

UNIT - I:

UNIT - I: Introduction to Ethical Hacking and Legality

Purpose of Ethical Hacking, The Phases of Ethical Hacking, How to Be Ethical, Keeping It Legal. Cyber Laws in India, Gathering Target Information: Information-Gathering Methodology

Defining Ethical Hacking

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them. Also known as “white hats,” ethical hackers are security experts that perform these security assessments. With prior approval from the organization or owner of the IT asset they do helps to improve an organization’s security posture, the mission of ethical hacking is opposite from malicious hacking.

Purpose of Ethical Hacking

Ethical Hackers uses the same software tools and techniques as malicious hackers to find the security weakness in computer networks and systems. Then apply the necessary fix or patch to prevent the malicious hacker from gaining access to the data. This is a never-ending cycle as new weaknesses are constantly being discovered in computer systems and patches are created by the software vendors to mitigate the risk of attack.

Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and tool sets for defensive and protective purposes. They test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network.

The term *cracker* describes a hacker who uses their hacking skills and tool set for destructive or offensive purposes such as disseminating viruses or performing denial-of- service (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

Hackers can be divided into three groups:

White Hats Good guys, ethical hackers

Black Hats Bad guys, malicious hackers

Gray Hats Good or bad hacker; depends on the situation

Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who *now* 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. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity.

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 systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats 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 favor. For instance, if a weakness is discovered in a service offered by an investment bank, the hacker is doing the bank a favor by giving the bank a chance to rectify the vulnerability.

From a more controversial point of view, some people 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 behavior 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. Make sure you know the law and your legal liabilities when engaging in ethical hacking activity.

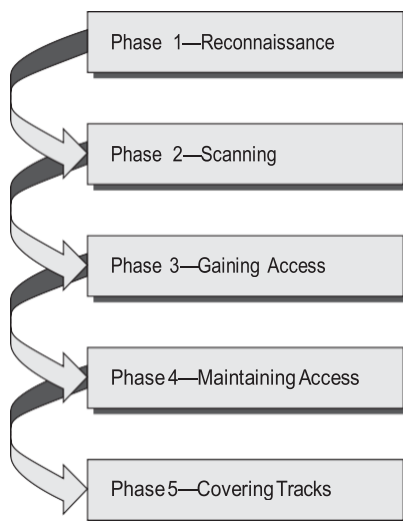
Many self-proclaimed ethical hackers are trying to break into the security field as consultants.

The difference between white hats and gray hats is that *permission* word. Although gray hats might have good intentions, without the correct permission they can no longer be considered ethical.

The Phases of Ethical Hacking

The process of ethical hacking can be broken down into five distinct phases. An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Figure 1.1 illustrates the five phases that hackers generally follow in hacking a computer system.

Figure 1.1 Phases of hacking



Phase 1: Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about a potential target without actively engaging with the target.

When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information on a topic. This process when used to gather information regarding an TOE is generally called *information gathering*. Social engineering and dumpster diving are also considered passive information-gathering methods.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing

network traffic is similar to building monitoring: a hacker watches the flow of data to see what time certain transactions take place and where the traffic is going. It let you see all the data that is transmitted on the network. Many times this includes user names and passwords and other sensitive data.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called *rattling the doorknobs*. Active reconnaissance can give a hacker an indication of security measures in place, but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.

Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase include

- Dialers
- Port scanners
- Internet Control Message Protocol (ICMP) scanners
- Ping sweeps
- Network mappers
- Simple Network Management Protocol (SNMP) sweepers
- Vulnerability scanners

Hackers are seeking any information that can help them perpetrate an attack on a target, such as the following:

- Computer names
- Operating system (OS)
- Installed software
- IP addresses
- User accounts

Phase 3: Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack- based buffer overflows, denial of service, and session hijacking. Gaining access is known in the hacker world as *owning* the system because once a system has been hacked, the hacker has control and can use that system as they wish.

Phase 4: Maintaining Access

Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks. Sometimes, hackers *harden* the system from other hackers or security personnel by securing their exclusive access with back doors, root kits, and Trojans. 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.

Phase 5: Covering Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include

- Steganography
- Using a tunneling protocol
- Altering log files

How to Be Ethical

Ethical hacking is usually conducted in a structured and organized manner, usually as part of a penetration test or security audit. The depth and breadth of the systems and applications to be tested are usually determined by the needs and concerns of the client. Many ethical hackers are members of a tiger team. A tiger team works together to perform a full-scale test covering all aspects of network, physical, and systems intrusion.

The ethical hacker must follow certain rules to ensure that all ethical and moral obligations are met. An ethical hacker must do the following:

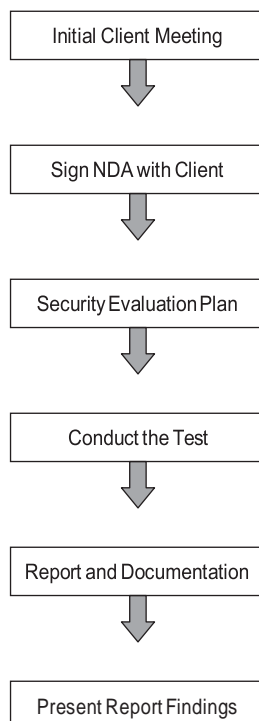
- n **Gain authorization** from the client and have a signed contract giving the tester permission to perform the test.
- n Maintain and follow a **nondisclosure agreement (NDA)** with the client in the case of confidential information disclosed during the test.

- n **Maintain confidentiality** when performing the test. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.
- n Perform the test up to but not beyond the **agreed-upon limits**. For example, DoS attacks should only be run as part of the test if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers as a result of the testing.

The following steps (shown in Figure 1.4) are a framework for performing a security audit of an organization and will help to ensure that the test is conducted in an organized, efficient, and ethical manner:

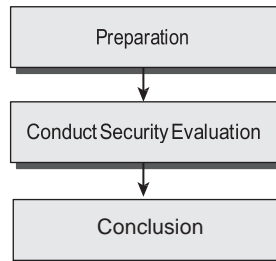
1. Talk to the client, and discuss the needs to be addressed during the testing.
2. Prepare and sign NDA documents with the client.
3. Organize an ethical hacking team, and prepare a schedule for testing.
4. Conduct the test.
5. Analyze the results of the testing, and prepare a report.
6. Present the report findings to the client.

Figure 1.4 Security audit steps



Performing a Penetration Test

Many ethical hackers acting in the role of security professionals use their skills to perform security evaluations or penetration tests. These tests and evaluations have three phases, generally ordered as follows:



Preparation This phase involves a formal agreement between the ethical hacker and the organization. This agreement should include the full scope of the test, the types of attacks (inside or outside) to be used, and the testing types: white, black, or gray box.

Conduct Security Evaluation During this phase, the tests are conducted, after which the tester prepares a formal report of vulnerabilities and other findings.

Conclusion The findings are presented to the organization in this phase, along with any recommendations to improve security.

Notice that the ethical hacker does not “fix” or patch any of the security holes they may find in the target of evaluation. This is a common misconception of performing security audits or penetration tests. The final goal or deliverable is really the findings of the test and an analysis of the associated risks in the final report and must be well documented by taking screenshots, copying the hacking tool output, or printing important log files.

Keeping It Legal

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization. Ethical hackers need to be judicious with their hacking skills and recognize the consequences of misusing those skills.

Computer crimes can be broadly categorized into two categories: crimes facilitated by a computer and crimes where the computer is the target. As globalization and computerization grew rapidly in India, cyber regulations

n
began to take shape. Every year, a startling number of cyber crimes are reported in India, and the problem is only getting worse. This is due to India's digital transformation, which has increased the pool of naive targets for cyber con artists. Year 2008 saw an amendment to India's Cyber Laws, often known as the Information Technology Act, which added cyber crimes relating to banking and financial operations.

What do you mean by Cyber Law?

The area of the legal system that is related to legal informatics and that regulates the electronic exchange of information, e-commerce, software, and information security is known as cyber law or Internet law. It is connected to legal informatics and electronic components like computers, software, hardware, and information systems. It covers a wide range of themes, including online privacy and freedom of expression, as well as access to and use of the Internet, which includes several subtopics.

Areas of Cyber Laws

There are seven areas where cyber law used most –



- **Fraud** – Cyber laws are essential to consumers' protection against online fraud. Legislation is created to stop online financial crimes, including credit card theft, identity theft, and others. Identity thieves may be charged as accomplices or as state criminals. They might also run into a victim-driven civil lawsuit. Cyber attorneys work to both defend and prosecute clients accused of online fraud.
- **Copyright** – Copyright violations have become easier because of the internet. Copyright infringement was all too common in the early days of online communication. To file a lawsuit to impose copyright protections, businesses and individuals both need lawyers. Cyber law defends people's and businesses' rights to make money off of their creative works in the domain of copyright violation.
- **Defamation** – Many employees use the internet to express themselves. Using the internet to spread untrue information might cross the line into defamation. Laws against defamation are civil laws that protect people from false public statements that might hurt someone's reputation or a business. Defamation legislation refers to when individuals use the internet to make claims that are illegal under civil laws.
- **Harassment and Stalking** – Criminal laws that prohibit stalking and harassment can occasionally be broken by online words. There is a violation of both civil and criminal statutes when someone repeatedly posts threatening comments about another individual online. When stalking occurs online or through other electronic communication, cyber lawyers both prosecute and defend the victim.
- **Freedom of Speech** – An essential component of internet law is freedom of speech. Freedom of speech rules also let people express their opinions, despite the fact that cybercrime laws prohibit specific acts online. The boundaries of free expression, particularly those imposed by laws against obscenity, must be discussed with clients by cyber attorneys. In cases where it is disputed whether a client's acts qualify as free speech, cyber lawyers may also stand up for their clients.
- **Trade secrets** – Cyber laws are frequently used by businesses doing online transactions to safeguard their trade secrets. For instance, the algorithms used by Google and other online search engines to generate search results are developed over a long period of time. They also devote a lot of work to creating other features, including search services for flights, intelligent assistance, and maps. Cyber security laws support these businesses in taking legal action when required to safeguard their trade secrets.
- **Contract and Employment** – Cyber law is used each time a user clicks a button acknowledging their agreement to a website's terms and conditions. Every website has terms and conditions relating to privacy issues in some way.

Cyber Laws in India

India has laws against cyber crime, which is any crime committed using technology and a computer as a tool. Citizens are prevented from sharing private information with strangers online by cyber crime laws. The IT Act 2000, which was passed and revised in 2008 to cover many types of offenses under Indian cyber law, has been in effect since the establishment of cyber laws in India.

- Internet law and regulation are collectively referred to as "cyber law" in this context. Cyber laws cover anything that has to do with, is connected to, or results from legal matters or any citizen activity in cyberspace.
- Legal issues relating to the usage of network information technology and devices' distributive, transactional, and communicative features are covered by cyber law. It covers all of the laws, regulations, and constitutional clauses that apply to networks and computers.

The Act defines the various types of cyber crime and the penalties associated with them.

Advantages of Cyber Laws

Following are the major advantages of cyber law

- Utilizing the legal framework, the Act provides, businesses can now conduct e-commerce.
- In the Act, digital signatures have been given legitimacy and authorization.
- It has made it possible for corporate organizations to issue digital signature certificates and operate as certifying authorities.
- It paves the way for e-government by enabling the government to publish alerts online.
- It allows businesses or organizations to electronically submit any forms, applications, or other documents to any offices, authorities, bodies, or agencies that are owned or managed by the appropriate government using any e-forms that may be specified by that government.
- The IT Act also addresses the crucial security concerns that are essential to the success of electronic transaction.

Historical Background

On October 17, 2000, the Information Technology Act of 2000 went into effect. This Act is applicable to all of India, and its provisions also apply to any violation or offense committed by any individual, regardless of nationality, even outside the Republic of India's territorial authority. Such an offense or contravention shall include a computer, computer system, or computer network located in India that is

subject to the provisions of this Act. The extraterritorial applicability of the provisions of the IT Act 2000 is provided by Section 1(2) read in conjunction with Section 75.

The Information Technology Act of 2000 in India has made an effort to include legal ideas found in other information technology-related laws that have already been passed in other nations as well as different information technology law-related guidelines. The Act recognizes electronic signatures and grants electronic contracts legal validity. Defamation (sending offensive communications), hacking, data theft, virus spreading, identity theft, pornography, child pornography, and cyber terrorism are now all considered crimes under this modern legislation.

Cyber laws cover the following statutes, rules, and guidelines.

- Information Technology Act, 2000
- Information Technology (Certifying Authorities) Rules, 2000
- Information Technology (Security Procedure) Rules, 2004
- Information Technology (Certifying Authority) Regulations, 2001
- The Indian Evidence Act, 1872
- The Bankers Books Evidence Act, 1891

The government has moved to expedite the process of updating the IT Act as a result of emerging technology, an explosion in digital business models, and a significant rise in cybercrime.

By providing the necessary inputs, the computer or data itself serves as the victim, the object of the crime, or a tool in committing another crime in a cybercrime. All of these criminal activities fall under the broad concept of "cybercrime."

Cyber law includes regulations on

- Online crimes
- Digital and electronic signatures
- Intangible assets
- Preserving the privacy of data

Gathering Information

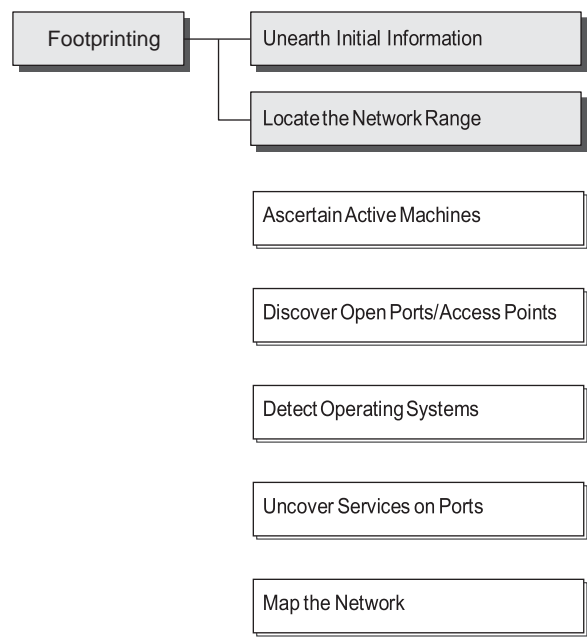
The first step of the hacking process is gathering information on a target. Information gathering, also known as *foot- printing*, is the process of gathering all available information about an organization. A hacker uses information-gathering techniques not only to help identify high- value targets (which is where the valuable information is located), but it also helps determine the best way to

gain access to the targets. This information can then be used to identify and eventually hack target systems. It also minimizing the chance of detection and assessing where to spend the most time and effort.

Information-Gathering Methodology

Foot printing is performed during the first two steps of unearthing initial information and locating the network range.

FIGURE 2 .1 Seven steps of pre attack



Foot printing

Foot printing is defined as the process of creating a blueprint or map of an organization’s network and systems. Foot printing begins by determining the target system, application, or physical location of the target. Once this information is known, specific information about the organization is gathered using non intrusive methods. For example, the organization’s own web page may provide a personnel directory or a list of employee bios

The information the hacker is looking for during the foot printing phase is anything that gives clues as to the network architecture, server, and application types where valuable data is stored. Before an attack or exploit can be launched,

the operating system and version as well as application types must be uncovered so the most effective attack can be launched against the target. Here are some of the pieces of information to be gathered about a target during foot printing:

- Domain name
- Network blocks
- Network services and applications
- System architecture
- Intrusion detection system
- Authentication mechanisms
- Specific IP addresses
- Access control mechanisms
- Phone numbers
- Contact addresses

Foot printing Tools

By using these foot printing tools, a hacker can gain some basic information on, or “footprint,” about the target which minimizes the chance of detection as fewer hacking attempts can be made by using the right tool for the job. By first foot printing the target, a hacker can eliminate tools that will not work against the target systems or network. For example, if a graphics design firm uses all Macintosh computers, then all hacking software that targets Windows systems can be eliminated.

Some of the common tools used for foot printing and information gathering are as follows:

- Domain name lookup
- Whois
- NSlookup
- Sam Spade

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 using other lookup web tools are forms of open source foot printing. Most of this information is fairly easy to get and legal to obtain.

Foot printing a Target

Foot printing is part of the preparatory preattack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of revealing system vulnerabilities, remote access capabilities, its ports and services, and any specific aspects of its security and identify the ease with which they can be exploited. belong to.

Using Google to Gather Information

A hacker may also do a Google search or a Yahoo! People search to locate information about employees or the organization itself. The use of the Google search engine to retrieve information has been termed Google hacking. Go to <http://groups.google.com> to search the Google newsgroups. The following commands can be used to have the Google search engine gather target information:

site Searches a specific website or domain. Supply the website you want to search after the colon.

filetype Searches only within the text of a particular type of file. Supply the file type you want to search after the colon. Don't include a period before the file extension.

link Searches within hyperlinks for a search term and identifies linked pages.

cache Identifies the version of a web page. Supply the URL of the site 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 to locate certain types of vulnerable web applications:

```
INURL:["parameter=""] with FILETYPE:[ext] and INURL:[script name]
```

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.

Understanding 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 user names, computer names, and IP addresses of potential target systems.

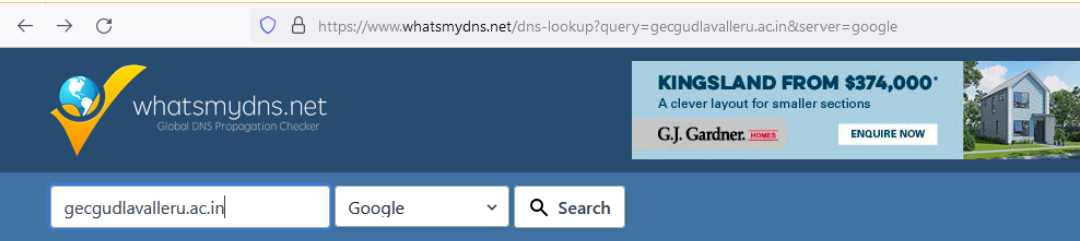
NSlookup, DNSstuff, the American Registry for Internet Numbers (ARIN), and Whois can all be used to gain information that can then be used to perform DNS enumeration.

NSlookup and DNS

NSlookup (see Figure 2.2) 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, you can discover the IP address of the mail server.

FIGURE 2 . 2 NSlookup



ANY Records

ANY records for **gecgudlavalleru.ac.in**:

Record	Type	Value	TTL
gecgudlavalleru.ac.in	A	119.18.54.49	14400
gecgudlavalleru.ac.in	MX	0 mail.gecgudlavalleru.ac.in.	14400
gecgudlavalleru.ac.in	NS	cns6001.hostgator.in.	21600
gecgudlavalleru.ac.in	NS	cns6002.hostgator.in.	21600
gecgudlavalleru.ac.in	SOA	cns6001.hostgator.in. root.cs3001.hostgator.in. 2023072505 86400 7200 3600000 86400	21600
gecgudlavalleru.ac.in	TXT	"v=spf1 a mx include:websitewelcome.com ~all"	14400

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 www.whatsmydns.net, and you can do a DNS record search.


FIGURE 2.3 DNS record search

```
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>nslookup www.gecgudlavalleru.ac.in
Server: Unknown
Address: 192.168.43.1

Non-authoritative answer:
Name:   gecgudlavalleru.ac.in
Address: 64:ff9b::7712:3631
        119.18.54.49
Aliases: www.gecgudlavalleru.ac.in
```

This search reveals all the alias records and the IP address of the web server. You can even discover all the name servers and associated IP addresses.



Enter Keywords or IP Address...

Search

ABOUT

MY IP

IP LOOKUP

HIDE MY IP

VPNS

TOOLS

My IP Address is:

IPv4: 42.106.185.149

IPv6: Not detected

My IP Information:

ISP: Vodafone Idea Ltd

City: Namagiripettai

Region: Tamil Nadu

Country: India

```
Command Prompt
C:\Users\toshiba>ipconfig
Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:
    Connection-specific DNS Suffix  . :
    IPv6 Address . . . . . : 2402:3a80:1953:a289:1
    Temporary IPv6 Address . . . . : 2402:3a80:1953:a289:e
    Link-local IPv6 Address . . . . : fe80::18e6:6ae9:bci:e
    IPv4 Address . . . . . : 192.168.43.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::8031:e0ff:feb1:
    192.168.43.1

Tunnel adapter isatap.{26C9BF93-2A5D-4873-B220-D46D6F199B66}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\toshiba>
```




Understanding Whois and ARIN Lookups

Whois tool identifies who has registered domain names used for email or websites. A uniform resource locator (URL), such as www.Microsoft.com, contains the domain name (Microsoft.com) and a hostname 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.

The Whois tool queries the registration database to retrieve contact information about the individual or organization that holds a domain registration.

ARIN is a database that includes such information as the owners of static IP addresses. The ARIN database can be queried using the Whois tool, such as the one located at www.arin.net. Notice that addresses, emails, and contact information are all contained in this Whois search.

FIGURE 2.4 ARIN output

https://search.arin.net/rdap/?query=142.251.46.174

Your IPv6 address is 2402:3a80:1953:a289:18e6:6ae9:bct1:e1c4

IP Addresses & ASNs Policy & Participation Reference & Tools

ARIN Whois/RDAP

142.251.46.174

» Search www.arin.net instead

"142.251.46.174"

Network: NET-142-250-0-0-1

Source Registry	ARIN
Net Range	142.250.0.0 - 142.251.255.255
CIDR	142.250.0.0/15
Name	GOOGLE
Handle	NET-142-250-0-0-1
Parent	NET-142-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS15169

https://www.nslookup.io/domains/google.com/dns-records/

DNS course for developers — \$90 off

Nslookup.io

google.com

DNS records for google.com

Cloudflare Google DNS OpenDNS Authoritative Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve this period, Cloudflare will update its cache by querying one of the authoritative na

A records

IPv4 address	Revalidate in
> 142.251.46.174	3m 13s

AAAA records

IPv6 address	Revalidate in
> 2607:f8b0:4005:812::200e	3m 53s

Analyzing Whois Output

Listing 2.1

WHOIS OUTPUT

https://www.whois.com/whois/gecgudlavalлерu.ac.in

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS

gecgudlavalлерu.ac.in

Updated 6 minutes ago

Domain Information

Domain:	gecgudlavalлерu.ac.in
Registrar:	ERNET India
Registered On:	2004-10-27
Expires On:	2027-10-27
Updated On:	2021-07-27
Status:	OK
Name Servers:	cns6001.hostgator.in cns6002.hostgator.in

Registrant Contact

State:	Andhra Pradesh
Country:	IN
Email:	Please contact the Registrar listed above

Raw Whois Data

Domain Name: gecgudlavalлерu.ac.in

Registry Domain ID: D12836-IN

Registrar WHOIS Server:

Registrar URL: http://www.ernet.in

Updated Date: 2021-07-27T05:09:21Z

Creation Date: 2004-10-27T15:14:46Z

Registry Expiry Date: 2027-10-27T15:14:46Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: ok <http://www.icann.org/epp#OK>
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Andhra Pradesh
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY

Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: cns6001.hostgator.in
Name Server: cns6002.hostgator.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of WHOIS database: 2023-07-29T06:02:56Z <<<

Finding the Address Range of the Network

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.

Identifying Types of DNS Records

The following list describes the common DNS record types and their use:

A (Address) Maps a hostname 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 hostnames

NS (Name Server) Identifies other name servers for the domain

Using Traceroute in Foot printing

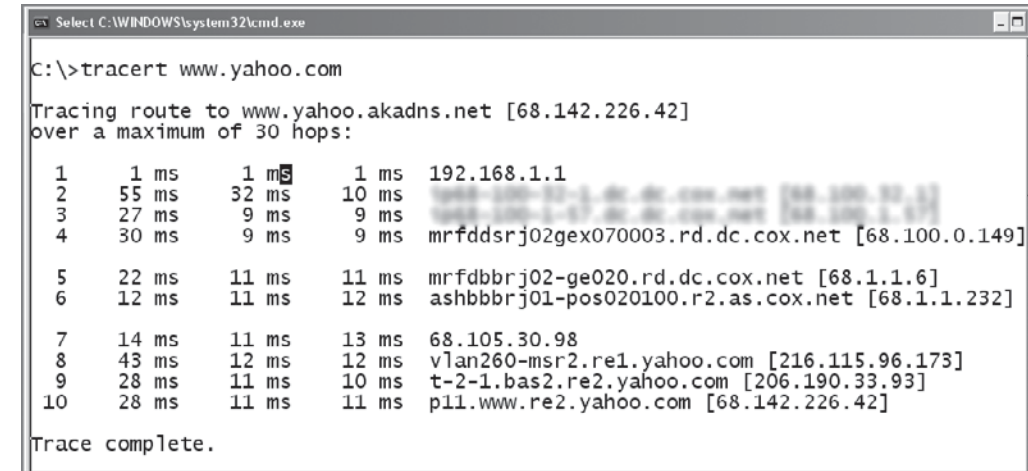
Traceroute is a packet-tracking tool that is available for most operating systems. It operates by sending an Internet Control Message Protocol (ICMP) echo to each hop (router or gateway) along the path, until the destination address is

reached. When ICMP messages are sent back from the router, the time to live (TTL) is decremented by one for each router along the 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) when it encounters a firewall or a packet-filtering router. Although a firewall stops the trace- route tool from discovering internal hosts on the network, it can alert an ethical hacker to the presence of a firewall; then, techniques for bypassing the firewall can be used.

Sam Spade and many other hacking tools include a version of traceroute. The Windows operating systems use the syntax `tracert hostname` to perform a traceroute. Figure 2.5 is an example of traceroute output for a trace of `www.yahoo.com`.

FIGURE 2.5 Traceroute output for `www.yahoo.com`



Notice in Figure 2.5 that the message first encounters the outbound ISP to reach the Yahoo! web server, and that the server’s IP address is revealed as 68.142.226.42. Knowing this IP address enables the ethical hacker to perform additional scanning on that host during the scanning phase of the attack.

The `tracert` command identifies routers located en route to the destination’s network. Because routers are generally named according to their physical location, `tracert` results help you locate these devices.

```
Command Prompt - tracert www.gecgudlavaluru.ac.in
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\toshiba>tracert www.gecgudlavaluru.ac.in

Tracing route to www.gecgudlavaluru.ac.in [119.18.54.4]
over a maximum of 30 hops:
  0  5 ms  1 ms  1 ms  192.168.43.1
  1  48 ms  28 ms  26 ms  172.21.4.62
  2  *  *  *  Request timed out.
  3  *  *  *  Request timed out.
  4  *  *  *  Request timed out.
  5  *  *  *  Request timed out.
  6  *  *  *  Request timed out.
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  *  *  *  Request timed out.
 10  *  *  *  Request timed out.
 11  *  *  *  Request timed out.
 12  *  *  *  Request timed out.
 13  *  *  *  Request timed out.
 14  *  *  *  Request timed out.
 15  87 ms  59 ms  66 ms  119.18.54.49

Trace complete.
```

```
Command Prompt
C:\Users\toshiba>tracert www.google.co.in

Tracing route to www.google.co.in [2404:6800:4009:821::2003]
over a maximum of 30 hops:
  0  2 ms  1 ms  1 ms  2402:3a80:1953:a289::e5
  1  56 ms  22 ms  41 ms  2402:8100:12:5:2000::27f
  2  *  *  *  Request timed out.
  3  *  *  *  Request timed out.
  4  86 ms  27 ms  28 ms  2402:8100:12:5:2000::37f
  5  44 ms  40 ms  47 ms  2400:5200:2c15:1::22
  6  49 ms  39 ms  46 ms  2001:4860:1:1::6eb
  7  56 ms  44 ms  54 ms  2001:4860:1:1::150e
  8  46 ms  39 ms  48 ms  2404:6800:8139::1
  9  44 ms  54 ms  49 ms  2001:4860:0:1::55aa
 10  21 ms  36 ms  49 ms  2001:4860:0:133f::9
 11  74 ms  68 ms  66 ms  2001:4860:9:4002:d931
 12  *  *  *  Request timed out.
 13  55 ms  60 ms  59 ms  2001:4860:0:1::2a47
 14  70 ms  59 ms  60 ms  bom12s11-in-x03.1e100.net [2404:6800:4009:821::2003]

Trace complete.
```

Understanding Email Tracking

Email-tracking programs allow the sender of an email to know whether the recipient reads, forwards, modifies, or deletes an email. Most email-tracking programs work by appending a domain name to the email address, such as readnotify.com. A single-pixel graphic file that isn't noticeable to the recipient is attached to the email. Then, when an action is performed on the email, this graphic file connects back to the server and notifies the sender of the action.

Understanding Web Spiders

Spammers and anyone else interested in collecting email 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 and then copies them into a list. These addresses are then added to a database and may be used later to send unsolicited emails.

Web spiders can 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.

Jack of All Trades

Sam Spade runs on all versions of Windows starting with Windows 95 and several features that are specific to the detection of spam and sites that relay spam. This software integrates the capabilities found in ping, traceroute, time, whois, nslookup, finger, DIG, a packet sniffer, a port scanner, a scripting language, and more, all with a nice GUI to boot.

