark comes in two options for Windows: 32-bit and 64-bit. Pick the correct version for your OS; the current release is 3.0.3 as of this writing.

Wireshark for Mac

Wireshark is available on Mac as a Homebrew install.

To install Homebrew, you need to run this command at your Terminal prompt:

```
/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

Once you have the Homebrew system in place, you can access several open-source projects for your Mac. To install Wireshark, run this command from the Terminal:

Capturing data packets on Wireshark

- 1) When you open Wireshark, you see a screen showing you a list of all the network connections you can monitor. You also have a capture filter field to only capture the network traffic you want to see.
- 2) Click the first button on the toolbar, titled "Start capturing packets."
- 3) You can select the menu item Capture -> Start.
- 4) Once you have captured all the packets needed, use the same buttons or menu options to stop the capture as you did to begin.

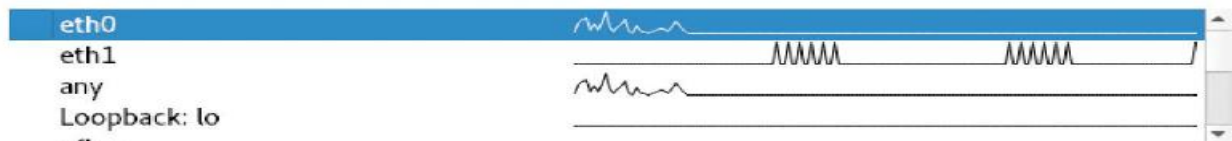


Welcome to Wireshark

Capture

...using this filter:

All interfaces shown ▾



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

Ready to load or capture No Packets Profile: Default

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
2345	11.159311	192.168.0.188	109.115.78.24	TCP	66	[TCP Dup ACK 2288#15] 36074 → 8080 [ACK] Seq=1 Ack=911316 Win=1032 Len=0 SLE=912768 SRE=934548
2346	11.169701	46.14.231.181	192.168.0.188	TCP	1514	8888 → 36078 [ACK] Seq=865058 Ack=1 Win=3456 Len=1460
2347	11.169935	192.168.0.188	46.14.231.181	TCP	66	[TCP Dup ACK 2339#3] 36078 → 8888 [ACK] Seq=1 Ack=853378 Win=1026 Len=0 SLE=856298 SRE=866518
2348	11.171760	46.14.231.181	192.168.0.188	TCP	1514	8888 → 36078 [ACK] Seq=866518 Ack=1 Win=3456 Len=1460
2349	11.171760	109.115.78.24	192.168.0.188	TCP	1506	8080 → 36074 [ACK] Seq=934548 Ack=1 Win=1025 Len=1452
2350	11.171760	109.115.78.24	192.168.0.188	TCP	1506	8080 → 36074 [ACK] Seq=936000 Ack=1 Win=1025 Len=1452
2351	11.171760	109.115.78.24	192.168.0.188	TCP	1506	[TCP Fast Retransmission] 8080 → 36074 [ACK] Seq=911316 Ack=1 Win=1025 Len=1452
2352	11.171986	192.168.0.188	46.14.231.181	TCP	66	[TCP Dup ACK 2339#4] 36078 → 8888 [ACK] Seq=1 Ack=853378 Win=1026 Len=0 SLE=856298 SRE=867978
2353	11.172077	192.168.0.188	109.115.78.24	TCP	66	[TCP Dup ACK 2288#16] 36074 → 8080 [ACK] Seq=1 Ack=911316 Win=1032 Len=0 SLE=912768 SRE=936000
2354	11.172128	192.168.0.188	109.115.78.24	TCP	66	[TCP Dup ACK 2288#17] 36074 → 8080 [ACK] Seq=1 Ack=911316 Win=1032 Len=0 SLE=912768 SRE=937452
2355	11.172232	192.168.0.188	109.115.78.24	TCP	54	36074 → 8080 [ACK] Seq=1 Ack=937452 Win=1032 Len=0
2356	11.172533	109.115.78.24	192.168.0.188	TCP	1506	8080 → 36074 [ACK] Seq=937452 Ack=1 Win=1025 Len=1452
2357	11.210847	46.14.203.136	192.168.0.188	TCP	1514	8080 → 36077 [ACK] Seq=147461 Ack=1 Win=432 Len=1460
2358	11.210847	46.14.231.181	192.168.0.188	TCP	1514	[TCP Retransmission] 8888 → 36078 [ACK] Seq=853378 Ack=1 Win=3456 Len=1460
2359	11.211303	192.168.0.188	46.14.231.181	TCP	66	36078 → 8888 [ACK] Seq=1 Ack=854838 Win=1026 Len=0 SLE=856298 SRE=867978
2360	11.226263	192.168.0.188	109.115.78.24	TCP	54	36074 → 8080 [ACK] Seq=1 Ack=938904 Win=1032 Len=0
2361	11.229279	46.14.203.136	192.168.0.188	TCP	1514	8080 → 36077 [ACK] Seq=148921 Ack=1 Win=432 Len=1460
2362	11.229571	192.168.0.188	46.14.203.136	TCP	54	36077 → 8080 [ACK] Seq=1 Ack=150381 Win=513 Len=0
2363	11.272706	109.115.78.24	192.168.0.188	TCP	1506	8080 → 36074 [ACK] Seq=938904 Ack=1 Win=1025 Len=1452

> Frame 1: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF...
> Ethernet II, Src: D-Linkin_66:f2:6b (e0:1c:fc:66:f2:6b), Dst: IntelCor_fe:5d:df (f0:77:c3:fe:5d:df)
> Internet Protocol Version 4, Src: 109.115.78.24, Dst: 192.168.0.188
▼ Transmission Control Protocol, Src Port: 8080, Dst Port: 36074, Seq: 1, Ack: 1, Len: 1452
 Source Port: 8080
 Destination Port: 36074
 [Stream index: 0]
 [Conversation completeness: Incomplete (12)]
 [TCP Segment Len: 1452]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 2859886249
 [Next Sequence Number: 1453 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 797112921
 0101 = Header Length: 20 bytes (5)
 > Flags: 0x010 (ACK)
 Window: 1025
 [Calculated window size: 1025]
 [Window size scaling factor: -1 (unknown)]

0000 f0 77 c3 fe 5d df e0 1c fd 66 f2 6b 08 00 45 00 ...w...f.k.E-
0010 05 d4 1e 0e 40 00 6c 06 6e 26 6d 73 4e 18 c0 a8 ...@.l.n&msN...
0020 00 bc 1f 90 8c ea aa 76 66 a9 2f 82 fa 59 50 10 ...v f./..YP-
0030 04 01 94 81 00 00 e5 cb ee c4 98 c6 52 f7 a4 33 ...R...3
0040 54 db 05 85 ad b6 ed cd bb 73 6d ac ad 05 2d cb T.....sm....
0050 b3 cf b5 fe f2 2f f0 d4 35 52 34 87 c2 0d 4c 7f .../...SR4...L
0060 f5 b2 ff 00 75 5d 95 7f dd 5a 56 6d ab b9 a9 89 ...u]...ZVm...
0070 f3 22 b3 7d e6 f9 b7 7f 7a ae 33 97 28 72 fb c3 Y...j...6.T]...n'
0080 59 15 bf 85 6a 17 81 36 ee 54 5d df dd a9 6e 27 ...-j...-j]...n'
0090 4b 68 9a 49 5b 68 aa af 2c 9e 43 c9 2a 2c 49 b7 Kh.I[h...C.*.I
00a0 e5 dc df 35 54 67 3f 84 25 08 82 5d 4b 13 37 93 ...5Tg?..%..]K.7
00b0 77 71 17 fb ae cb 56 22 d6 f5 78 be e6 a0 ed fe wq...V...x....
00c0 fa ab 56 33 cf 76 db 76 c4 8a ab fd f6 f9 9a 9a ...V3.v.v...
00d0 b7 9b 5d 52 75 68 9d be ee e6 f9 5b fe 05 57 cd ...Ruh...[...W
00e0 12 79 4d 9b 9f 12 6a ed 67 2a 4f 2c 4c 8e 8c ad yM...j g*O.L...
00f0 fb ad ad b6 b2 3c 3d 2a d8 e9 de 6f f1 cf ff 00 ...<e*...o...
0100 8e aa fd da 6d f4 ed f6 29 57 77 de 5d ba 36 e5 ...m...w]w]-6-
0110 55 ff 00 76 a6 fe f7 30 7c 43 f5 08 ae 75 18 6e U...v...0[C...u-n
0120 27 b4 b5 79 7e ca 9b a5 f2 97 73 2a ff 00 bb f7 '.yow...s*...
0130 9b f8 ab 09 16 46 81 65 64 65 56 5d db 59 6b b2 ...F.e dev].Yk-
0140 d1 ee 5b 45 b0 b8 d4 d5 76 dc 33 2d ba 44 df 75 ...[E...v.3-.D u
0150 db ef 7c df dd db ba b9 fb db c9 6f af 26 b9 99o.&...

Wi-Fi: <live capture in progress> Packets: 2459 · Displayed: 2459 (100.0%)

AIM:

(II) Find the link accessed by the victim using Wireshark.

Description:**Using Wireshark to get the IP address of an Unknown Host**

Wireshark is a powerful tool that can analyze traffic between hosts on your network. But it can also be used to help you discover and monitor unknown hosts, pull their IP addresses, and even learn a little about the device itself. Here's how I use Wireshark to find the IP address of an unknown host on my LAN.

What are Wireshark and IP Addresses?

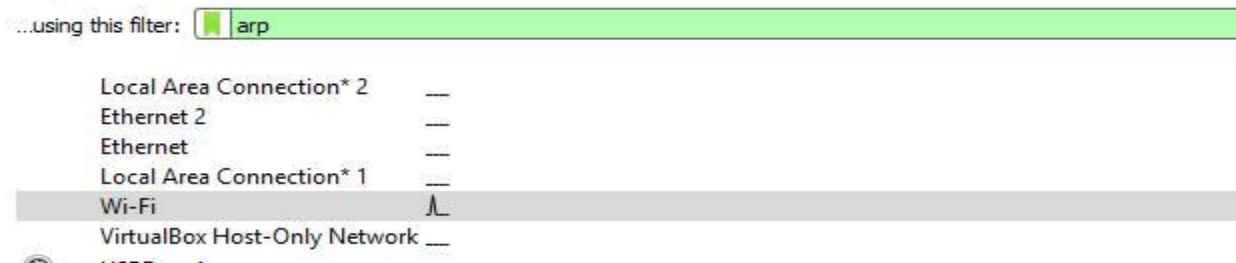
Wireshark is a network monitor and analyzer. It works below the packet level, capturing individual frames and presenting them to the user for inspection. Using Wireshark, you can watch network traffic in real-time, and look inside to see what data is moving across the wire.

An IP address is a unique identifier used to route traffic on the network layer of the OSI model. If you think of your local network as a neighborhood, a network address is analogous to a house number. When you know the IP address of a host, it's possible to access and interact with it.

Finding an IP address with Wireshark using ARP requests

Address Resolution Protocol (ARP) requests can be used by Wireshark to get the IP address of an unknown host on your network. ARP is a broadcast request that's meant to help the client machine map out the entire host network.

ARP is slightly more foolproof than using a DHCP request – which I'll cover below – because even hosts with a static IP address will generate ARP traffic upon startup.

Capture

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_2b:ca:e6	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.181
2	13.727047	Apple_a5:19:b6	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.182 (Request)
3	13.926147	Apple_a5:19:b6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.182
4	15.052525	Apple_a5:19:b6	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.182 (Request)
5	15.359676	Apple_a5:19:b6	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.182
6	35.954122	Azurewav_44:ec:bc	BelkinIn_2a:4a:47	ARP	42	Who has 192.168.1.1? Tell 192.168.1.219
7	35.955304	BelkinIn_2a:4a:47	Azurewav_44:ec:bc	ARP	42	192.168.1.1 is at 14:91:82:2a:4a:47
8	50.073270	IntelCor_2b:ca:e6	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.181
9	82.328786	BelkinIn_2a:4a:47	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1

To pull an IP address of an unknown host via ARP, start Wireshark and begin a session with the Wireshark capture filter set to arp, as shown above.

▼ Address Resolution Protocol (request/gratuitous ARP)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
[Is gratuitous: True]	
Sender MAC address: Apple_a5:19:b6 (54:33:cb:a5:19:b6)	
Sender IP address: 192.168.1.182	
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.1.182	

Once you've spotted the request, click on it. Use Wireshark's Packet details view to analyze the frame. Look at the Address resolution protocol section of the frame, especially the Sender IP address and Sender MAC address.

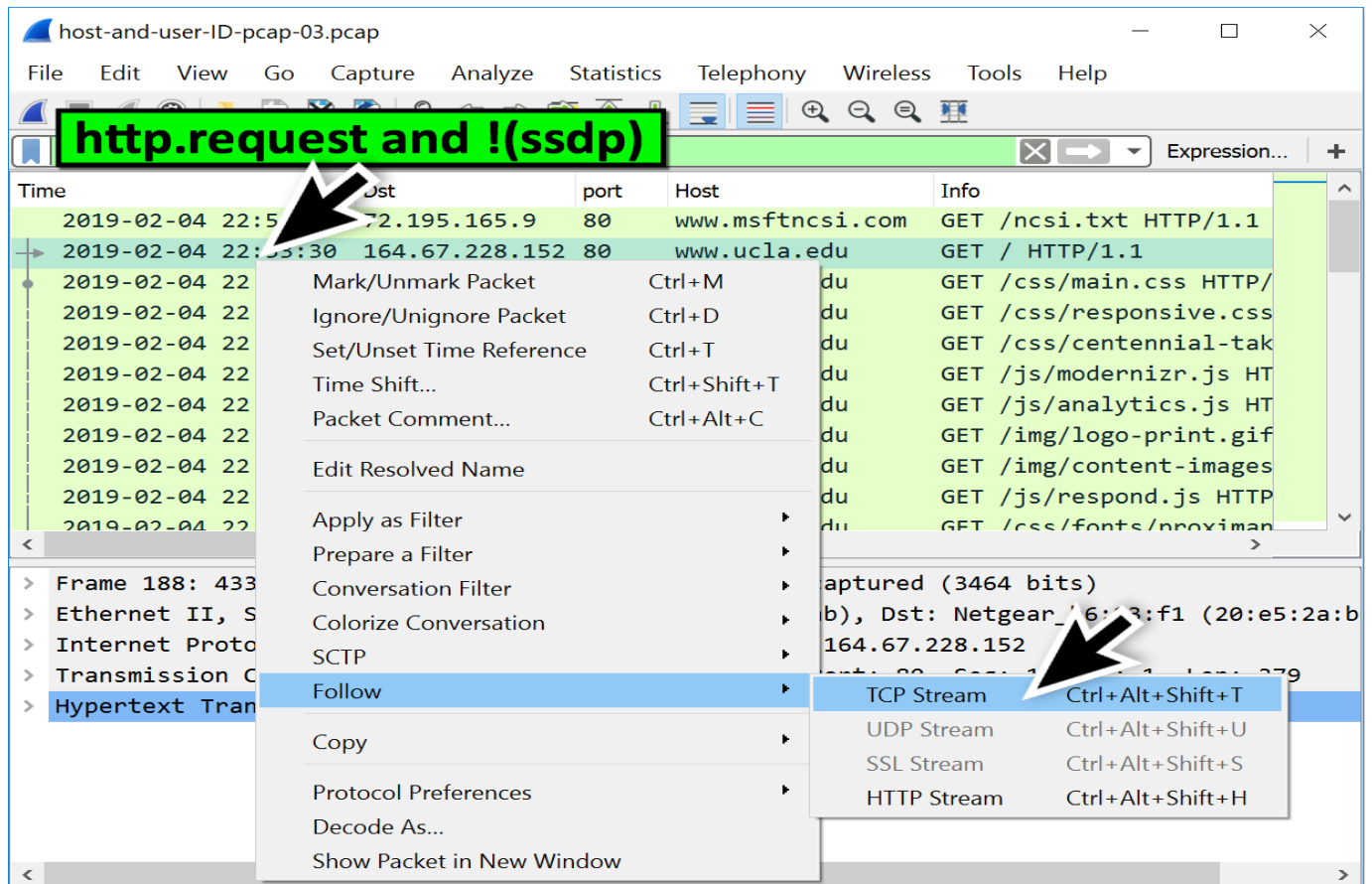
In this case, you can see my phone received an IP address of 192.168.1.182 from the router, and you can identify the device as an Apple phone by looking at the vendor OUI.

Device Models and Operating Systems from HTTP Traffic

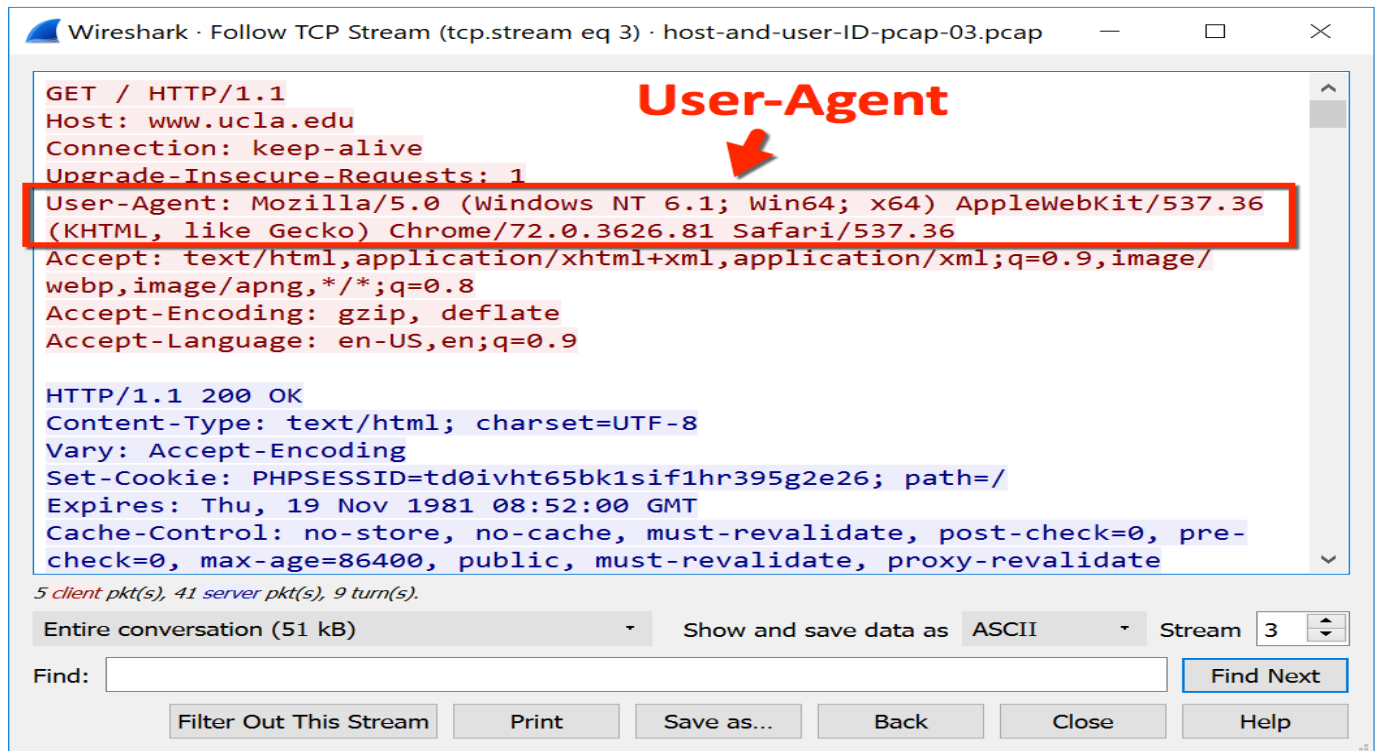
User-agent strings from headers in HTTP traffic can reveal the operating system. If the HTTP traffic is from an Android device, you might also determine the manufacturer and model of the device.

The third pcap for this tutorial, host-and-user-ID-pcap-03.pcap, is available here. This pcap is from a Windows host using an internal IP address at 192.168.1.[.]97.

Open the pcap in Wireshark and filter on http.request and !(ssdp). Select the second frame, which is the first HTTP request to www.ucla[.]edu, and follow the TCP stream as shown in Figure



This TCP stream has HTTP request headers as shown in Figure 8. The User-Agent line represents Google Chrome web browser version 72.0.3626[.]81 running on Microsoft's Windows 7 x64 operating system.



PROGRAM 5

Perform Session hijacking/ find credentials of unsecured real-time websites using Wireshark.

AIM :

Perform Session hijacking/ find credentials of unsecured real-time websites using Wireshark.

Description:

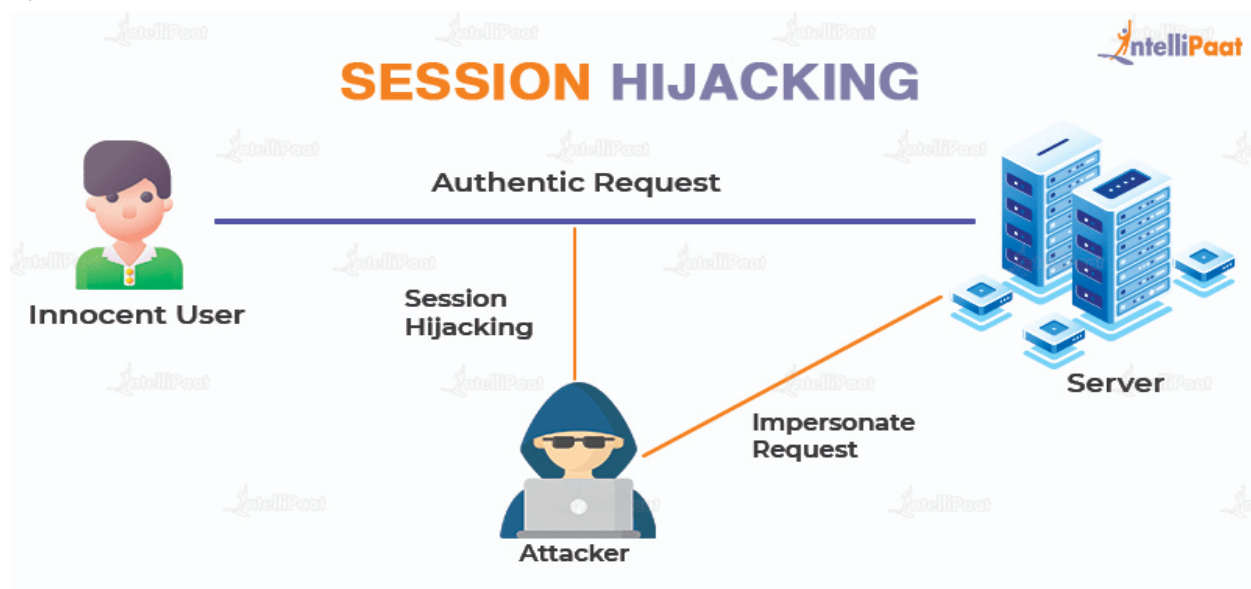
Session Hijacking

Session hijacking stands for a cyberattack where a malicious hacker places himself in between your computer and the website's server while you are engaged in an active computer session (the time between you first log into your bank account, and then log off after your operation, for example) in order to steal it. The hacker actively monitors everything that happens on your account, and can even kick you out and take control of it. It is often called cookie hijacking or cookie side-jacking because the hacker gains knowledge of your session cookie giving him access to the session ID that lets him impersonate the user and perform actions on his behalf: transferring your money to his account for instance.

Session Hijacking Types

- 1) Cross-Site Scripting (XSS) or Misdirected Trust
- 2) Session side-jacking
- 3) Session fixation

- 4) Malware infections
- 5) Brute-forcing the Session ID
- 6) Man-in-the-Browser



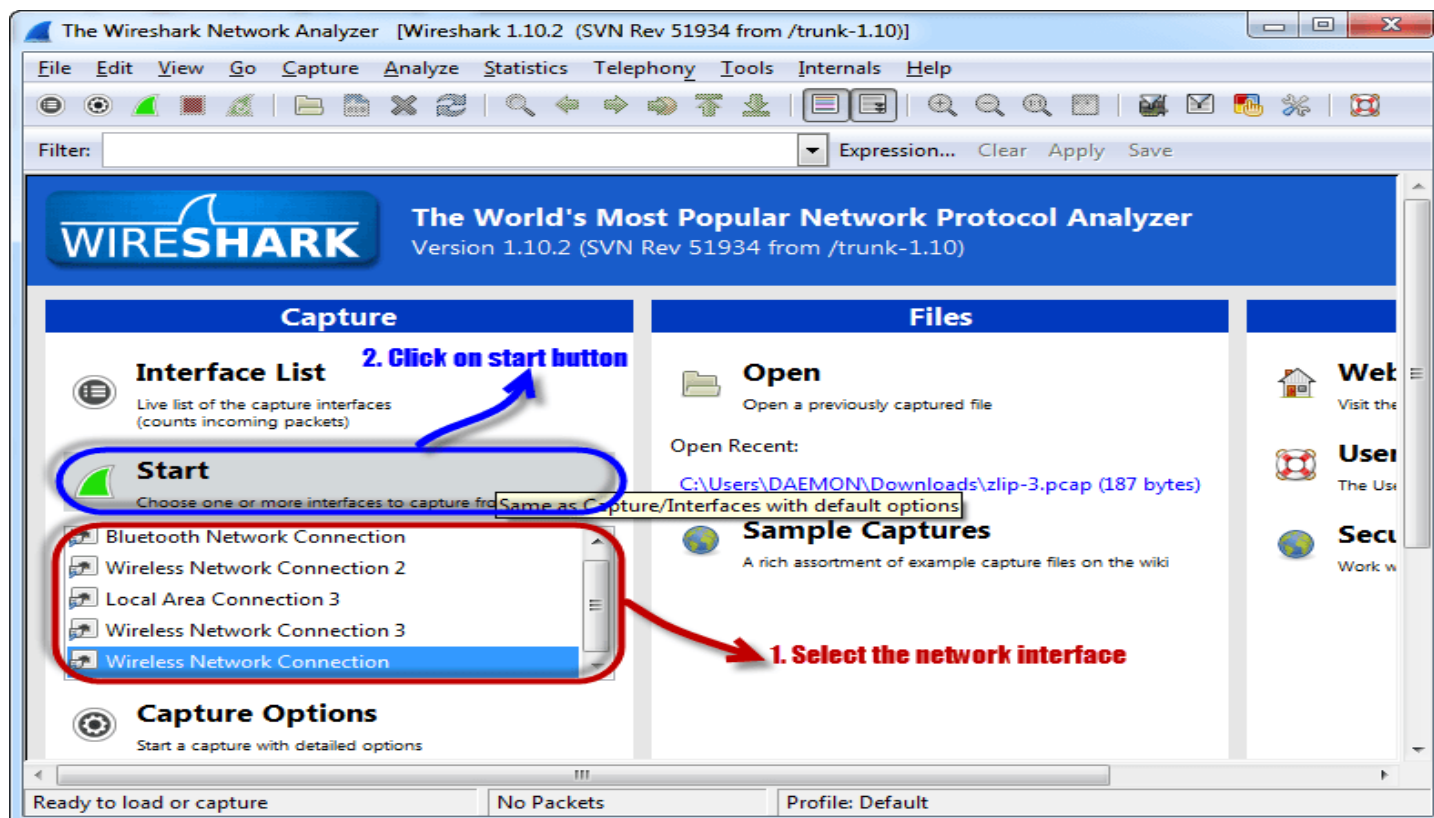
Session hijacking/ find credentials of unsecured real-time websites using Wireshark

Sniffing the network using Wireshark

The illustration below shows you the steps that you will carry out to complete this exercise without confusion

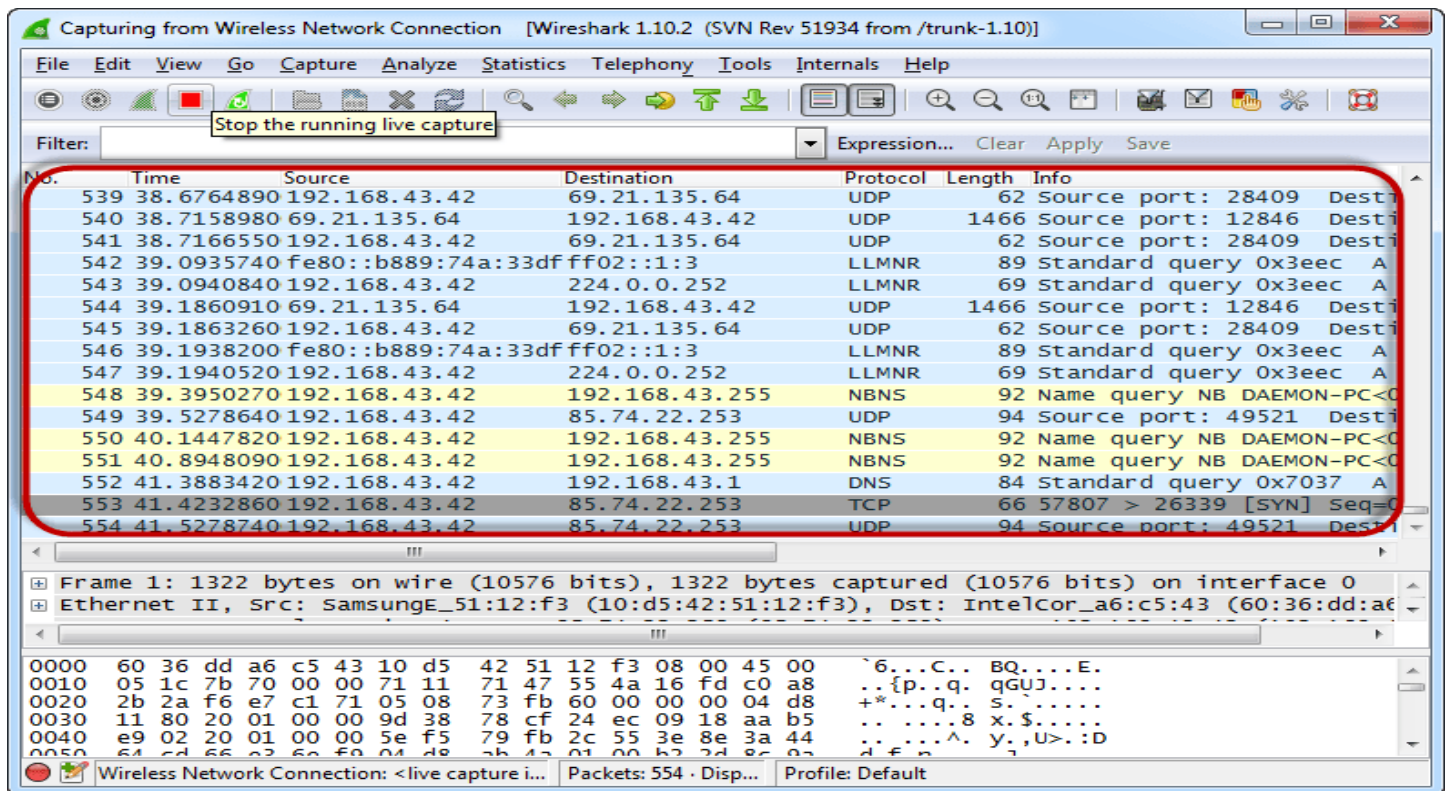
Download Wireshark from this link <http://www.wireshark.org/download.html>

1) Open Wireshark

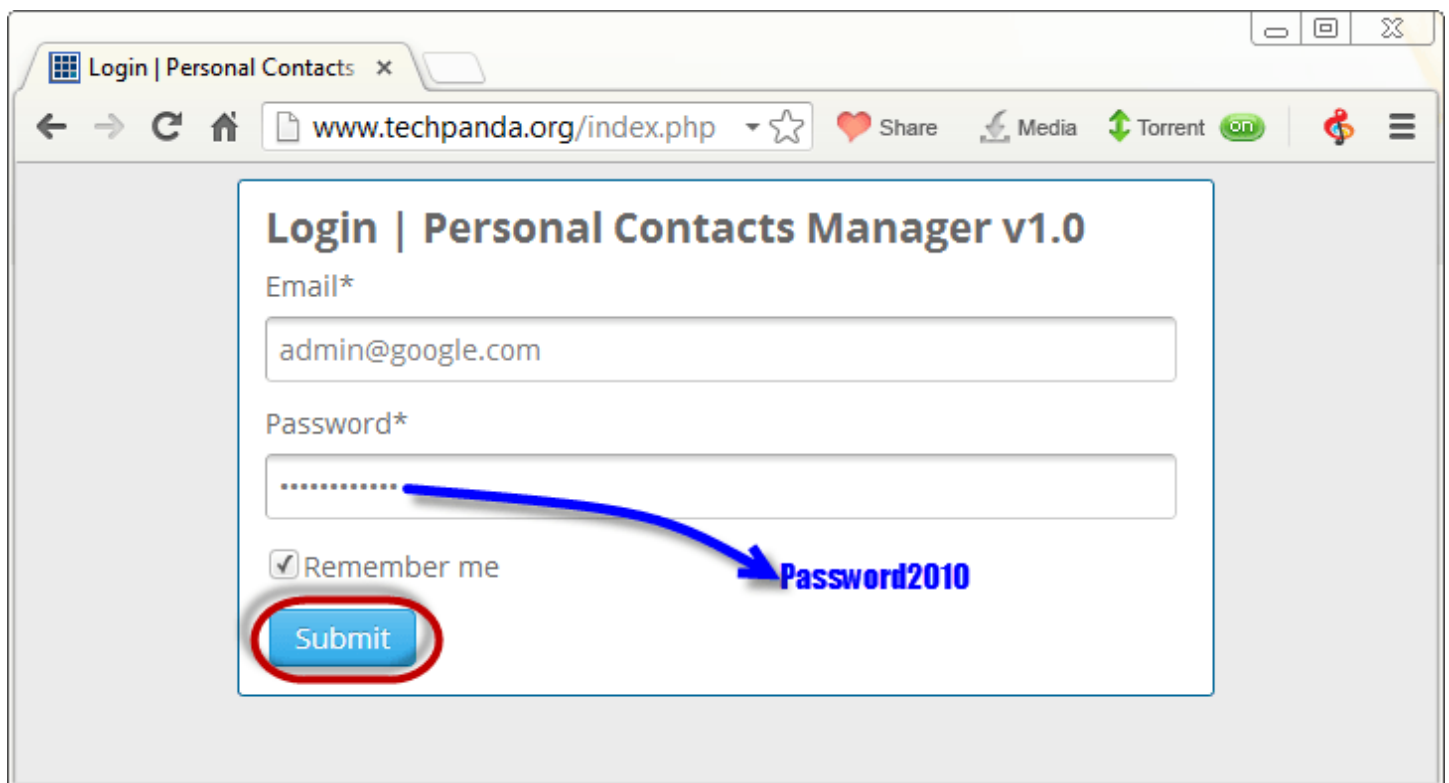


2) Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.

Click on start button as shown above



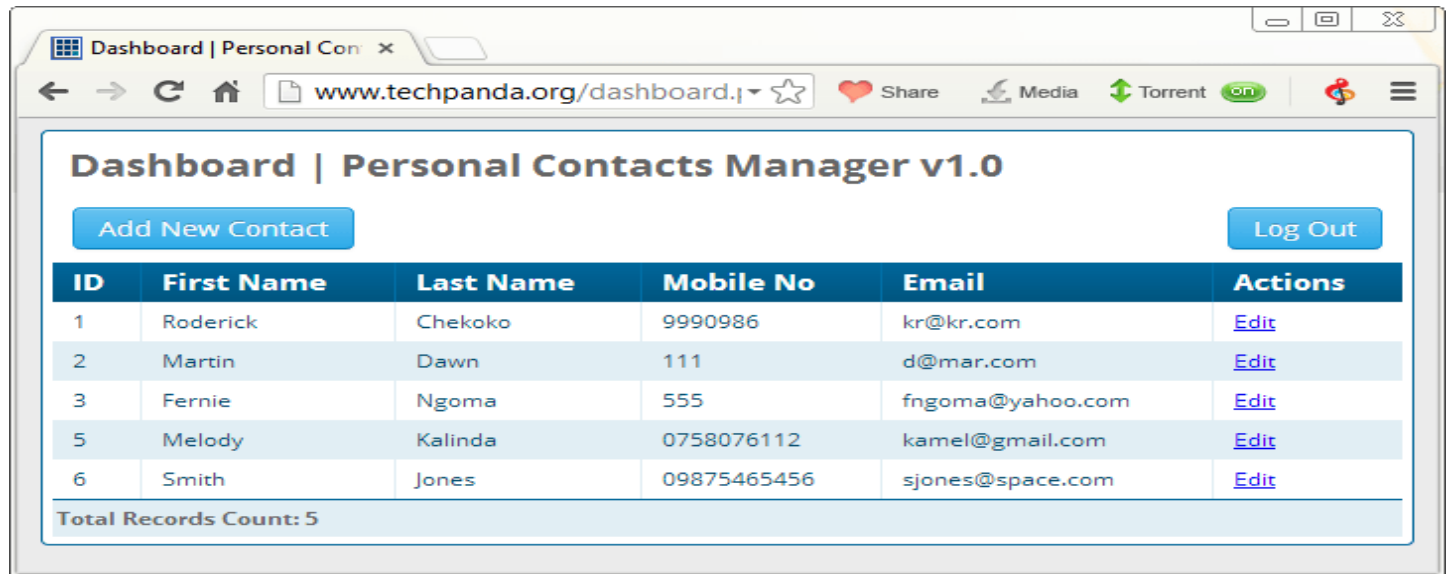
3) Open your web browser and type in <http://www.techpanda.org/>



4) The login email is admin@google.com and the password is Password2010

Click on submit button

A successful logon should give you the following dashboard

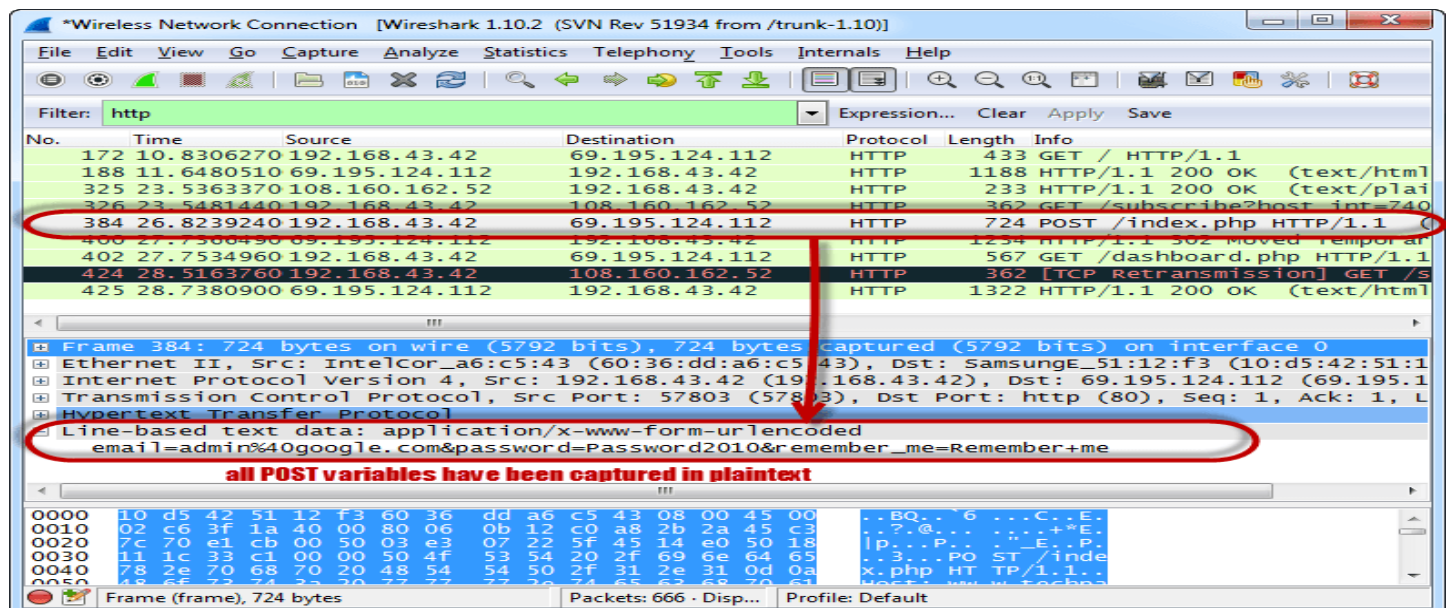


5) Go back to Wireshark and stop the live capture

Filter for HTTP protocol results only using the filter textbox

Locate the Info column and look for entries with the HTTP verb POST and click on it

Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded.



You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

PROGRAM 6:

Use the Nessus tool to find all the vulnerabilities with its level and generate a report for an organization

AIM:

Use the Nessus tool to find all the vulnerabilities with its level and generate a report for an organization

DESCRIPTION:

Nessus

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Vulnerability scanning with Nessus

Nessus performs its scans by utilizing plugins, which run against each host on the network in order to identify vulnerabilities. Plugins can be thought of as individual pieces of code that Nessus uses to conduct individual scan types on targets. Plugins are numerous and wide in their capabilities. For instance, a plugin could be launched and targeted at a host to:

- 1) Identify which operating systems and services are running on which ports
- 2) Identify which software components are vulnerable to attacks (FTP, SSH, SMB and more)
- 3) Identify if compliance requirements are met on various hosts



When you launch a scan, Nessus goes through a series of steps.

Step 1: Nessus will retrieve the scan settings. The settings will define the ports to be scanned, the plugins to be enabled and policy preferences definitions.

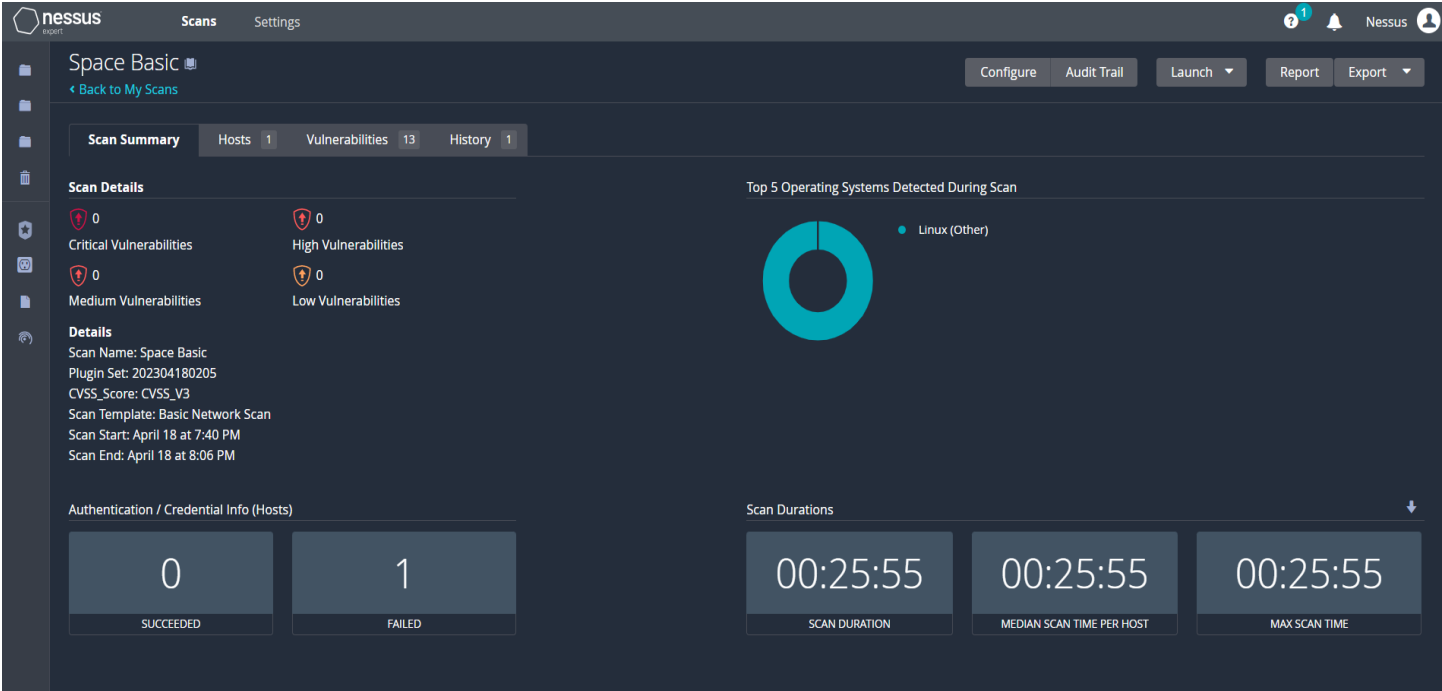
Step 2: Nessus will then perform host discovery to determine the hosts that are up. The protocols used in host discovery will be ICMP, TCP, UDP and ARP. You can specify these per your desires.

Step 3: Nessus then performs a port scan of each host that is discovered to be up. You can also define which ports you will want to be scanned. Ports can be defined in ranges or individually, with valid ports ranging from 1 to 65535.

Step 4: Nessus will then perform service detection to determine the services that are running behind each port on each host discovered

Step 5: Nessus then performs operating system detection.

Step 6: Once all the steps are complete, Nessus runs each host against a database of known vulnerabilities in an attempt to discover which host contains which vulnerabilities.



The screenshot shows the 'Vulnerabilities' tab in the Nessus dashboard. It displays a table of 13 vulnerabilities found during the scan. The table has columns for severity, CVSS score, VPR, name, family, and count. To the right of the table, there is a 'Scan Details' sidebar showing policy, status, severity base, scanner, start/end times, and elapsed time. Below that is a 'Vulnerabilities' sidebar with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	CVSS	VPR	Name	Family	Count
INFO			HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO			Nessus SYN scanner	Port scanners	2
INFO			Service Detection	Service detection	2
INFO			Asset Attribute: Fully Qualified Domain Name (FQDN)	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO			Nessus Scan Information	Settings	1
INFO			OS Identification	General	1
INFO			Service Detection (HELP Request)	Service detection	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Hosts 1 Vulnerabilities 66 Remediations 2 History 1

Filter Search Vulnerabilities 66 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1		
<input type="checkbox"/>	CRITICAL	MS17-010: Security Update f...	Windows	1		
<input type="checkbox"/>	HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1		
<input type="checkbox"/>	HIGH	Jenkins < 2.138.4 LTS / 2.150...	CGI abuses	1		
<input type="checkbox"/>	HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1		
<input type="checkbox"/>	HIGH	MS12-020: Vulnerabilities in ...	Windows	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	Microsoft Windows Remote ...	Windows	1		

Scan Details

Name: Basic Network
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: February 25 at 9:03 AM
End: February 25 at 9:07 AM
Elapsed: 4 minutes

Vulnerabilities



Program 7

- (1) Execute basic commands of Linux.
- (ii) Use CHMOD command to change the privileges & permissions

AIM:

- (1) Execute basic commands of Linux.

DESCRIPTION:

A Linux command is a program or utility that runs on the command line. A command line is an interface that accepts lines of text and processes them into instructions for your computer.

Any graphical user interface (GUI) is just an abstraction of command-line programs. For example, when you close a window by clicking on the “X,” there’s a command running behind that action.

A flag is a way we can pass options to the command you run. Most Linux commands have a help page that we can call with the flag -h. Most of the time, flags are optional.

An argument or parameter is the input we give to a command so it can run properly. In most cases, the argument is a file path, but it can be anything you type in the terminal.

You can invoke flags using hyphens (-) and double hyphens (--), while argument execution depends on the order in which you pass them to the function.

COMMANDS:

1. ls Command

ls is probably the first command every Linux user typed in their terminal. It allows you to list the contents of the directory you want (the current directory by default), including files and other nested directories.

2. alias Command

The alias command lets you define temporary aliases in your shell session. When creating an alias, you instruct your shell to replace a word with a series of commands.

3. unalias Command

As the name suggests, the unalias command aims to remove an alias from the already defined aliases. To remove the previous ls alias.

4. pwd Command

The pwd command stands for “print working directory,” and it outputs the absolute path of the directory you’re in. For example, if your username is “john” and you’re in your Documents directory, its absolute path would be: /home/john/Documents.

5. cd Command

The cd command is highly popular, along with ls. It refers to “change directory” and, as its name suggests, switches you to the directory you’re trying to access.

6. cp Command

It’s so easy to copy files and folders directly in the Linux terminal that sometimes it can replace conventional file managers.

7. rm Command

Now that you know how to copy files, it'll be helpful to know how to remove them.

8. mv Command

You use the mv command to move (or rename) files and directories through your file system.

9. mkdir Command

To create folders in the shell, you use the mkdir command. Just specify the new folder's name, ensure it doesn't exist, and you're ready to go.

10. man Command

Another essential Linux command is man. It displays the manual page of any other command (as long as it has one).

11. touch Command

The touch command allows you to update the access and modification times of the specified files.

12. chmod Command

The chmod command lets you change the mode of a file (permissions) quickly. It has a lot of options available with it.

The basic permissions a file can have are:

r (read)

w (write)

x (execute)

13. ./ Command

Maybe the ./ notation isn't a command itself, but it's worth mentioning in this list. It lets your shell run an executable file with any interpreter installed in your system directly from the terminal.

14. exit Command

The exit command does exactly what its name suggests: With it, you can end a shell session and, in most cases, automatically close the terminal you're using:

15. sudo Command

This command stands for "superuser do," and it lets you act as a superuser or root user while you're running a specific command. It's how Linux protects itself and prevents users from accidentally modifying the machine's filesystem or installing inappropriate packages.

16. shutdown Command

As you may guess, the shutdown command lets you power off your machine. However, it also can be used to halt and reboot it.

17. ping Command

ping is the most popular networking terminal utility used to test network connectivity. ping has a ton of options, but in most cases, you'll use it to request a domain or IP address

18. history Command

If you're struggling to remember a command, history comes in handy. This command displays an enumerated list with the commands you've used in the past:

19. passwd Command

passwd allows you to change the passwords of user accounts. First, it prompts you to enter your current password, then asks you for a new password and confirmation.

20. whoami Command

The whoami command (short for “who am i”) displays the username currently in use

1.is	1.clear	1.diff	1.kill and killall	1.apt, pacman, yum, rpm
2.pwd	2.echo	2.cmp	2.df	2.sudo
3.cd	3.less	3.comm	3.mount	3.cal
4.mkdir	4.man	4.sort	4.chmod	4.alias
5.mv	5.unman	5.export	5.chown	5.dd
6.cp	6.whoami	6.zip	6.ifconfig	6.whereis
7.rm	7.tar	7.unzip	7.traceroute	7.whatis
8.touch	8.grep	8.ssh	8.wget	8.top
9.in	9.head	9.service	9.ufw	9. useradd
10.cat	10.tail	10.ps	10.iptables	10.passwd

AIM:

(ii) Use CHMOD command to change the privileges & permissions

Description:

Using Linux as your operating system allows you to easily provide access to many users simultaneously. However, that access also presents potential security risks. Understanding the variety and types of Linux file permissions for users and groups will ensure that your system is optimally secure.

Changing directory permissions in Linux

To change directory permissions in Linux, use the following:

chmod +rwx filename to add permissions

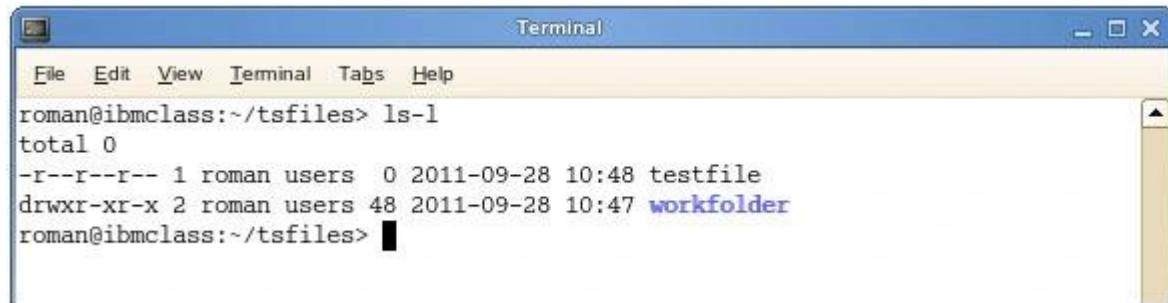
chmod -rwx directory name to remove permissions.

chmod +x filename to allow executable permissions.

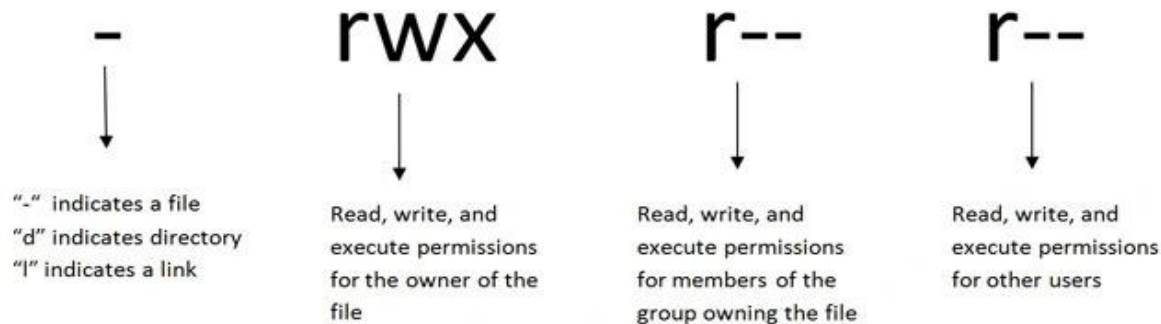
chmod -wx filename to take out write and executable permissions.

Note that “r” is for read, “w” is for write, and “x” is for execute.

This only changes the permissions for the owner of the file.



```
roman@ibmclass:~/tsfiles> ls-l
total 0
-r--r--r-- 1 roman users 0 2011-09-28 10:48 testfile
drwxr-xr-x 2 roman users 48 2011-09-28 10:47 workfolder
roman@ibmclass:~/tsfiles>
```



The three permission groups

There are three options for permission groups available to you in Linux. These are

owners: these permissions will only apply to owners and will not affect other groups.

groups: you can assign a group of users specific permissions, which will only impact users within the group.

all users: these permissions will apply to all users, and as a result, they present the greatest security risk and should be assigned with caution.

Three kinds of file permissions in Linux

There are three kinds of file permissions in Linux:

Read (r): Allows a user or group to view a file.

Write (w): Permits the user to write or modify a file or directory.

Execute (x): A user or group with execute permissions can execute a file or view a directory.

How to Change Directory Permissions in Linux for the Group Owners and Others

The command for changing directory permissions for group owners is similar, but add a "g" for group or "o" for users:

- `chmod g+w filename`
- `chmod g-wx filename`
- `chmod o+w filename`

- `chmod o-rwx foldername`

To change directory permissions for everyone, use “u” for users, “g” for group, “o” for others, and “ugo” or “a” (for all).

`chmod ugo+rwx foldername` to give read, write, and execute to everyone.

`chmod a=r foldername` to give only read permission for everyone.



```
Terminal
File Edit View Terminal Tabs Help
roman@ibmclass:~/tsfiles> ls -l
total 0
-rwxr-xr-x 1 roman users 0 2011-09-28 10:48 testfile
d--x--x--x 2 roman users 48 2011-09-28 10:47 workfolder
roman@ibmclass:~/tsfiles> chmod g-rx testfile
roman@ibmclass:~/tsfiles> chmod o+w testfile
roman@ibmclass:~/tsfiles> ls -l
total 0
-rwx---rwx 1 roman users 0 2011-09-28 10:48 testfile
d--x--x--x 2 roman users 48 2011-09-28 10:47 workfolder
roman@ibmclass:~/tsfiles>
```

Changing Groups of Files and Directories in Linux

By issuing these commands, you can change groups of files and directories in Linux.

`chgrp groupname filename`

`chgrp groupname foldername`

Note that the group must exist before you can assign groups to files and directories.

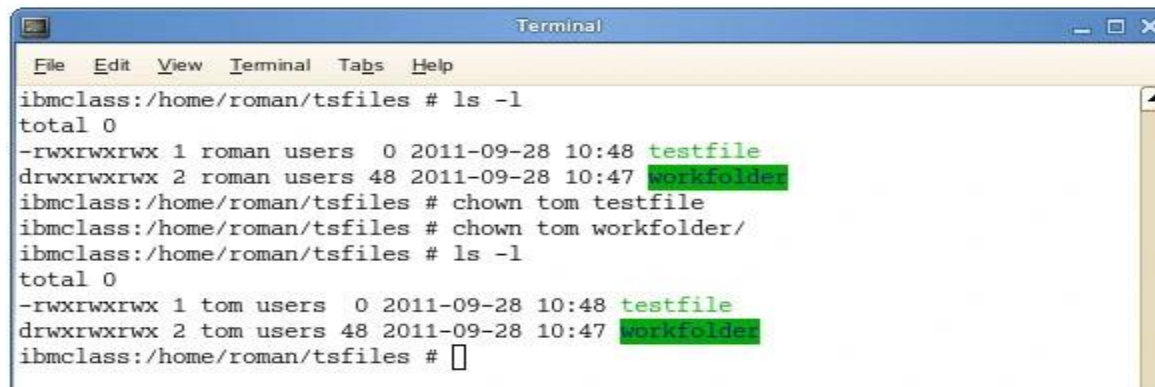


```
Terminal
File Edit View Terminal Tabs Help
roman@ibmclass:~/tsfiles> ls -l
total 0
-rwxr-xr-x 1 roman users 0 2011-09-28 10:48 testfile
d--x--x--x 2 roman users 48 2011-09-28 10:47 workfolder
roman@ibmclass:~/tsfiles>
```

Changing ownership in Linux

Another helpful command is changing ownerships of files and directories in Linux:

- `chown name filename`
- `chown name foldername`

A terminal window titled "Terminal" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The user is in the directory /home/roman/tsfiles. They run 'ls -l' showing 'testfile' with permissions -rwxrwxrwx and 'workfolder' with drwxrwxrwx. Then they run 'chown tom testfile' and 'chown tom workfolder/'. A second 'ls -l' shows both files now owned by 'tom' with the same permissions.

```
ibmclass:/home/roman/tsfiles # ls -l
total 0
-rwxrwxrwx 1 roman users 0 2011-09-28 10:48 testfile
drwxrwxrwx 2 roman users 48 2011-09-28 10:47 workfolder
ibmclass:/home/roman/tsfiles # chown tom testfile
ibmclass:/home/roman/tsfiles # chown tom workfolder/
ibmclass:/home/roman/tsfiles # ls -l
total 0
-rwxrwxrwx 1 tom users 0 2011-09-28 10:48 testfile
drwxrwxrwx 2 tom users 48 2011-09-28 10:47 workfolder
ibmclass:/home/roman/tsfiles #
```

Changing Linux permissions in numeric code

You may need to know how to change permissions in numeric code in Linux, so to do this you use numbers instead of “r”, “w”, or “x”.

0 = No Permission

1 = Execute

2 = Write

4 = Read

Basically, you add up the numbers depending on the level of permission you want to give.

A terminal window titled "Terminal" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The user is in /home/roman. They run 'ls -l' showing 'tsfiles' with permissions drwxr-xr-x. Then they run 'chown -R tom:sales /home/roman/tsfiles'. A second 'ls -l' shows 'tsfiles' now owned by 'tom:sales' with the same permissions.

```
ibmclass:/home/roman # ls -l
total 0
drwxr-xr-x 3 roman users 104 2011-09-28 10:56 tsfiles
ibmclass:/home/roman # chown -R tom:sales /home/roman/tsfiles
ibmclass:/home/roman # ls -l
total 0
drwxr-xr-x 3 tom sales 104 2011-09-28 10:56 tsfiles
ibmclass:/home/roman #
```

Permission numbers are:

0 = ---

1 = --x

2 = -w-

3 = -wx

4 = r-

5 = r-x

6 = rw-

7 = rwx

For example:

`chmod 777 foldername` will give read, write, and execute permissions for everyone.

`chmod 700 foldername` will give read, write, and execute permissions for the user only.

`chmod 327 foldername` will give write and execute (3) permission for the user, w (2) for the group, and read, write, and execute for the users.

As you can see, there are several options when it comes to permissions. You have the capability to dictate usability among users. While it may be easier to just give all permission to everyone, it may end up biting you in the end. So choose wisely.

Program 8

Generate Word list from using wordlist generator Crunch.

AIM:

Generate a Word list using wordlist generator Crunch.

DESCRIPTION:

Crunch is a wordlist generating utility used to create a worklist using letters, numbers, and symbols. Mostly, Hackers use this tool to create passwords. It has a very simple syntax and can be used using the command line. Crunch comes pre-installed in Kali Linux.

If crunch is not installed in your system, Install it by running the following command:

sudo apt install crunch

```
(sid@kali)-[~]
$ sudo apt install crunch
[sudo] password for sid:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  crunch
0 upgraded, 1 newly installed, 0 to remove and 851 not upgraded.
Need to get 30.3 kB of archives.
After this operation, 85.0 kB of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 crunch amd64 3.6-3 [30.3 kB]
Fetched 30.3 kB in 12s (2,615 B/s)
Selecting previously unselected package crunch.
(Reading database ... 224500 files and directories currently installed.)
Preparing to unpack .../crunch_3.6-3_amd64.deb ...
Unpacking crunch (3.6-3) ...
Setting up crunch (3.6-3) ...
Processing triggers for kali-menu (2021.4.2) ...
Processing triggers for man-db (2.9.4-4) ...
```

Crunch: Syntax

The basic syntax to create a wordlist is:

crunch <min> <max> <charset> <options>

Here,

min:- It is the minimum password length

max:- It is the maximum password length

charset:- Character set to be used

options:- options to be used (like -o to save the output to a file)

Steps to Create a Wordlist Using Crunch

Open a terminal by pressing Ctrl+Alt+T and execute the following command:

crunch 3 6 0123456789


```

(sid@kali)-[~]
$ crunch 3 6 0123456789
Crunch will now generate the following amount of data: 7654000 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1111000
000
001
002
003
004
005
006
007
008
009
010
011
012
013
014
015
016

```

Here, the minimum password length is 3 and the maximum number of combinations will be of six characters. It uses permutations and combinations to create a wordlist with all the possible combinations.

To save the output to a file, use -o by running the following command:

crunch 3 6 0123456789 -o list.txt

```

(sid@kali)-[~]
$ crunch 3 6 0123456789 -o list.txt
Crunch will now generate the following amount of data: 7654000 bytes
7 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1111000

crunch: 100% completed generating output

```

If you want to create a wordlist with passwords of 10 character that ends with 123, You can do so by executing the following command:

crunch 10 10 @@@@123 -o list1.txt

```

(sid@kali)-[~]
$ crunch 10 10 @@@@123 -o list1.txt
Crunch will now generate the following amount of data: 11534336 bytes
11 MB
0 GB
0 TB
0 PB

```

You can also use letters and symbols as shown below:

crunch 4 8 123abcdefgh#\$% -o list2.txt

```
(sid@kali)-[~]
$ crunch 4 8 123abcdefgh#$% -o list2.txt
Crunch will now generate the following amount of data: 14181535312 bytes
13524 MB
13 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1589308336

crunch: 4% completed generating output
crunch: 9% completed generating output
crunch: 14% completed generating output
crunch: 19% completed generating output
crunch: 23% completed generating output
crunch: 28% completed generating output
crunch: 33% completed generating output
crunch: 37% completed generating output
crunch: 42% completed generating output
crunch: 47% completed generating output
```

You can use the `-c` parameter to set the number of lines to be printed, `-s` to specify a particular string to begin the wordlist with, `-b` to set the maximum size of the wordlist. Examples for these parameters are shown below:

crunch 2 6 hbfue43487 -c 50

```
(sid@kali)-[~]
$ crunch 2 6 hbfue43487 -c 50
Crunch will now generate the following amount of data: 390608 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 66470
hh
hb
hf
hu
he
h4
h3
h8
h7
bh
bb
bf
bu
be
b4
b3
b8
b7
fh
fb
```

crunch 3 6 qwebdhf32uibvru33223 -s qwe -o START

```
(sid@kali)-[~]  
$ crunch 3 6 qwebdhf32uibvru33223 -s qwe -o START  
Crunch will now generate the following amount of data: 36166954 bytes  
34 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 5228845  
  
crunch: 100% completed generating output
```

Always use -o START with -b and -c parameters.

crunch 2 10 webjhweb32562356 -b 3mb -o START

```
(sid@kali)-[~]  
$ crunch 3 3 webjhweb32562356 -b 1mb -o START  
Crunch will now generate the following amount of data: 2916 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 729  
  
crunch: 100% completed generating output  
  
(sid@kali)-[~]  
$
```

Conclusion

So, We discussed how to create a custom wordlist using crunch utility in kali Linux. Many parameters are mentioned along with the examples. To know more about crunch, Refer to the manpage by running `man crunch` in a terminal window.

