# INDEX

| Sr. No. | PRACTICAL |
|---|---|
| 1 | **Using the tools for whois, traceroute, email tracking, google hacking.** |
| | Ping Utility |
| | Traceroute using Ping Utility |
| | Nslookup |
| | SmartWhois |
| | Search Diggity |
| | HTTrack Website Copier |
| | eMailTracker Pro |
| 2 | **Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.** |
| | Advanced IP Scanner |
| | Amap |
| | Nmap |
| | CurrPorts |
| | GFI Languard 2012 |
| | LANSurveyor |
| | Nessus |
| | HTTPort/HTTHost |
| | MegaPing |
| | G-Zapper |
| | Colasoft Packet Builder |
| | The Dude |
| 3 | **Using NETBIOS Enumeration tool, SNMP Enumeration tool, LINUX/ UNIX. enumeration tools, NTP Enumeration tool, DNS analyzing and enumeration tool.** |
| | Null Session with Nmap |
| | SuperScan |
| | NetBIOS Enumerator |
| | SolarWinds Toolset |
| | Hyena |
| | SoftPerfect Network Scanner |
| 4 | **Study of System Hacking tool** |
| | PWdump7 |
| | LCP |
| | RainbowCrack and WinRTGen |
| | L0pthCrack |
| | OphCrack |
| | NTFS Streams |
| | ADS Spy |
| | Stealth Files Tool |
| | Snow |
| | CHNTPW.ISO |

| | |
|---|---|
| | QuickStego |
| 5 | Study of Denial of Service attack tools. |
| | Hping3 |
| | DoSHTTP |
| 6 | Study of Web server Attack tools |
| | IBM Security AppScan |
| | HTTPRecon |
| | IDServe |
| | MetaSploit |
| 7 | Using Cryptanalysis Tools |
| | HashCalc |
| | MD5Calculator |
| | AES Encryption Package |
| | TrueCrypt |
| | CrypTool |
| | BCTextEncoder |
| | Rohos Disk Encryption |
| 8 | Study of Session Hijacking tools |
| | ZAP |
| 9 | Study of Other Security Tools |
| | Snort |
| | KFCSensor |

# Practical 1

**Aim: Using the tools for whois, traceroute, email tracking, google hacking.**

**Tools:** Ping, Tracert using ping, NSLookup, SmartWhois, Search Diggity, HTTrack Website Copier, eMailTracker Pro

***Tool 1: Ping (Packet INternet Gropher)***

The ping command works by sending special Internet Protocol (IP) packets, called Internet Control Message Protocol (ICMP) Echo Request datagrams, to a specified destination. Each packet sent is a request for a reply. The output response for a ping contains the success ratio and round-trip time to the destination. From this information, it is possible to determine if there is connectivity to a destination. The ping command is used to test the NIC transmit and receive function, the TCP/IP configuration, and network connectivity.

**Steps:**

To ping a computer using the 'ping' command open command prompt.

To specify the data length in bytes we use –l switch. To specify that the packet should not be fragmented we use –f.

To Check for connectivity to particular IP address or hostname or website name

ping www.google.com

To find out the maximum frame size on the network

ping www.google.com -f -l 1500

The –l value needs to be adjusted till we get a reply. The border where the reply is received is said to be its MTU (Maximum Transmission Unit)

To find out what happens when TTL expires

ping www.google.com -i 3

***Tool 2: Tracert using ping (Using ping to emulate tracert)***

This command is a computer network diagnostic tool for displaying or tracing the route (path) between the sender and destination host.

Traceroute can be performed by using the –n and –i switches. -n means number of replies to show and –i means obtain reply from the machine in the next hop

ping www.google.com -i 1 -n 1

Keep on increasing the i value until the www.google.com site directly replies to the ping. At each i value, the device in the route will reply back.

***Tool 3: NSLookup***

NSLookup is used to perform DNS Foorprinting by using the windows command nslookup.

Type nslookup in command prompt and then check the 'set type=' for SOA, NS, A, PTR, CNAME, MX, SRV

***Tool 4: SmartWhois***

SmartWhois is a network information utility that allows you to look up most available information on a hostname, IP address or domain

SmartWhois helps you to search for information such as:

The owner of the domain

The domain registration date and the owner's contact information

The owner of die IP address block

**Steps:**

Start > Programs > SmartWhois

Type an IP address/hostname/domain in the field tab

Click on query and select ‘As IP address/hostname’ or ‘As Domain’

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| SmartWhois | **Domain name query results:** Owner of the website |
| | **Host name query results:** Geographical location of the hosted website |
| | **IP address query results:** Owner of the IP address block |

***Tool 5: Search Diggity***

Search Diggity is the primary attack tool of the Google Hacking Diggity Project. It is an MS Windows GUI application that serves as a front-end to the latest versions of Diggity tools: Google Diggity, Bing Diggity, Link From Domain Diggity, CodeSearch Diggity, DLP Diggity, Flash Diggity, Malware Diggity, PortScan Diggity, SHODAN Diggity, BingMalware Search, and NotlnMyBackYard Diggity.

**Steps:**

Start > Programs > Search Diggity

The Search Diggity main window appears with Google as the default search engine

Select “Sites/Domains/IP Ranges . Type a URL to perform Google Hacking against and then click on the Add button.

Select the vulnerability database to use from the left and then select the search queries you would like to search for

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Search Diggity | Many error messages found relating to vulnerabilities |

***Tool 6: HTTrack Website Copier***

HTTrack Website Copier is an Offline browser utility that allows you to download a World Wide Web site through the Internet to your local directory.

**Steps:**

Start > Programs > HTTrack Website Copier

Click on ‘Next’ to create Project and give a name to project and Click on ‘Next’.

Click on ‘Add URL’ and give the URL of the site to mirror from.

Any additional options that need to be set, can be set from the ‘Set Options’ menu, then click ‘Next’

By default, the radio button will be selected for Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.

The mirroring of the site now begins. The site will be downloaded and saved in the C:\My Web Sites\<Project Name>

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| HTTrack Web Site Copier | ▪ Offline copy of the website www.certifiedhacker.com is created |

***Tool 7: eMailTracker Pro***

The objective of **using eMailTrackerPro is** to:

Trace an email to its true **geographical** source

**Collect Network** (ISP) and **domain Whois** information for any email traced

**Steps:**

Start > Programs > eMailTracker Pro

Click on ‘Trace an email I have received’, then copy the email header fields under the ‘Enter Details’ and then click on Trace

The results shows a location map, the Trace Route below and the Whois/Network/Email summary in the right columns.

To view the HTML Report of it, go to the “My Trace Reports” tab and then click on the “HTML Report” button.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| eMailTrackerPro | **Map:** Location of traced email in GUI map |
| | **Table:** Hop in the route with IP |
| | **Email Summary:** Summary of the traced email<br>▪ From & To email address<br>▪ Date<br>▪ Subject<br>▪ Location |
| | **Trace Information:**<br>▪ Subject<br>▪ Sender IP<br>▪ Location |

# Practical 2

**Aim: Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.**

**Tools**: Advanced IP Scanner, AMap, NMap, CurrPorts, GFI Languard 2012, LANSurveyor, Nessus, HTTPort/HTTHost, MegaPing, G-Zapper, Colasoft Packet Builder, The Dude

**Note**: For all tools in this practical you will require two VM's, one will be the attacker and other will be the victim.

***Tool 1: Advanced IP Scanner***

Advanced IP Scanner is a free network scanner that gives you various types of information regarding local network computers. This tool is used to:

- Perform a system and network scan
- Enumerate user accounts
- Execute remote penetration
- Gather information about local network computers

**Steps:**

- On the attacker's machine: Start > Programs> Advanced IP Scanner
- Then start the victim's machine
- Switch back to the attacker's victim
- In the main window of Advanced IP Scanner, enter IP address range in the 'Select Range' field
- Click Scan to start the scan
- Advanced IP Scanner scans all the IP addresses within the range and displays the scan results after completion
- It will detect the victim's IP address and display the status as live
- Right-click any of the detected IP addresses. It will list Wake-On-LAN, Shut down, and Abort Shut down.
- The list displays properties of the detected computer, such as IP address, Name, MAC, and NetBIOS information.
- You can forcefully Shutdown, Reboot, and Abort Shutdown the selected victim machine/IP address
- Now you have the IP address, Name, and other details of the victim machine

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Advanced IP Scanner | **Scan Information:**<br>▪ IP address<br>▪ System name<br>▪ MAC address<br>▪ NetBIOS information<br>▪ Manufacturer<br>▪ System status |

***Tool 2: Amap***

Amap determines the applications running on each open port. With this tool you can:

- Identify the application protocols running on open ports 80
- Detect application protocols

**Steps:**

- Start > Programs > Command Prompt
- Navigate to the Amap directory
- Type 'amap www.certifiedhacker.com 80', and press Enter
- You can see the specific application protocols running on the entered host name and the port 80

Use the IP address to check the applications running on a particular port. In the command prompt, type the IP address of your virtual machine ‘amap 10.0.0.4 75-81’ and press Enter (IP address will be different in your network)

Try scanning different websites using different ranges of switches like ‘amap www.certifiedhacker.com 1-200’

***Tool 3: Nmap***

Nmap (Zenmap is the official Nmap GUI) is a free, open source (license) utility for network exploration and security auditing. With the help of this tool you can:

Scan TCP and UDP ports

Analyze host details and their topology

Determine the types of packet filters

Record and save all scan reports

Compare saved results for suspicious ports

**Steps:**

Start > Programs > Zenmap. The Nmap - Zenmap GUI window appears.

Enter the victim virtual machine IP address in the ‘target’ text field. You are performing a network inventory for the victim virtual machine

In the ‘Profile’ text field, select from the drop-down list, the type of profile you want to scan. In this lab, select ‘Intense Scan’ and click ‘Scan’ to start scanning the virtual machine

Nmap scans the provided IP address with Intense scan and displays the scan result below the Nmap Output tab.

Click the Ports/Hosts tab to display more information on the scan results. Nmap also displays the Port, Protocol, State, Service, and Version of the scan

Click the Topology tab to view Nmap’s topology for the provided IP address in the Intense scan Profile

Click the Host Details tab to see the details of all hosts discovered during the intense scan profile

Click the Scans tab to scan details for provided IP addresses.

Now, click the Services tab located in the right pane of the window. This tab displays the list of services.

Click the http service to list all the HTTP Hostnames/IP addresses, Ports, and their states (Open/Closed).

Click the msrpc service to list all the Microsoft Windows RPC.

Click the netbios-ssn service to list all NetBIOS hostnames.

***Xmas Scan***

Xmas scan sends a TCP frame to a remote device with URG, ACK, RST, SYN, and FIN flags set. FIN scans only with OS TCP/IP developed according to RFC 793.

Now, to perform a Xmas Scan, you need to create a new profile. Click Profile > New Profile or Command Ctrl+P

On the Profile tab, enter Xmas Scan in the Profile name text field.

Click the Scan tab, and select Xmas Tree scan (-sX) from the TCP scans: drop-down list.

Select None in the Non-TCP scans: drop-down list & Aggressive (-T4) in Timing template list & click Save Changes

Enter the IP address in the Target field, select the Xmas scan option from the Profile field and click Scan

Nmap scans the target IP address provided and displays results on the Nmap Output tab.

Click the Services tab located at the right side of the pane. It displays all the services of that host.

***Null Scan***

Null scan works only if the operating system’s TCP/IP implementation is developed according to RFC 793. In a null scan, attackers send a TCP frame to a remote host with NO Flags.

To perform a null scan for a target IP address, create a new profile. Click Profile > New Profile or Command Ctrl+P

On the Profile tab, input a profile name Null Scan in the Profile name text field.

Click the Scan tab in the Profile Editor window. Now select Null Scan (-sN) option from TCP scan drop-down list.

Select None from the Non-TCP scans drop-down field and select Aggressive (-T4) from the Timing template drop-down field.

Click Save Changes to save the newly created profile.

In the main window of Zenmap, enter the target IP address to scan, select the Null Scan profile from the Profile drop-down list, and then click Scan.

Nmap scans the target IP address provided and displays results in Nmap Output tab.

Click the Host Details tab to view the details of hosts, such as Host Status, Addresses, Open Ports, and Closed Ports

***ACK Flag Scan***

Attackers send an ACK probe packet with a random sequence number. No response means the port is filtered and an RST response means the port is not filtered.

To perform an ACK Flag Scan for a target IP address, create a new profile. Click Profile > New Profile or Command Ctrl+P.

On the Profile tab, input ACK Flag Scan in the Profile name text field.

To select the parameters for an ACK scan, click the Scan tab in the Profile Editor window, select ACK scan (-sA) from the Non-TCP scans drop-down list, and select None for all the other fields but leave the Targets field empty.

Now click the Ping tab and check IPProto probes (-PO) to probe the IP address, and then click Save Changes.

In the Zenmap main window, input the IP address of the victim virtual machine, select ACK Flag Scan from Profile drop-down list, and then click Scan.

Nmap scans the target IP address provided and displays results on Nmap Output tab.

To view more details regarding the hosts, click the Host Details tab

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Nmap | **Types of Scan used:**<br>▪ Intense scan<br>▪ Xmas scan<br>▪ Null scan<br>▪ ACK Flag scan |
| | **Intense Scan – Nmap Output**<br>▪ ARP Ping Scan – 1 host<br>▪ Parallel DNS resolution of 1 host<br>▪ SYN Stealth Scan<br>• Discovered open port on 10.0.0.4<br>o 135/tcp, 139/tcp, 445/tcp, …<br>▪ MAC Address<br>▪ Operating System Details<br>▪ Uptime Guess<br>▪ Network Distance<br>▪ TCP Sequence Prediction<br>▪ IP ID Sequence Generation<br>▪ Service Info |

***Tool 4: CurrPorts***

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. With the help of this tool you can:

Scan the system for currently opened TCP/IP and UDP ports

Gather information on the ports and processes that are opened

List all the IP addresses that are currently established connections

Close unwanted TCP connections and kill the process that opened the ports

**Steps:**

Start > Programs > CurrPorts. It automatically displays process name, ports, IP and remote addresses, and their states

CurrPorts lists all the processes and their IDs, protocols used, local and remote IP address, local and remote ports, and remote host names

To view all the reports as an HTML page, click View > HTML Report - All Items

To view only the selected report as HTML page, select reports and click View > HTML Reports - Selected Items

To view the properties of a port, select the port and click File > Properties

To close a TCP connection you think is suspicious, select the process and click File > Close Selected TCP Connections (or Ctrl+T)

To kill the processes of a port, select the port and click File > Kill Processes of Selected Ports

To exit from the CurrPorts utility, click File > Exit. The CurrPorts window closes

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| CurrPorts | **Profile Details:** Network scan for open ports<br>**Scanned Report:**<br>▪ Process Name<br>▪ Process ID<br>▪ Protocol<br>▪ Local Port<br>▪ Local Address<br>▪ Remote Port<br>▪ Remote Port Name<br>▪ Remote Address<br>▪ Remote Host Name |

***<u>Tool 5: GFI Languard 2012</u>***

GFI LanGuard scans networks and ports to detect, assess, and correct any security vulnerabilities that are found. With the help of this tool you can:

Perform a vulnerability scan

Audit the network

Detect vulnerable ports

Identify security vulnerabilities

Correct security vulnerabilities with remedial action

**Steps:**

Start > Programs > GFI LanGuard

Click 'Launch a Scan' option to perform a network scan

Launch a New scan window will appear

In the Scan Target option, select localhost from the drop-down list

In the Profile option, select Full Scan from the drop-down list

In the Credentials option, select currently logged on user from the drop-down list

Click Scan.

Scanning will start; it will take some time to scan the network. After completing the scan, the scan result will be shown in the left panel

To check the Scan Result Overview, click IP address of the machine. It shows the Vulnerability Assessment and Network & Software Audit.

Click Vulnerability Assessment. It shows all the Vulnerability Assessment indicators by category

Click Network & Software Audit in the right panel, and then click System Patching Status, which shows all the system patching statuses

Click Ports and under this click Open TCP Ports

Click System Information in the right side panel; it shows all the details of the system information

Click Password Policy

Click Groups; it shows all the groups present in the system

Click the Dashboard tab; it shows all the scanned network information

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| GFI LanGuard 2012 | Vulnerability Level |
| | Vulnerable Assessment |
| | System Patching Status |
| | Scan Results Details for Open TCP Ports |
| | Scan Results Details for Password Policy |
| | **Dashboard – Entire Network**<br>▪ Vulnerability Level<br>▪ Security Sensors<br>▪ Most Vulnerable Computers<br>▪ Agent Status<br>▪ Vulnerability Trend Over Time<br>▪ Computer Vulnerability Distribution<br>▪ Computers by Operating System |

***Tool 6: LANSurveyor***

LANSurveyor discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data. With the help of this tool you can:

Draw a map showing the logical connectivity of your network and navigate around the map

Create a report that includes all your managed switches and hubs

**Steps:**

Start > Programs > LANSurveyor. Review the limitations of the evaluation software and then click 'Continue with Evaluation' to continue the evaluation.

The Getting Started with LANsurveyor dialog box is displayed. Click Start Scanning Network.

The Create A Network Map window will appears; in order to draw a network diagram enter the IP address in Begin Address and End Address, and click Start Network Discovery

LANsurveyor displays the map of your network

***Tool 7: Nessus***

Nessus allows you to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities. Nessus helps to learn, understand, and determine vulnerabilities and weaknesses of a system and network in order to know how a system can be exploited. Network vulnerabilities can be network topology and OS vulnerabilities, open ports and running services, application and service configuration errors, and application and service vulnerabilities. With the help of this tool you can:

Scan the network for vulnerabilities

**Steps:**

To install Nessus double-click the Nessus-5.0.1-x86_64.msi file.

The Open File - Security Warning window appears; click Run

The Nessus - InstallShield Wizard appears. During the installation process, the wizard prompts you for some basic information. Follow the instructions. Click Next.

Before you begin installation, you must agree to the license agreement. Select the radio button to accept the license agreement and click Next.

Select a destination folder and click Next.

The wizard prompts for Setup Type. With the Complete option, all program features will be installed. Check Complete and click Next.

The Nessus wizard will prompt you to confirm installation. Click Install. Once installation is complete, click Finish.

Nessus Major Directories: The major directories of Nessus are shown in the following table.

| Nessus Home Directory | Nessus Sub-Directories | Purpose |
|---|---|---|
| **Windows** | | |
| \Program Files\Tenable\Nessus | \conf | Configuration files |
| | \data | Stylesheet templates |
| | \nessus\plugins | Nessus plugins |
| | \nessus\users\<username>\kbs | User knowledgebase saved on disk |
| | \nessus\logs | Nessus log files |

After installation Nessus opens in your default browser. The Welcome to Nessus screen appears, click the here link to connect via SSL

Click OK in Security Alert pop-up, if it appears. Click Continue to this web site (not recommended) link to continue

The Thank you for installing Nessus screen appears. Click the Get Started > button.

In Initial Account Setup enter the credentials given at the time of registration and click Next.

In Plugin Feed Registration, you need to enter the activation code. To obtain activation code, click the http://www.nessus.org/register/link

Click the Using Nessus at Home icon in Obtain an Activation Code. In Nessus for Home accept the agreement by clicking the Agree button

Fill in the Register a HomeFeed section to obtain an activation code and click Register. The Thank You for Registering window appears for Tenable Nessus HomeFeed.

Now log in to your email for the activation code provided at the time of registration

Now enter the activation code received to your email ID and click Next.

The Registering window appears. After successful registration click, Next: Download plugins to download Nessus plugins. Nessus will start fetching the plugins and it will install them, it will take time to install plugins and initialization

The Nessus Log In page appears. Enter the Username and Password given at the time of registration and click Log In.

After you successfully log in, the Nessus Daemon window appears. If you have an Administrator Role, you can see the Users tab, which lists all Users, their Roles, and their Last Logins.

To add a new policy, click Policies > Add Policy. Fill in the General policy sections, namely, Basic, Scan, Network Congestion, Port Scanners, Port Scan Options, and Performance.

To configure the credentials of new policy, click the Credentials tab shown in the left pane of Add Policy.

To select the required plugins, click the Plugins tab in the left pane of Add Policy.

To configure preferences, click the Preferences tab in the left pane of Add Policy.

In the Plugin field, select Database setting s from the drop-down list. Enter the Login details given at the time of registration. Give the Database SID: 4587, Database port to use: 124, and select Oracle auth type: SYSDBA. Click Submit.

A message Policy "NetworkScan_Policy" was successfully added is displayed

Now, click Scans > Add to open the Add Scan window.

Input the field Name, Type, Policy, and Scan Target

In Scan Targets, enter the IP address of your network

Click Launch Scan at the bottom-right of the window.

The scan launches and starts scanning the network. After the scan is complete, click the Reports tab. Double-click Local Network to view the detailed scan report.

Double-click any result to display a more detailed synopsis, description, security level, and solution

Click the Download Report button in the left pane.

You can download available reports with a '.nessus' extension from the drop-down list.

Now, click Log out. In the Nessus Server Manager, click Stop Nessus Server.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Nessus | **Scan Target Machine:** Local Host |
| | **Performed Scan Policy:** Network Scan Policy |
| | **Target IP Address:** 10.0.0.2 |
| | **Result:** Local Host vulnerabilities |

***Tool 8: HTTPort/HTTHost***

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall. HTTPort creates a transparent tunneling tunnel through a proxy server or firewall.

HTTPort allows using all sorts of Internet Software from behind the proxy. It bypasses HTTP proxies and HTTP, firewalls, and transparent accelerators.

**Steps:**

Before running the tool you need to stop IIS Admin Service and World Wide Web Publishing services on Windows virtual machine. Go to Administrative Privileges > Services > IIS Admin Service, right click and click Stop option.

Go to Administrative Privileges > Services > World Wide Web Publishing Services, right click and click Stop option.

Open HTTHost folder and double click htthost.exe. The HTTHost wizard will open; select the Options tab. On the Options tab, set all the settings to default except Personal Password field, which should be filled in with any other password. In this lab, the personal password is 'magic'

Check the Revalidate DNS names and Log Connections options and click Apply.

Now leave HTTHost intact, and don't turn off Windows Virtual Machine.

Now switch to other Windows Virtual Machine, and install HTTPort, double-click httport3snfm.exe and follow the wizard-driven installation steps.

Start HTTPort. Start > Programs > HTTPort

Select the Proxy tab and enter the hostname or IP address of victim machine (First Virtual Machine).

You cannot set the Username and Password fields.

In the User personal remote host at section, click start and then stop and then enter the targeted Host machine IP address and port, which should be 80.

Here any password could be used. Enter the password as 'magic'

Select the Port Mapping tab and click Add to create New Mapping

Select New Mapping Node, and right-click New Mapping, and click Edit

Rename this to ftp certified hacker, and select Local port node; then right-click Edit and enter Port value to 21. Now right click on Remote host node to Edit and rename it as ftp.certifiedhacker.com. Now right click on Remote port node to Edit and enter the port value to 21.

Click Start on the Proxy tab of HTTPort to run the HTTP tunneling.

Now switch to the first Windows virtual machine and click the Applications log tab. Check the last line if Listener listening at 0.0.0.0:80, and then it is running properly.

Now switch to the second Windows virtual machine and turn ON the Windows Firewall. Go to Windows Firewall with Advanced Security

Select Outbound rules from the left pane of the window, and then click New Rule in the right pane of the window.

In the New Outbound Rule Wizard, select the Port option in the Rule Type section and click Next

Now select All remote ports in the Protocol and Ports section, and click Next

In the Action section, select the Block the connection option and click Next

In the Profile section, select all three options. The rule will apply to Domain, Public and Private and then click Next

Type Port 21 Blocked in the Name field, and click Finish

The new rule Port 21 Blocked is created. Right-click the newly created rule and select Properties

Select the Protocols and Ports tab. Change the Remote Port option to Specific Ports and enter the Port number as 21. Leave the other settings as their defaults and click Apply then click OK.

Type ftp ftp.certifiedhacker.com in the command prompt and press Enter. The connection is blocked in the first Windows virtual machine by firewall.

Now open the command prompt on the second Windows virtual machine and type ftp 127.0.0.1 and press Enter

### ***Tool 9: MegaPing***

MegaPing is an ultimate toolkit that provides complete essential utilities for information system administrator and IT solution providers. MegaPing security scanner checks your network for potential vulnerabilities that might be used to attack your network, and saves information in security reports. With the help of this tool you can:

Ping a destination address list

Traceroute

Perform NetBIOS scanning

**Steps:**

Start > Programs > MegaPing

Select any one of the options from the left pane of the window.

Select IP scanner, and type in the IP range in the From and To field and click Start. You can select the IP range depending on your network. It will list down all the IP addresses under that range with their TTL (Time to Live), Status (dead or alive), and the statistics of the dead and alive hosts.

Select the NetBIOS Scanner from the left pane and type in the IP range in the From and To fields and click Start. The NetBIOS scan will list all the hosts with their NetBIOS names and adapter addresses

Right-click any IP address and select the Traceroute option. It will open the Traceroute window, and will trace the IP address selected.

Select Port Scanner from the left pane and add www.certifiedhacker.com in the Destination Address List and then click the Start button. After clicking the Start button it toggles to Stop. It will lists the ports associated with www.certifiedhacker.com with the keyword, risk, and port number.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| MegaPing | **IP Scan Range:** 10.0.0.1 – 10.0.0.254 |
| | **Performed Actions:**<br>▪ IP Scanning<br>▪ NetBIOS Scanning<br>▪ Traceroute<br>▪ Port Scanning |
| | **Result:**<br>▪ List of Active Host<br>▪ NetBios Name<br>▪ Adapter Name |

### ***Tool 10: G-Zapper***

G-Zapper is a utility to block Google cookies, clean Google cookies, and help you stay anonymous while searching online. G-Zapper helps protect your identity and search history. G-Zapper will read the Google cookie installed on your PC, display the date it was installed, determine how long your searches have been tracked, and display your Google searches. G-Zapper allows you to automatically delete or entirely block the Google search cookie from future installation.

**Steps:**

Start > Programs > G-Zapper

To delete the Google search cookies, click the Delete Cookie button; a window will appear that gives information about the deleted cookie location. Click OK

To block the Google search cookie, click the Block cookie button. A window will appear asking if you want to manually block the Google cookie. Click Yes

It will show a message that the Google cookie has been blocked. To verify, click OK

To test the Google cookie that has been blocked, click the Test Google button. Your default web browser will now open to Google's Preferences page. Click OK.

To view the deleted cookie information, click the Setting button, and click View Log in the cleaned cookies log. The deleted cookies information opens in Notepad.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| G-Zapper | **Action Performed:**<br>▪ Detect the cookies<br>▪ Delete the cookies<br>▪ Block the cookies |
| | **Result:** Deleted cookies are stored in C:\Users\Administrator\Application Data |

***Tool 11: Colasoft Packet Builder***

The Colasoft Packet Builder is a useful tool for creating custom network packets. Colasoft Packet Builder creates and enables custom network packets. This tool can be used to verify network protection against attacks and intruders. Colasoft Packet Builder features a decoding editor allowing users to edit specific protocol field values much easier. Users are also able to edit decoding information in two editors: Decode Editor and Hex Editor. Users can select any one of the provided templates: Ethernet Packet, IP Packet, ARP Packet, or TCP Packet.

**Steps:**

Start > Programs > Colasoft Packet Builder

Before starting of your task, check that the Adapter settings are set to default and then click OK.

To add or create the packet, click Add in the menu section. When an Add Packet dialog box pops up, you need to select the template and click OK. You can view the added packets list on your right-hand side of your window.

Colasoft Packet Builder allows you to edit decoding information in the two editors: Decode Editor and Hex Editor.

To send all packets at one time, click Send All from the menu bar. Check the Burst Mode option in the Send All Packets dialog window, and then click Start.

To export the packets sent from the File menu, select File > Export > All Packets.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Colasoft Packet Builder | **Adapter Used:** Realtek PCIe Family Controller |
| | **Selected Packet Name:** ARP Packets |
| | **Result:** Captured packets are saved in packets.cscpkt |

## ***Tool 12: The Dude***

The Dude network monitor is a new application that can dramatically improve the way you manage your network environment. The Dude automatically scans all devices within specified subnets, draws and lays out a map of your networks, monitors services of your devices, and alerts you in case some service has problems.

**Steps:**

Start > Programs > The Dude

Click the Discover button on the toolbar of the main window. The Device Discovery window appears.

In the Device Discovery window, specify Scan Networks range, select default from the Agent drop-down list, select DNS, SNMP, NETBIOS, and IP from the Device Name Preference drop-down list, and click Discover.

Once the scan is complete, all the devices connected to a particular network will be displayed.

Select a device and place the mouse cursor on it to display the detailed information about that device. Now, click the down arrow for the Local drop-down list to see information on History Actions, Tools, Files, Logs, and so on. Select options from the drop-down list to view complete information.

As described previously, you may select all the other options from the drop-down list to view the respective information. Once scanning is complete, click the  button to disconnect.

# Practical 3

**Aim: Using NETBIOS Enumeration tool, SNMP Enumeration tool, LINUX/ UNIX. enumeration tools, NTP Enumeration tool, DNS analyzing and enumeration tool.**

**Tools:** Null session with NMap, SuperScan, NetBIOS Enumerator, SolarWinds Toolset, Hyena, SoftPerfect Network Scanner.

***Tool 1: Null session with NMap***

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

**Steps:**

Start > Programs > Nmap-Zenmap GUI

Perform the nmap -O scan to find the open ports running on the target/victim machine

If Ports 139 and 445 are open then the machine can be NetBIOS enumerated.

Run Nbtstat by the command nbtstat -A <IPAddress>

To create a null scan, in the command prompt, type net use \\X.X.X.X\IPC$ “”/u:”” (where X.X.X.X is the address of the host machine, and there are no spaces between the double quotes).

Confirm it by issuing a generic net use command to see connected null sessions from your host. To confirm, type net use, which should list your newly created null session.

***Tool 2: SuperScan***

SuperScan is a TCP port scanner, pinger, and resolver. The tool's features include extensive Windows host enumeration capability, TCP SYN scanning, and UDP scanning.

**Steps:**

Start > Programs > SuperScan

Click the Windows Enumeration tab located on the top menu. Enter the Host name/IP/URL in the text box.

Check the types of enumeration you want to perform. Now, click Enumerate.

SuperScan starts enumerating the provided host name and displays the results in the right pane of the window.

Wait for a while to complete the enumeration process. After the completion of the enumeration process, an Enumeration completion message displays.

***Tool 3: NetBIOS Enumerator***

Enumeration involves making active connections, so that they can be logged. Typical information attackers look for in enumeration includes user account names for future password guessing attacks. NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other interesting web techniques, such as SMB.

**Steps:**

Start > Programs > NetBIOS Enumerator

In the IP range to scan section at the top left of the window, enter an IP range in from and to text fields. Click Scan.

NetBIOS Enumerator starts scanning for the range of IP addresses provided. After the completion of scanning, the results are displayed in the left pane of the window.

A Debug window section, located in the right pane, show’s the scanning of the inserted IP range and displays Ready! after completion of the scan.

***Tool 4: SolarWinds Toolset***

The SolarWinds Toolset provides the tools you need as a network engineer or network consultant to get your job done. Toolset includes best-of-breed solutions that work simply and precisely, providing the diagnostic, performance, and bandwidth measurements you want, without extraneous, unnecessary features.

**Steps:**

Configure SNMP services and select Start > Control Panel > Administrative Tools > Services.

Double-click SNMP service. Click the Security tab, and click Add. The SNMP Services Configuration window appears. Select READ ONLY from Community rights and Public in Community Name, and click Add.

Select Accept SNMP packets from any host, and click OK.

Launch the tool. Start > Programs > SolarWinds Workspace Studio

Click External Tools, and then select Classic tools > Network Discovery > IP Network Browser.

IP Network Browser will be shown. Enter the victim virtual machine IP address and click Scan Device.

It will show the result in a line with the IP address and name of the computer that is being scanned.

Now click the Plus (+) sign before the IP address. It will list all the information of the targeted IP address.

***Tool 5: Hyena***

Hyena uses an Explorer-style interface for all operations, including right mouse click pop-up context menus for all objects. Management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, expo/ting job scheduling, processes, and printing are all supported.

**Steps:**

Start > Programs > Hyena. The Registration window will appear. Click OK to continue.

Click '+' to expand Local workstation, and then click Users.

To check the services running on the system, double-click Services

To check the User Rights, click '+' to expand it.

To check the Scheduled jobs, click '+' to expand it.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| | **Intention :** Enumerating the system |
| Hyena | **Output:**<br>▪ Local Connections<br>▪ Users<br>▪ Local Group<br>▪ Shares<br>▪ Shares<br>▪ Sessions<br>▪ Services<br>▪ Events<br>▪ User Rights<br>▪ Performance<br>▪ Registry<br>▪ WMI |

***Tool 6: SoftPerfect Network Scanner***

SoftPerfect Network Scanner is a free multi-threaded IP, NetBIOS, and SNMP scanner with a modern interface and many advanced features.

**Steps:**

Start > Programs > SoftPerfect Network Scanner

To start scanning your network, enter an IP range in the Range From field and click Start Scanning.

The status bar displays the status of the scanned IP addresses at the bottom of the window.

To view the properties of an individual IP address, right-click that particular IP address.

# Practical 4

**Aim: Study of System Hacking tool**

**Tools:** PWdump7, LCP, RainbowCrack and WinRTGen, L0pthCrack, Ophcrack, NTFS Streams, ADS Spy, Stealth Files Tool, Snow, CHNTPW.ISO, Quick Stego.

***Tool 1: PWdump7***

Pwdump7 can be used to dump protected files. You can always copy a used file just by executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key

**Steps:**

Open the command prompt and navigate to the PWdump7 folder

Now type pwdump7.exe and press Enter, which will display all the password hashes

Now type pwdump7.exe > c:\hashes.txt in the command prompt, and press Enter

This command will copy all the data of pwdump7.exe to the c:\hashes.txt file. (To check the generated hashes you need to navigate to the C: drive)

***Tool 2: LCP***

Link Control Protocol (LCP) is part of the Point-to-Point (PPP) protocol. In PPP communications, both the sending and receiving devices send out LCP packets to determine specific information required for data transmission. LCP program mainly audits user account passwords and recovers them in Windows 2008 and 2003. General features of this protocol are password recovery, brute force session distribution, account information importing, and hashing. It can be used to test password security, or to recover lost passwords. The program can import from the local (or remote) computer, or by loading a SAM, LC, LCS, PwDump or Sniff file. LCP supports dictionary attack, brute force attack, as well as a hybrid of dictionary and brute force attacks.

**Steps:**

Start > Programs > LCP

From the menu bar, select Import and then Import from remote computer.

Select Computer name or IP address, select the Import type as Import from registry, and click OK. The output window appears.

Now select any User Name and click the Play button. This action generates passwords.

***Tool 3: RainbowCrack and WinRTGen***

***WinRTGen***

Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM , LMCHALL, Half LMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes.

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering plaintext passwords, up to a certain length, consisting of a limited set of characters.

**Steps:**

Double-click the winrtgen.exe file and click the Add Table button.

Rainbow Table properties window appears:

Select ntlm from the Hash drop-down list

Set the Min Len as 4, the Max Len as 9, and the Chain Count of 4000000

Select loweralpha from the Charset drop-down list (this depends on the password)

Click OK.

A file will be created; click OK.

Creating the hash table will take some time, depending on the selected hash and charset. Created a hash table saved automatically in the folder containing winrtgen.exe

***RainbowCrack***

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password.

**Steps:**

Double-click the rcrack_gui.exe file. Click File, and then click Add Hash

The Add Hash window appears:

Navigate to c:\hashes, and open the hashes.txt file (which is already generated using Pwdump7 located at c:\hashes.txt)

Right-click, copy the hashes from hashes.txt file

Paste into the Hash field, and give the comment (optional)

Click OK. The selected hash is added

To add more hashes, repeat the above step

Click the Rainbow Table from the menu bar, and click Search Rainbow Table

Browse the Rainbow Table that is already generated using WinRTGen and click Open

It will crack the password

***Tool 4: L0pthCrack***

L0phtCrack is packed with powerful features, such as scheduling, hash extraction from 64-bit Windows versions; multiprocessor algorithms, and network monitoring and decoding. It can import and crack UNIX password files and remote Windows machines. L0phtCrack provides a scoring metric to quickly assess password quality. Passwords are measured against current industry best practices and are rated as Strong, Medium, Weak, or Fail.

**Steps:**

Start > Programs > L0phtCrack6

Launch L0phtCrack, and in the L0phtCrack Wizard, click Next

Choose Retrieve from the local machine in the Get Encrypted Passwords wizard and click Next

Choose Strong Password Audit from the Choose Auditing Method wizard and click Next

In Pick Reporting Style, select all Display encrypted password hashes, click Next and then click Finish

L0pthCrack6 shows an Audit Completed message, Click OK

Click Session options from the menu bar

Auditing options For This Session window appears:

Select the Enabled, Crack NTLM Passwords check boxes in Dictionary Crack.

Select the Enabled, Crack NTLM Passwords check boxes in Dictionary/Brute Hybrid Crack.

Select the Enabled, Crack NTLM Passwords check boxes in Brute Force Crack.

Select the Enable Brute Force Minimum Character Count check box.

Select the Enable Brute Force Maximum Character Count check box.

Click OK.

Click Begin from the menu bar. L0phtCrack cracks the administrator password

A report is generated with the cracked passwords

***Tool 5: OphCrack***

OphCrack is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables. Rainbow tables for LM hashes of alphanumeric passwords are provided for free by developers. By default, OphCrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters.

**Steps:**

Start > Programs > OphCrack

Click Load, and then click PWDUMP file.

Browse the PWDUMP file that is already generated by using PWDUMP7 (located at c:\hashes.txt) and click Open

Loaded hashes are shown

Click Table. The Table Selection window will appear

Note: You can download the free XP Rainbow Table, Vista Rainbow Tables from http://ophcrack.sourceforge.net/tables.php

Select XP free fast, and click Install

The Browse For Folder window appears; select the table_xp_free_fast and click OK

The selected table XP free fast is installed, it shows a green color ball which means it is enabled. Click OK

Click Crack; it will crack the password

***Tool 6: NTFS Streams***

A stream consists of data associated with a main file or directory (known as the main unnamed stream). Each fie and directory in NTFS can have multiple data streams that are generally hidden from the user. NTFS supersedes the FAT file system as the preferred file system for Microsoft Windows operating systems. NTFS has several improvements over FAT and HPFS (High Performance File System), such as improved support for metadata and use of advanced data structures.

**Steps:**

Run this practical in Windows virtual machine and ensure the C:\ drive is formatted for NTFS.

Create a folder called magic on the C:\ drive and copy calc.exe from C:\windows\system32 to C:\magic.

Open a command prompt and go to C:\magic and type notepad readme.txt in command prompt and press Enter.

readme.txt in Notepad appears. (Click Yes button if prompted to create a new readme.txt file). Type Hello World! and Save the file.

Note the file size of the readme.txt by typing dir in the command prompt.

Now hide calc.exe inside the readme.txt by typing the following in the command prompt:

type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

Type dir in command prompt and note the file size of readme.txt

The file size of the readme.txt should not change. Now navigate to the directory c:\magic and delete calc.exe

Return to the command prompt and type command:

mklink backdoor.exe readme.txt:calc.exe and press Enter

Type backdoor, press Enter, and the the calculator program will be executed

| Tool/Utility | Information Collected/Objectives Achieved |
| --- | --- |
| NTFS Streams | **Output:** Calculator (calc.exe) file executed |

***Tool 7: ADS Spy***

Ads Spy is a tool used to list, view, or delete Alternate Data Stream (ADS) on Windows Server 2008 with NTFS file systems. ADS Spy is a method of storing meta-information of files, without actually storing the information inside the file it belongs to.

**Steps:**

Double click to launch ADS Spy

Start an appropriate scan that you need. Click Scan the system for alternate data streams.

Find the ADS hidden info file while you scan the system for alternative data streams.

To remove the Alternate Data Stream, click Remove selected streams.

| Tool/Utility | Information Collected/Objectives Achieved |
| --- | --- |
| ADS Spy | **Scan Option:** Full Scan (all NTFS drives) |
| | **Output:**<br>▪ Hidden files with its location<br>▪ Hidden files size |

***Tool 8: Stealth Files Tool***

Stealth files use a process called steganography to hide any files inside of another file. It is an alternative to encryption of files because no one can decrypt the encrypted information/data from the files unless they know that the hidden files exist.

**Steps:**

Follow the wizard-driven installation instructions to install Stealth Files Tool

Launch Notepad and write Hello World and save the file as Readme.txt on the desktop

Click Start > Programs > Stealth Files Tool

In the main window of Stealth Files 4.0, click Hide Files to start the process of hiding the files and click Add files.

In Step 1, add the Calc.exe from c:\windows\system32\calc.exe

In Step 2 , choose the carrier file and add the file Readme.txt from the desktop

In Step 3, choose a password such as magic (you can type any desired password)

Click Hide Files. It will hide the file calc.exe inside the readme.txt located on the desktop

Open the notepad and check the file; calc.exe is copied inside it

Now open the Stealth files Control panel and click Retrieve Files

In Step 1, choose the file (Readme.txt) from desktop in which you have saved the calc.exe

In Step 2, choose the path to store the retrieved hidden file. For this practical, save it on the desktop

Enter the password magic (the password that is entered to hide the file) and click on Retrieve Files!

The retrieved file is stored on the desktop

| Tool/Utility | Information Collected/Objectives Achieved |
| --- | --- |
| Stealth Files Tool | **Hidden Files:** Calc.exe (calculator) |
| | **Retrieve File:** readme.txt (Notepad) |
| | **Output:** Hidden calculator executed |

***Tool 9: Snow***

Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected. Snow exploits the steganographic nature of whitespace. Locating trailing whitespace in text is like finding a polar bear in a snowstorm. It uses the ICE encryption algorithm, so the name is thematically consistent.

**Steps:**

Open a command prompt and navigate to the folder 'snow'

Open Notepad and type Hello World! and then press enter and press the Hyphen key to draw a line below it

Save the file as readme.txt

Type this command in command shell: readme2.txt. It is the name of another file that will be created automatically.

snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt

(magic is the password, you can type your desired password also)

Now the data ("My Swiss bank account number is 45656684512263") is hidden inside the readme2.txt the with the contents of readme.txt

The contents of readme2.txt are readme.txt + My Swiss bank account number is 45656684512263.

Now type 'snow -C -p "magic" readme2.txt': this will show the contents of readme.txt (magic is the password which was entered while hiding the data)

To check the file in a GUI, open the readme2.txt in Notepad and select Edit > Select all. You will see the hidden data inside readme2.txt in the form of spaces and tabs

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Snow Steganography | **Output:** You will see the hidden data inside Notepad |

***<u>Tool 10: CHNTPW.ISO</u>***

CHNTPW.ISO is a password recovery tool that runs on Windows Server 2003, Windows Server 2008, and Windows 7 Virtual-Machine. CHNTPW.ISO is an offline NT password and registry editor, boot disk/CD.

**Steps:**

Start VMWare Virtual Manager Workstation. Ensure that the Windows XP Virtual Machine is shut down

Select the Windows XP Virtual Machine and click settings

Select CD/DVD drive and select the Image file option and browse for the location of CHNTPW.ISO, and select Apply > OK

Now start by clicking on Power on this Virtual Machine

After booting, Window will prompt you with: Step one: Select disk where Windows installation is, and Press Enter

Now you will see: Step TWO: Select PATH and registry files; press Enter

Select which part of the registry to load, use predefined choices, or list files with space as delimiter, and press Enter

When you see: Step THREE: Password or registry edit, type yes (y), and press Enter

Loaded hives: <SAM><system><SECURITY>

1 — Edit user data and passwords

9 — Registry editor, now with full write support!

Q — Quit (you will be asked if there is something to save)

In What to do? the default selected option will be [1]. Press Enter

In chntpw Edit User Info & Passwords, press Enter to enter the user name to change

In the User Edit Menu:

1 — Clear (blank) user password

2 — Edit (set new) user password (careful with this on XP or Vista)

3 — Promote user (make user an administrator)

4 — Unlock and enable user account [seems unlocked already]

q — Quit editing user, back to user select

The default option, Quit [q], is selected. Type 1 and press Enter

Type ! after clearing the password of the user account, and press Enter

Load hives: <SAM><system><SECURITY>

1 - Edit user data and passwords

9 - Registry editor, now with full write support!

Q — Quit (you will be asked if there is something to save)

In What to do?, the default selected option will be [1]. Type quit (q), and press Enter

In Step FOUR: Writing back Changes, About to write file(s) back! Do it?, here the default option will be [n]. Type yes [y] and press Enter

The edit is completed

Now turn off the Windows Virtual Machine

Go to settings and change the CD/DVD option to Auto-detect and then click Apply > OK

Start the Windows Virtual Machine, you will note that the operating systems starts without requiring any password

***Tool 11: QuickStego***

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include stenographic coding inside of a transport layer, such as a document file, image file, program, or protocol. QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages.

**Steps:**

Follow the wizard-driven installation steps to install QuickStego

Launch Quick Stego from Start menu apps, Start > Programs > QuickStego

Click Open Image in the Picture, Image, Photo File dialog box

Browse and select the image and then click Open

The selected image is added; it will show a message that reads: THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE

To add the text to the image, click Open Text from the Text File dialog box

Browse and select the text file and then click Open

The selected text will be added; click Hide Text in the Steganography dialog box

It shows the following message: The text message is now hidden in image

To save the image (where the text is hidden inside the image) click Save Image in the Picture, Image, Photo File dialog box

Provide the file name as stego, and click Save (to save this file on the desktop)

Exit from the QuickStego window. Again open QuickStego, and click Open Image in the Picture, Image, Photo File dialog box

Browse the Stego file (which is saved on desktop)

The hidden text inside the image will appear

# Practical 5

**Aim: Study of Denial of Service attack tools.**

**Tools:** HPing3, DOSHTTP.

***Tool 1: HPing3***

Hping3 is a command-line oriented TCP/IP packet assembler/analyzer. Hping3 is a network tool able to send custom TCP/IP packets and to display target replies like a ping program does with ICMP replies. Hping3 handles fragmentation, arbitrary packets body, and size and can be used in order to transfer files encapsulated under supported protocols. With the help of this tool you can:

Perform denial-of-service attacks

Send huge amount of SYN packets continuously

**Steps:**

Open terminal in Linux

Hping3 -S -flood -p 80 192.168.0.2 --rand-source

Where -S stays to set SYN Flag, 80 is the port number to DOS attack and all packets sent will seem to be coming from a random source

To view the packets on the victim's machine, launch Wireshark and observe the SYN packets

| Tool/Utility | Information Collected/Objectives Achieved |
| --- | --- |
| **hping3** | SYN packets observed over flooding the resources in victim machine |

***Tool 2: DoSHTTP***

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. DoSHTTP includes port designation and reporting. HTTP flooding is an attack that uses enormous useless packets to jam a web server. DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. It includes URL verification, HTTP redirection, and performance monitoring. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a distributed denial-of-service (DDoS) attack. This tool is used by IT professionals to test web server performance.

**Steps:**

Start > Programs > DoSHTTP

The DoSHTTP main screen appears asking about free trial version. Click Try to continue.

Enter the URL or IP address in the Target URL field. Select a User Agent, number oft Sockets to send, and the type of Requests to send. Click Start.

Click OK in the DoSHTTP evaluation pop-up.

DoSHTTP sends asynchronous sockets and performs HTTP flooding of the target network.

Go to the victim virtual machine, open Wireshark and observe that a lot of packet traffic is captured by Wireshark.

| Tool/Utility | Information Collected/Objectives Achieved |
| --- | --- |
| **DoSHTTP** | HTTP packets observed flooding the host machine |

# Practical 6

**Aim: Study of Web server Attack tools**

**Tools:** IBM Security AppScan, HTTPRecon, IDServe, MetaSploit.

***Tool 1: IBM Security AppScan***

**Steps:**

Download and install trial version of IBM Security AppScan

To Run the application, Start > Programs > IBM Security AppScan

This application will scan the web server and web applications and detect the vulnerabilities on the server and show the remedies to resolve the vulnerabilities

***Tool 2: HTTPRecon***

The httprecon project undertakes research in the field of web server fingerprinting, also known as http fingerprinting. Httprecon is a tool for advanced web server fingerprinting, similar to httprint. The httprecon project does research in the field of web server fingerprinting, also known as http fingerprinting. The goal is highly accurate identification of given httpd implementations.

**Steps:**

Start > Programs > HTTPRecon

Enter the web site (URL) www.juggyboy.com that you want to footprint and select the port number.

Click Analyze to start analyzing the entered web site. You should receive a footprint of the entered web site.

Click the GET long request tab, which will list down the GET request. Then click Fingerprint Details.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| **httprecon Tool** | **Output:** Footprint of the juggyboy website<br>▪ Content-type: text/html<br>▪ content-location: http://juggyboy.com/index.html<br>▪ ETag: "a47ee9091e0cd1:7a49"<br>▪ server: Microsoft-IIS/6.0<br>▪ X-Powered-By: ASP.NET |

***Tool 3: IDServe***

IDServe is a simple,free, small (26 Kbytes), and fast general-purpose Internet server identification utility. IDServe attempts to determine the domain name associated with an IP. This process is known as a reverse DNS lookup and is handy when checking firewall logs or receiving an IP address from someone. Not all IPs that have a forward direction lookup (Domain-to-IP ) have a reverse (IP-to-Domain) lookup, but many do.

**Steps:**

Start > Programs > IDServe

Click the Server Query tab. In option 1, enter (or copy/paste an Internet server URL or IP address) the web site (URL) you want to footprint.

Click Query the Server to start querying the entered web site.

After the completion of the query. IDServe displays the results of the entered web site.

***Tool 4: Metasploit***

Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments.

In this practical, we demonstrate the exploit that takes advantage of two issues in JDK 7: the ClassFinder and MethodFinder.findMethod(). Both were newly introduced in JDK 7. ClassFinder is a replacement for classForName back in JDK 6. It allows untrusted code to obtain a reference and have access to a restricted package in JDK 7, which can be used to abuse sun.awt.SunToolkit (a restricted package). With sun.awt.SunToolkit, we can actually invoke getField() by abusing findMethod() in Statement ivokeInternal() (but getField() must be public, and that's not always the case in JDK 6. In order to access Statement.acc's private field, modify AccessControlContext and then disable Security Manager. Once Security Manager is disabled, we can execute arbitrary Java code.

**Steps:**

Installation of Metasploit will require you create a username, password and then activate the product through email.

After activation, go to Administration and click Software Updates. Click Check for Updates, and after checking the updates, click Install. After completing the updates it will ask you to restart, so click Restart.

After completion of restart it will redirect to Metasploit - Home. Now click Create New Project from the Project drop-down list.

In Project Settings, provide the Project Name and enter a Description, leave the Network Range set to its default, and click Create Project.

Click the Modules tab after the project is created. Enter CVE ID (2012-4681) in Search Modules and click Enter.

Click the Java 7 Applet Remote Code Execution link.

Configure the exploit settings:

In Payload Options set the Payload type as Meterpreter, Connection Type as Reverse and in Listener Host ,enter the IP address where Metasploit is running.

In Module Options, enter the SRV Host IP address where Metasploit is running.

Enter the URI Path and click Run Module button. It will then create a website that will be in the format http://ipaddress:portno/uripath

After the task starts make the victim open their browser and visit the URL

Once the victim visits the URL, the exploit will take advantage of the Java 7 running in his browser and the metasploit machine will start a session with the victim.

The moment Sending stage shows, it means a session has been created and the exploit is successful

Go to session tab, click on the command shell button, and type ipconfig. You will get all the details of the other computers in your network

Click the Go back one page button in Metasploit browser to exit the command shell.

Click Terminate Session to close the session and click OK to confirm

It will display Session Killed. Now from the Account drop-down list, select Logout.

# Practical 7

**Using Cryptanalysis Tools**

**Tools:** HashCalc, MD5Calculator, AES Encryption Package, TrueCrypt, Cryptool, BCText Encoder, ROHOS Disk Encryption.

### *Tool 1: HashCalc*

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey and eMule tools.

HashCalc is a fast and easy-to-use calculator that allows computing message digests, checksums, and HMACs for files, as well as for text and hex strings. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

**Steps:**

Start > Programs > HashCalc

From the Data Format drop-down list, select File. Enter/Browse the data to calculate.

Choose the appropriate Hash algorithms and check the check boxes.

Now, click Calculate.

Document all Hash, MD5, and CRC values for further reference.

### *Tool 2: MD5Calculator*

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files (some GB). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 Calculator is a bare-bones program for calculating and comparing MD5 files. While its layout leaves something to be desired, its results are fast and simple.

**Steps:**

To find MD5 Hash o f any file, right-click the file and select MD5 Calculator from the context menu.

MD5 Calculator shows the MD5 digest of the selected file.

Note: Alternatively, you can browse any file to calculate the MD5 hash and click the Calculate button to calculate the MD5 hash of the file.

### *Tool 3: AES Encryption Package*

Advanced Encryption Package is most noteworthy for its flexibility; not only can you encrypt files for your own protection, but you can easily create 'self-decrypting' versions of your files that others can run without needing this or any software.

**Steps:**

Start > Programs > Advanced Encryption Package

The Register Advanced Encryption Package 2013 trial period window appears. Click Try Now!

The main window of Advanced Encryption Package appears

Select a sample file to encrypt. Click Encrypt. It will ask you to enter the password.

Type the password in the Password field, and again type the password in the Again field.

Click Encrypt Now! The encrypted sample file can be shown in the same location of the original file.

To decrypt the file, first select the encrypted file. Click Decrypt; it will prompt you to enter the password.

Click Decrypt Now!

***Tool 4: TrueCrypt***

TrueCrypt is a software system for establishing and maintaining an on-the-fly encrypted data storage device. On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

**Steps:**

Start > Programs > TrueCrypt

Select the desired volume to be encrypted and click Create Volume.

The TrueCrypt Volume Creation Wizard window appears. Select the Create an encrypted file container option. This option creates a virtual encrypted disk within a file. By default, the Create an encrypted file container option is selected. Click Next to proceed.

In the next step of the wizard, choose the type of volume. Select Standard TrueCrypt volume; this creates a normal TrueCrypt volume. Click Next to proceed.

In the next wizard, select Volume Location. Click Select File. Select desired location; provide File name and Save it.

After saving file, Volume Location wizard continues. Click Next to proceed. Encryption Options appear in wizard.

Select AES Encryption Algorithm and RIPEMD-160 Hash Algorithm and click Next.

In next step, Volume Size option appears. Specify the size of the TrueCrypt container to be 2 MB and click Next.

The Volume Password option appears. This is one of the most important steps. Read the information displayed in the wizard window on what is considered a good password carefully. Provide a good password in the first input field, re-type it in the Confirm field, and click Next.

The Volume Format option appears. Select FAT Filesystem, and set the cluster to Default. Move your mouse as randomly as possible within the Volume Creation Wizard window at least for 30 seconds.

Click Format.

After clicking Format volume creation begins. TrueCrypt will now create a file called MyVolume in the provided folder. This file depends on the TrueCrypt container. Depending on the size of the volume, the volume creation may take a long time. After it finishes, a dialog box appears. Click OK to close the dialog box.

You have successfully created a TrueCrypt volume (file container). In the TrueCrypt Volume Creation wizard window, click Exit.

To mount a volume, launch TrueCrypt. In the main window of TrueCrypt. click Select File.

In the file selector, browse to the container file, select the file, and click Open.

The file selector window disappears and returns to the main TrueCrypt window. Click Mount.

The Password prompt dialog window appears. Type the password (which you specified earlier for this volume) in the Password input field and click OK.

The Virtual disk has been successfully mounted. The virtual disk is entirely encrypted (including file names, allocation tables, tree space, etc.) and behaves like a real disk. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.

To dismount a volume, select the volume to dismount and click Dismount. The volume is dismounted.

***Tool 5: Cryptool***

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

**Steps:**

Start > Programs > CrypTool

The How to Start dialog box appears. Check Don't show this dialog again and click Close.

The main window of CrypTool appears

To encrypt the desired data, click the File option and select New from the menu bar.

Type a few lines in the opened Unnamed1 Notepad of CrypTool.

On the menu bar, select Encrypt/Decrypt, Symmetric (modern), and select any encrypting algorithm. Select the RC2 encrypting algorithm.

In the Key Entry: RC2 wizard, select Key length from the drop-down list. Enter the key using hexadecimal characters and click Encrypt.

RC2 encryption of Unnamed1 notepad will appear.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| CrypTool | **Encrypted Algorithm**: RC2 |
| | **Result:** Encrypted data for selected text |

***Tool 6: BCText Encoder***

BCTextEncoder simplifies encoding and decoding text data. Plaintext data is compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file.

**Steps:**

Double-click the BCTextEncoder.exe file. The main window of BCTextEncoder appears.

To encrypt the text, type the text in Clipboard (OR) select the secret data and put it to clipboard with Ctrl+V.

Click Encode. The Enter Password window will appear. Set the password and confirm the same password in the respective fields. Click OK.

The encoded text appears

To decrypt the data, you first clean the Decoded plain text clipboard. Click the Decode button

The Enter password for encoding text widow will appear. Enter the password in the Password held, and click OK.

Decoded plaintext appears

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| BCTText Encoder | **Result:** Encoding and Decoding text for selected data |

***Tool 7: ROHOS Disk Encryption***

ROHOS Disk Encryption creates hidden and password protected partitions in the computer or USB flash drive with megabytes of sensitive files and private data on your computer or USB drive. ROHOS Disk uses NIST-approved AES encryption algorithm, and 256 bit encryption key length. Encryption is automatic and on-the-fly.

**Steps:**

To install ROHOS Disk Encryption, double-click the rohos.exe file and follow the instructions

After installation, the ROHOS Get Ready Wizard window will appear. Specify the password to access the disk in the respective field. Click Next.

The Setup USB Key window appears. Read the information, and click Next.

The ROHOS Updates window appears. Click Finish. The encrypted disk is created successfully.

To decrypt the disk, click Disconnect.

After decrypting the disk, it will be displayed.

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Rohos Disk Encryption | **Result:** Successful connection of encrypted disk |

# Practical 8

**Aim: Study of Session Hijacking tools**

**Tools:** ZAP

***Tool 1: ZAP***

The OWASP Zed Attack Proxy (ZAP) is an easy-to-use integrated penetration testing too for finding vulnerabilities in web applications. Zed Attack Proxy (ZAP) is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pentester's toolbox. Its features include intercepting proxy, automated scanner, passive scanner, and spider. With the help of this tool:

Intercept and modify web traffic

Simulate a Trojan, which modifies a workstation's proxy server settings

**Steps:**

Start > Programs > ZAP

As soon as the program starts, it will prompt you with SSL Root CA certificate . Click Generate to continue.

In Options window, select Dynamic SSL certificates then click Generate to generate a certificate. Then click Save. Save the certificate in the default location of ZAP. If the certificate already exists, replace it with the new one. Click OK in the Options window.

Your Paros proxy server is now ready to intercept requests.

Launch any web browser. Change the Proxy Server settings on the web browser.

Check Use a proxy server for your LAN, type 127.0.0.1 in the Address, enter 8080 in the Port field, and click OK.

Click Set break on all requests and Set break on all responses to trap all the requests and responses from the browser.

Now navigate to a browser, and open www.bing.com. Start a search for "Cars".

Open ZAP, which shows first trapped incoming web traffic. Observe the first few lines of the trapped traffic in the trap windows, and keep clicking Submit and step to next request or response until you see cars in the GET request in the Break tab.

Now change the query text from Cars to Cakes in the GET request. Click Submit and step to next request or response.

Search for a title in the Response pane and replace Cakes with Cars. In the same Response pane, replace Cakes with Cars. Here we are changing the text Cakes to Cars ; the bing search shows Cars, whereas the results displayed are for Cakes.

Observe the Bing search web page displayed in the browser with search query as "Cakes".

| Tool/Utility | Information Collected/Objectives Achieved |
|---|---|
| Zed Attack Proxy | ▪ SSL certificate to hack into a website<br>▪ Redirecting the request made in Bing |

# Practical 9

**Aim: Study of Other Security Tools**

**Tools:** Snort, KFSensor.

***Tool 1: Snort***

Snort is an open source network intrusion prevention and detection system (IDS/IPS). An IPS is a network security appliance that monitors network and system activities for malicious activity. The main functions of IPSes are to identify malicious activity, log information about said activity, attempt to block/stop activity, & report activity. An IDS is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. It performs intrusion detection and attempt to stop detected possible incidents.

**Steps:**

Open snort.conf file (C:/Snort/etc/snort.conf) with notepad++

Replace all ipvar by var

Change HOME_NET value to IP address of the local host.

Change the EXTERNAL_NET value from any to !$HOME_NET.

Set RULE_PATH, PREPOC_RULE_PATH to point to C:\Snort\rules and C:\Snort\prepoc_rules respectively

Set WHITE_LIST_PATH and BLACK_LIST_PATH to C:\Snort\Rules

Set config logdir to point to the Snort log folder, ie C:\Snort\log

Configure the dynamicpreprocessor, dynamicengine, dynamicdetection directories

Comment out all preprocessor normalize lines

In step 7, keep the line include $RULE_PATH/local.rules and delete/comment all the include directories.

In C:\Snort\rules create text files local.rules black_list.rules white_list.rules . They all have the .rules extension

To test if Snort has been configured properly, run the command

‘snort -i 4 -c C:\Snort\etc\snort.conf -l C:\Snort\log -A console -T’

-i is the interface number we get when we run snort with the –W command

-c is the location of the .conf file

-l is the location of the log folder

-A console states to output to console immediately

-T means to test the configuration

-K ascii means to generate a log folder for each machine interaction over the network.

If test is successful it will show you a success message

Open local.rules file and specify the custom rules.

Here we are creating an alert that will be displayed when our machine detects a ping

```
alert icmp any any -> 172.16.151.0 any (msg:"ICMP packet detected!! ";sid:1000001;)
```

Now run snort without the –T switch and ping the machine running snort to generate the logs

‘snort -i 4 -c C:\Snort\etc\snort.conf -l C:\Snort\log -A console -T’

To install Snort as a service, we use the switch /service/install

```
C:\Snort\bin>snort /service /install -E -K ascii -c C:\Snort\etc\snort.conf -l C
:\Snort\log
```

To verify if the service has been configured properly

```
C:\Snort\bin>snort /Service /show
```

***Tool 2: KFSensor***

KFSensor is a Windows based honeypot Intrusion Detection System (IDS).

**Steps:**

Start > Programs > KFSensor

At the first-time launch of the KFSensor Set Up Wizard, click Next.

Check all the port classes to include and click Next.

Leave the domain name Held as default and click Next.

If you want to send KFSensor alerts by email, then specify the email address details and click Next.

Choose options for Denial of Service, Port activity, Proxy Emulation, and Network Protocol Analyzer and click Next.

Check the Install as system service option and click Next.

Click Finish to complete the Set Up wizard.

The KFSensor main window appears. It displays list of ID protocols, Visitor, and Received automatically when it starts. All the nodes in the left block crossed out with blue lines are the ports that are being used.

Start the command prompt. In the command prompt window, type netstat -an. This will display a list of listening ports.

Once KFSensor is configured, it behaves like a Honeypot

Start a MegaPing Port Scan or NMap scan targeting the KFSensor machine. The scan will start raising alerts which show up in red. When you click on them you can see more detailed information on a port basis or visitor basis

Right click any ID and click on event details