Introduction to Ethical Hacking, Ethics and Legality

- Prepared by Dr. A.Haritha

Contents-Part-1

UNDERSTANDING PURPOSE OF ETHICAL HACKING

- Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for **defensive and protective purposes.**
- T**est their network** and systems security for vulnerabilities using the **same tools** that a hacker might use to compromise the network.
- Any computer professional can learn the skills of ethical hacking.

•The term **cracker** describes a hacker who uses their **hacking skills and toolset 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.

HACKER TYPES

- **White Hat:** hacking skills for **defensive purposes**. locate weaknesses **and implement countermeasures**. White hats are those who hack with **permission from the data owner**. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a **malicious hacker who cannot be trusted.**

- **Black:** Having gained **unauthorized access**, black-hat hackers
destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

- **Grey Hat:** work offensively or defensively, depending on the situation.
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. difference between white hats and gray hats is that ***permission word***

Color of the Hat…

The 6 Different Types of Hackers

Black Hat Hackers: Bad hackers who use cyber attacks to gain money or to achieve another agenda.

These hackers penetrate systems without permission to exploit known or zero-day vulnerabilities.

White Hat Hackers: Ethical hackers who protect your systems from black hat hackers.

Penetrate the system with the owner's permission to find and fix security vulnerabilities and mitigate cyberattacks.

Grey Hat Hackers: Hackers who cruise the line between being good and bad. Penetrate systems without permission but typically don't cause harm.

Draw attention to vulnerabilities and often offer a solution to patch them by charging fees.

Red Hat Hackers: Hackers who use cyber attacks to attack black hat hackers.

Their intentions are noble, but these hackers often take unethical or illegal routes to take down bad hackers.

Blue Hat Hackers: Hackers who seek to take personal revenge, or outside security professionals that companies hire to test new software & other products to find vulnerabilities prior to release.

Green Hat Hackers: Newbie hackers who are learning to hack.

They're often not aware of the consequences of their actions & cause unintentional damage without knowing how to fix it.

WHAT DO ETHICAL HACKERS DO

- They do the same as cracker.
- they're trying to determine **what an intruder can see on a targeted network** and what the hacker can do with that information.
- **Pen Test:** This process of testing the security of a system or network is known as a ***penetration test.***
- doing this doesn't usually involve a mysterious leap of hackerly brilliance, but rather persistence and the **dogged repetition of a handful of fairly well-known tricks** that exploit common weaknesses in the security of target systems.
- A pen test is no more than just performing those same steps with the same tools used by a malicious hacker to see what data could be exposed using **hacking tools and techniques**.
- When hired, an ethical hacker asks the organization **what is to be protected, from whom, and what resources the company** is willing to expend in order to gain protection.
- A **penetration test plan** can then be built around the data that needs to be protected and potential risks. **Documenting the results** of various tests is critical in producing the end product of the **pen test: pen test report**.
- Taking **screenshots of potentially valuable information** or **saving log files** is critical to presenting the findings to a client in a pen test report.
- The pen test report is a compilation of all the **potential risks** in a computer or system.

GOALS ATTACKERS TRY TO ACHIEVE

- Breach computer system security
- Security consists of.
  - Confidentiality
  - Authenticity
  - Integrity
  - Availability
- **Perform DOS**: hacker attacks the ***Availability elements of systems and network.*** main purpose is to use up system resources or bandwidth.
- A flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to legitimate users of the system
- **Information Theft:** stealing passwords or other data as it travels in clear text across trusted networks, is a ***Confidentiality attack, because it allows someone other than the intended recipient to gain access to the data.***
  This theft isn't limited to data on network servers. Laptops, disks, and backup tapes are all at risk. **Company owned devices** r loaded with confidential information and can give a hacker information about the security measures in place at an organization.

GOALS ATTACKERS TRY TO ACHIEVE…

- ***Bit-flipping :*** *are considered* ***integrity attacks*** *because the data may have been* tampered with in transit or at rest on computer systems;

- System admins are unable to verify the data is **as the sender intended it**. A bit-flipping attack is an attack on a **cryptographic cipher**: the attacker changes the cipher text in such a way as to result in a **predictable change of the plain text**, although the attacker doesn't learn the plain text itself.

- This type of attack isn't directed against the cipher but against a message or series of messages. In the extreme, this can become a DoS attack against all messages on a particular channel using that cipher. The attack is especially dangerous when the attacker knows the format of the message.

- When bit-flipping attack is applied to **digital signatures** attacker may be able to change a promissory note stating "I owe you $10.00" into one stating "I owe you $10,000."

GOALS ATTACKERS TRY TO ACHIEVE…

- ***MAC address spoofing*** *:*
- *is an* ***authentication attack*** *because it allows an* ***unauthorized*** **device to connect to the network when** Media Access Control (MAC) filtering is in place, such as on a wireless network.
- By spoofing the MAC address of a legitimate wireless station, an intruder can take on that station's identity and use the network.

ETHICAL HACKERS SKILL SET

- knowledgeable about **computer programming, networking, and operating systems**.
- In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement.
- **Patience, persistence, and immense perseverance** are important qualities for ethical hackers because of the **length of time and level of concentration** required for most attacks to pay off.
- **Networking, web programming, and database** skills are all useful in performing ethical hacking and vulnerability testing.
- an ethical hacker will act as part of a **"tiger team"** who has been hired to test network and computer systems and find vulnerabilities.
- In this case, each member of the team will have distinct specialties, and the ethical hacker may need more specialized skills in one area of **computer systems and networking**. Most ethical hackers are knowledgeable about security areas and related issues but don't necessarily have a strong command of the countermeasures that can prevent attacks.

ETHICAL HACKING TERMINOLOGY

- **Threat:**
  An **environment or situation** that could lead to a **potential breach of security**.
  Ethical hackers look for and prioritize threats when performing a security analysis.
  Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.
- **Exploit:**
  A **piece of software or technology** that takes advantage of a **bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system**.
  Malicious hackers are looking for exploits in computer systems to open the door to an initial attack.
  Most exploits are **small strings of computer code** that, when executed on a system, expose vulnerability.
  Experienced hackers create their own exploits, but it is not necessary to have any programming skills to be an ethical hacker as many
  hacking software programs have **ready-made exploits** that can be launched against a computer system or network. An exploit is a defined way to breach the security of an IT system through a vulnerability.

ETHICAL HACKING TERMINOLOGY

- Vulnerability:
  The existence of a **software flaw, logic design, or implementation error** that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.

- Exploit code is written to target a vulnerability and cause a fault in the system in order to retrieve valuable data.

ETHICAL HACKING TERMINOLOGY

- **Target of Evaluation:**

Target of Evaluation (TOE) A system, program, or network that is the subject of a security analysis or attack.

Ethical hackers are usually concerned with **high-value TOEs**,systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

- **Attack:**

An attack occurs when a system is compromised based on a vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to prevent an attack.

ETHICAL HACKING TERMINOLOGY

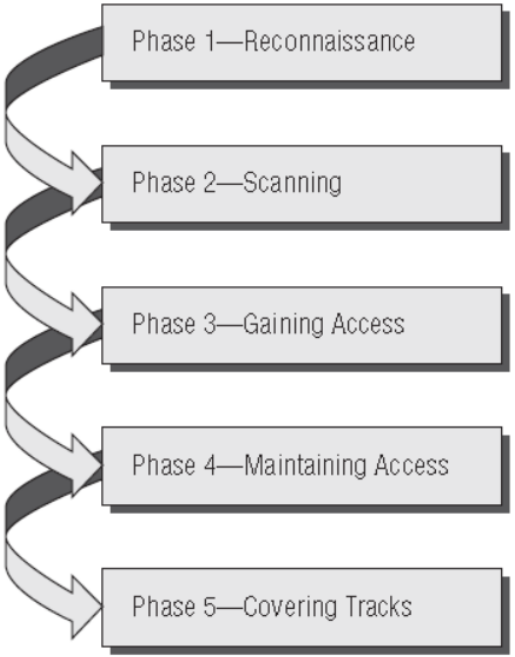
- **Remote : The exploit is sent over a network and exploits security vulnerabilities without** any prior access to the vulnerable system. Hacking attacks against corporate computer systems or networks initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term *hacker, but in reality most attacks are* in the next category..
- **Local : The exploit is delivered directly to the computer system or network, which requires** prior access to the vulnerable system to increase privileges.
- Information security policies should be created in such a way that only those who need access to information should be allowed access and they should **have the lowest level of access to perform their job function.**
- These concepts are commonly referred as **"need to know" and "least privilege**" and, when used properly, would prevent local exploits.
- Most hacking attempts occur from within an organization and are perpetuated by employees, contractors, or others in a trusted position.
- In order for an insider to launch an attack, they must have higher privileges than necessary based on the concept of "need to know." This can be accomplished by **privilege escalation or weak security safeguards.**

Phases in Ethical hacking

- Ethical Hacker follows the similar steps as a malicious hacker.
- The steps to gain main entry in computing system are similar to those of malicious hackers.

Reconnaissance

- ***Passive, Active***
- ***Information gathering***
- ***Social Engineering***
- ***Dumpster diving***
- ***Sniffing n/w***
- ***TOE***
- ***Web server and OS version company is using***
- ***Active-rattling the door knobs***



2. Scanning

- It involves taking the info collected during reconnaissance and use it to examine the network.

Tools employed

- ***Dialers, Port Scanners, ICMP Scanners,***
- ***Ping Sweeps***
- ***Network Mappers***
- ***Vulnerability Scanners***

Hackers are seeking any information that can help them perpetrate an attack on a target such as the following: Computer names,(OS),Installed software, IP addresses User accounts

3. Gaining Access

- The real hacking takes place.

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 stackbased 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.

3. 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 backdoors, rootkits, 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*.

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

Identifying the type of hacking Technologies

- Many tools exist to find the vulnerabilities, running exploits and compromising the system.
- Once vulnerability is found-trojans, malwares, backdoors, exploits
- **Buffer overflows and SQL injection** are the other methods to gain access to the system.- application servers that contain databases of information
- Areas where weakness can be exploited:
  - **Operating system:** many admins install **with default settings-** vulnerabilities unpatched
  - **Applications: Not tested to vulnerabilities while writing code**,; **feature driven-develop** robust applications in short time-deadlines..
  - **Shrink-Wrap code: off the shelf programs** come with extra features that common user is unaware of- can be used to exploit the system. **Macros in** MS Word

    Mis configurations: Systems can also be misconfigured or left at **the lowest common security settings** to increase ease of use for the user; this may result in vulnerability and an attack.

Identifying the type of ethical Hacks

- In the initial discussion with the client, one of the questions that should be asked is whether **there are any specific areas of concern**, such as wireless networks or social engineering.
- This enables the ethical hacker to **customize the test to be performed** to the needs of the client.
- Otherwise, **security audits** should include attempts to access data from all of the following methods..
- ***Remote Network***
- ***Remote Dial up Network***
- ***Local Network***
- ***Stolen Equipment***
- ***Social Engineering***
- ***Physical Entry***

Remote Network

- **Remote Network A remote network hack attempts to simulate an intruder launching an attack over the Internet**.
- The ethical hacker tries to break or find vulnerability in the outside defenses of the network, such as **firewall, proxy, or router vulnerabilities**.
- **The Internet is thought to be the most common hacking vehicle**, while in reality most organizations have strengthened their security defenses sufficient to prevent hacking from the public network.

Remote Dial up Network

- A remote dial-up network hack tries to simulate an intruder launching an attack against the **client's modem pools**.
- *War dialing is the process of* ***repetitive*** **dialing** to find an open system and is an example of such an attack.
- Many organizations have replaced **dial-in connections with dedicated Internet connections** so this method is less relevant than it once was in the past.

Local Network

- A local area network (LAN) hack **simulates someone with physical access** gaining additional unauthorized access using the local network.

- The ethical hacker must gain **direct access to the local network** in order to launch this type of attack.
- **Wireless LANs (WLANs)** fall in this category and have added an entirely new avenue of attack as radio waves travel through building structures.

- Because the WLAN signal can be **identified and captured outside the building, hackers no longer have to gain physical access** to the building and network to perform an attack on the LAN.
- Additionally, the huge growth of WLANs has made this an increasing source of attack and potential risk to many organizations.

Stolen Equipment

- A stolen-equipment hack simulates theft of a critical information resource such as **a laptop owned by an employee.**
- Information such as **usernames, passwords, security settings, and encryption** types can be gained by stealing a laptop.
- This is usually a commonly overlooked area by many organizations. Once a hacker has **access to a laptop authorized in the security domain**, a lot of information, such as security configuration, can be gathered.
- Many times laptops disappear and are not reported quickly enough to allow the security **administrator to lock that device out of the network**.

Social Engineering

- A social-engineering attack checks the **security and integrity of the organization's employees** by using the telephone or face-to-face communication to gather information for use in an attack.
- Social-engineering attacks can be used to **acquire usernames, passwords, or other organizational security measures.**
- Social-engineering scenarios usually consist of a hacker **calling the help desk and talking the help desk employee** into giving out confidential security information.

Physical Entry

Physical Entry A physical-entry attack attempts to compromise the organization's physical premises.
An ethical hacker who gains physical access can **plant viruses, Trojans, root kits, or hardware key loggers (physical device used to record keystrokes) directly** on systems in the target network.

- Additionally, confidential documents that are **not stored in a secure location** can be gathered by the hacker.
- Lastly, physical access to the building would allow a hacker **to plant a rogue device such as a wireless access point on the network.**
- These devices could then be used by the hacker to access the LAN from a remote location.

UNDERSTANDING TESTING TYPES

- **Black-box testing:**
- involves performing a **security evaluation and testing with no prior knowledge of the network infrastructure or system to be tested.**

- Testing **simulates an attack by a malicious hacker** outside the organization's security perimeter.
- Black-box testing can take the longest amount of time **and most effort as no information is given** to the testing team.
- Therefore, the information-gathering, reconnaissance, and scanning phases will take a great deal of time.
- The **advantage** of this type of testing is that it most closely **simulates a real malicious attacker's methods and results.**
- The **disadvantages** are primarily the **amount of time and consequently additional cost incurred by the testing team.**

White Box testing

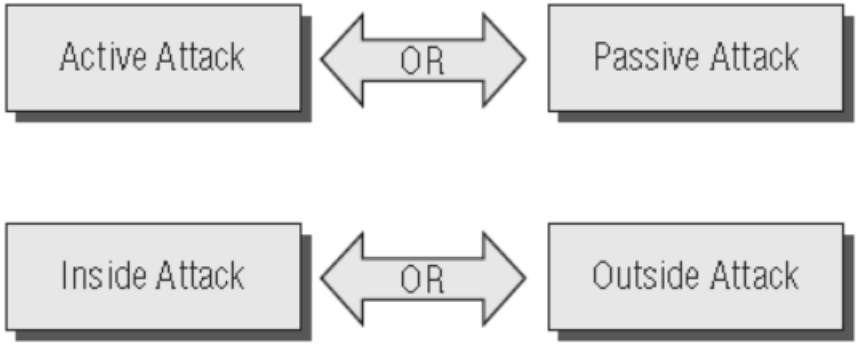
White-box testing

- involves performing a security evaluation and testing with **complete knowledge of the network infrastructure** such as a network administrator would have.
- This testing is **much faster than the other two methods as the ethical hacker can jump right to the attack phase, thus bypassing all the information-gathering, reconnaissance, and scanning phases**.
- Many security audits consist of white-box testing to avoid the additional time and expense of black-box testing.

GRAY-BOX TESTING

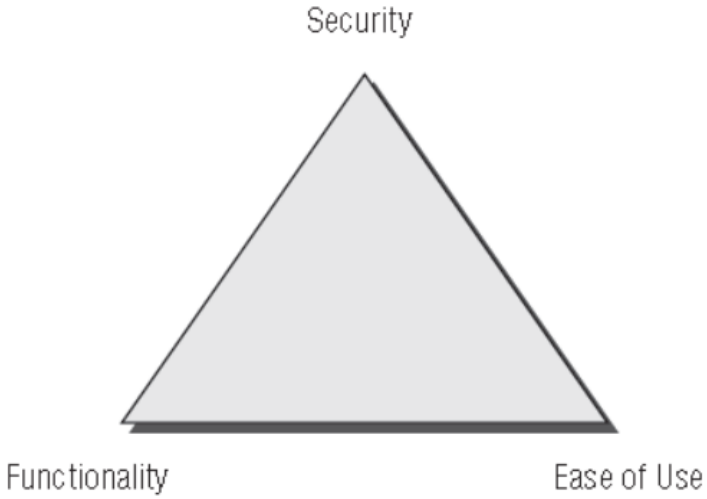
- Gray-box testing involves performing a security evaluation and **testing internally.**
- Testing examines the extent of **access by insiders** within the network.
- The purpose of this test is to simulate the most common form of attack, those that are initiated from within the network.
- The idea is to test or **audit the level of access given to employees or contractors and see if those privileges can be escalated to a higher level.**

Types of attacks



Security, Functionality and Ease of Use Triangle

Security, functionality, and ease of use triangle



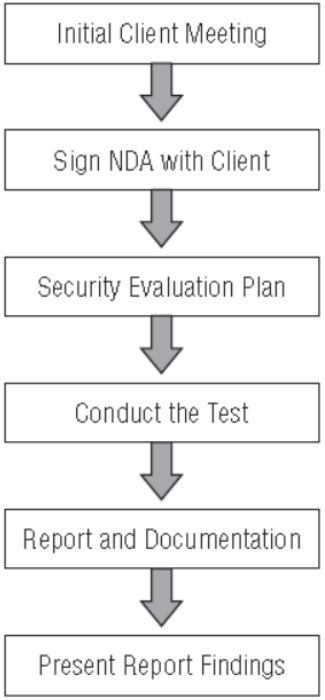
How to be ethical

- Conducted in structural and organized manner.
- Usually done as a part of Pen test or security audit

Ethical Hacker must do the following

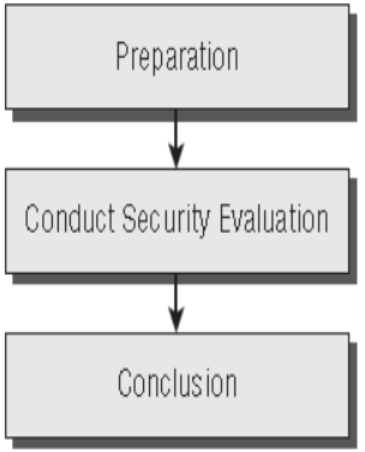
- Gain **authorization from the client and have a signed contract giving the tester permission to perform the test.**
- Maintain and follow a **nondisclosure agreement** (NDA) with the client in the case of confidential information disclosed during the test.
- **Maintain confidentiality** when performing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

Security audit steps



PERFORMING A PENETRATION TEST

- **Preparation: 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.

- 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

Performing a penetration test

- The ethical hacker usually **does not perform any patching or implementation of countermeasures.**
- The final goal or deliverable is really **the findings of the test and an analysis of the associated risks**. The test is what leads to the findings in the final report and must be well documented.
- Contrary to popular belief**, ethical hackers performing a penetration test must be very organized and efficient, and they must document every finding by taking screenshots, copying the hacking tool output, or printing important log files**.
- Ethical hackers must be very professional and present a well-documented report to be taken seriously in their profession.
- "Performing a Penetration Test."

KEEPING IT LEGAL

- 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.**

HACKTIVISM

- *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, and implementing 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.”

Cybersecurity Enhancement Act and spy Act

- The Cyber Security Enhancement Act of **2002 mandates life sentences for hackers who "recklessly" endanger the lives of others.**

- Malicious hackers who create a **life-threatening situation by attacking computer networks** for transportation systems, power companies, or other public services or utilities can be prosecuted under this law.

SPY ACT

- **The Securely Protect Yourself Against Cyber Trespass Act of 2007 (SPY ACT)** deals with the use of spyware on computer systems and **essentially prohibits the following**:

- Taking **remote control** of a computer when you have not been authorized to do so
- (commonly known as **spamming**)
- **Redirecting a web browser to another site** that is not authorized by the user
- Displaying advertisements that cause the user to have to close out of the web browser (**pop-up windows**)
- Collecting **personal information using keystroke logging**
- Changing the **default web page of the browser**
- Misleading users so they click on a web page link or duplicating a similar web page to mislead a user
- The SPY ACT is important in that it starts to recognize annoying pop-ups and spam as more than mere annoyances and as real hacking attempts. The SPY ACT lays a foundation for prosecuting hackers that use spam, pop-ups, and links in emails.

18 USC §1029 AND 1030

- The U.S. Code categorizes and defines the laws of the United States by titles.
- **Title 18 details "Crimes and Criminal Procedure."**

- **Section 1029, "Fraud and related activity in connection with access devices,"** states that if you produce, sell, or use counterfeit access devices or telecommunications instruments with intent to commit fraud and obtain services or products with a value over $1,000, you have broken the law.

- Section 1029 criminalizes the misuse of computer passwords and other access devices such as token cards.

- **Section 1030, "Fraud and related activity in connection with computers,"** prohibits accessing protected computers without permission and causing damage.

- This statute criminalizes the spreading of viruses and worms and breaking into computer systems by unauthorized individuals.

US STATE LAWS

- In addition to federal laws, many states have their own laws associated with hacking and auditing computer networks and systems.

- When performing penetration testing, review the applicable state laws to ensure that you are staying on the right side of the law.

- In many cases, **a signed testing contract and NDA will suffice** as to the intent and nature of the testing.
- The **National Security Institute** has a website **listing all the state laws applicable to computer crimes.**
- The URL is http://nsi.org/Library/Compsec/computerlaw/statelaws.html

Federal Managers Financial Integrity act

- The Federal Managers Financial Integrity Act of 1982 (FMFIA) is basically a **responsibility act to ensure that those managing financial accounts are doing so with the utmost responsibility and are ensuring the protection of the assets.**
- This description can be construed to encompass all measurable safeguards to protect the assets from a hacking attempt.
- The act essentially ensures that **Funds, property, and other assets are safeguarded against waste, unauthorized use, or misappropriation**.

- Costs are in compliance with applicable laws.

- The FMFIA is important to ethical hacking as it places the responsibility on an organization for the appropriate use of funds and other assets. Consequently, this **law requires management to be responsible for the security of the organization** and to ensure the appropriate safeguards against hacking attacks.

FREEDOM OF INFORMATION ACT(FOIA)

- The Freedom of Information Act (5 USC 552), or FoIA, makes many pieces of **information and documents about organizations public.**
- Most **records and government documents** can be obtained via the FoIA.
- Any information gathered using this act **is fair game** when you are performing reconnaissance and information gathering about a potential target.

Federal Information Security Management Act (FISMA)

- The Federal Information Security Management Act (FISMA) basically gives ethical hackers **the power to do the types of testing they perform** and makes it a mandatory requirement for government agencies.

- FISMA requires that each federal agency develop, document, and implement an agency wide **information security program** to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

- The information security program must include the following:

- **Periodic assessments of the risk and magnitude of the harm** that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency

Federal Information Security Management Act (FISMA)

- **Policies and procedures that are based on risk assessments**, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system

- **Subordinate plans** for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate

- **Security awareness training to inform personnel** (including contractors and other users of information systems that support the operations and assets of the agency) of the
information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks

Federal Information Security Management Act (FISMA)

- **Periodic testing and evaluation of the effectiveness of information** security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) with a frequency depending on risk, but no less than annually
- **A process** for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency
- **Procedures for detecting, reporting, and responding to security incidents** (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President
- **Plans and procedures** to ensure continuity of operations for information systems that support the operations and assets of the agency
- This act **is guaranteed job security for ethical white hat hackers to perform continual security audits of government agencies and other organizations**.

Privacy act 1974

- The Privacy Act of 1974 (5 USC 552a) ensures **nondisclosure of personal information and ensures that government agencies are not disclosing information without the prior written consent of the person whose information is in question.**

USA PATRIOT ACT 1974

- This act, with the official **name Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism** (USA PATRIOT) Act of 2001, gives the government the authority **to intercept voice communications** in computer hacking and other types of investigations.

- The Patriot Act was **enacted primarily to deal with terrorist activity** but can also be construed as a wiretap mechanism to discover and prevent hacking attempts..

The Government Paperwork Elimination Act (GPEA)

- The Government Paperwork Elimination Act (GPEA) of 1998 requires federal agencies to
  allow people the option of using electronic communications when interacting with a government agency.

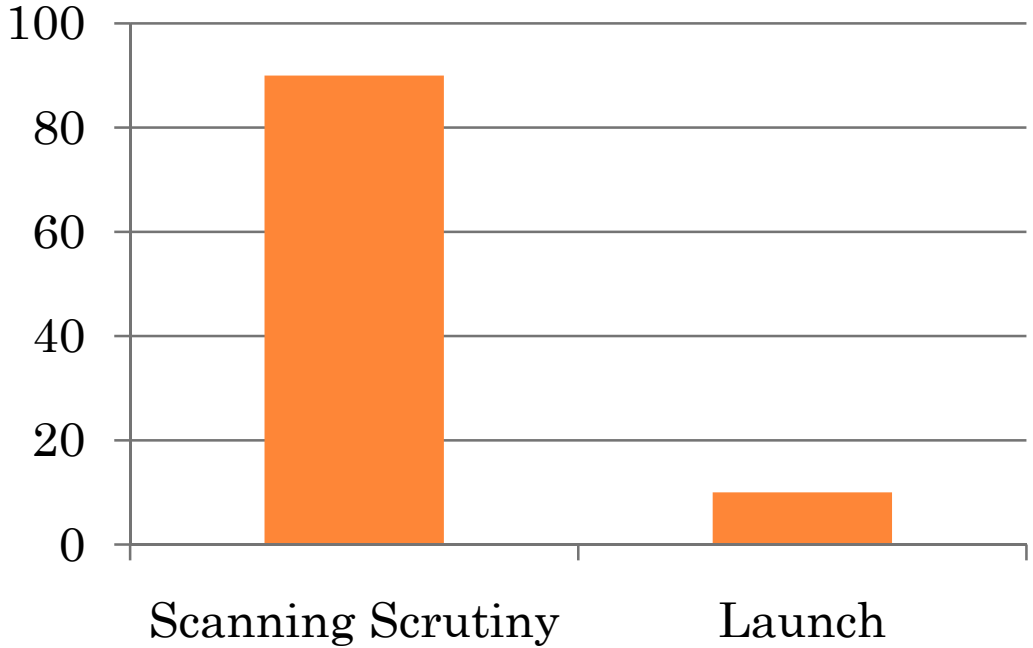
- GPEA also encourages the **use of electronic signatures**. When valuable government information is stored in electronic format, the targets and stakes for hackers
  is increased.

CYBERLAWS IN OTHER COUNTRIES

- When you're performing **penetration testing for international organizations**,
- it is imperative to check the laws of the governing nation to make sure the testing is legal in the country. With the use of the Internet and remote attacks, regional and international borders can be crossed very quickly.

- When you're performing an **outside remote attack**, the data may be stored on servers in another country and the laws of that country may apply. It is better to be safe than sorry, so do the research prior to engaging in a penetration test for an international entity.
- In some countries, laws may be more lenient than in the United States, and this fact may work to your advantage as you perform information gathering.

Scanning and Scrutinizing Gathered Info



Contents

Reconnaissance-Understanding Competitive Intelligence;Information-Gathering Methodology-Footprinting , Using Google to Gather Information , Understanding DNS Enumeration , Understanding Whois and ARIN Lookups , Identifying Types of DNS Records, Using Traceroute in Footprinting , Understanding Email Tracking ,Understanding Web Spiders;

RECONNAISANCE

- The term *reconnaissance comes from the* ***military and means to actively seek an enemy's*** **intentions by collecting and gathering information about an enemy's composition and capabilities via direct observation,** usually by scouts or military intelligence personnel trained in surveillance.

- In the world of ethical hacking, reconnaissance applies to the process of information gathering.

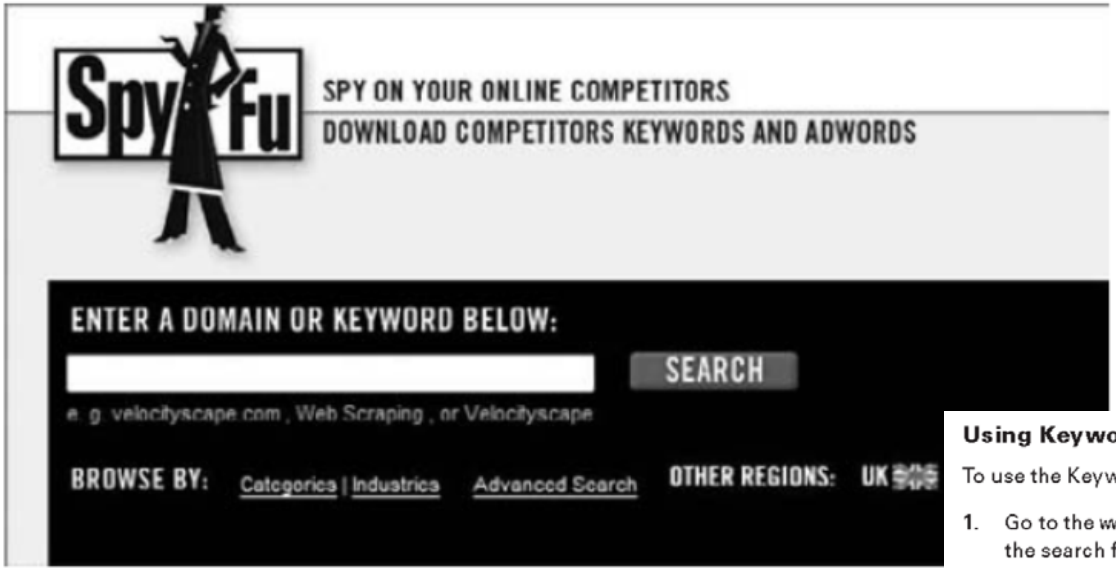
- Reconnaissance is a catchall term for watching the hacking target and gathering information about how, when, and where they do things. By **identifying patterns of behavior, of people or systems, an enemy could find and exploit a loophole**

Competitive intelligence

- Competitive intelligence means information gathering about competitors' products, marketing, and technologies. Most competitive intelligence is nonintrusive to the company being investigated and is benign in nature—it's used for product comparison or as a sales and **marketing tactic to better understand how competitors are positioning their products or services.**

- Several tools exist for the purpose of competitive intelligence gathering and can be used by hackers to gather in formation about a potential target.

Competitive intelligence



Using KeywordSpy

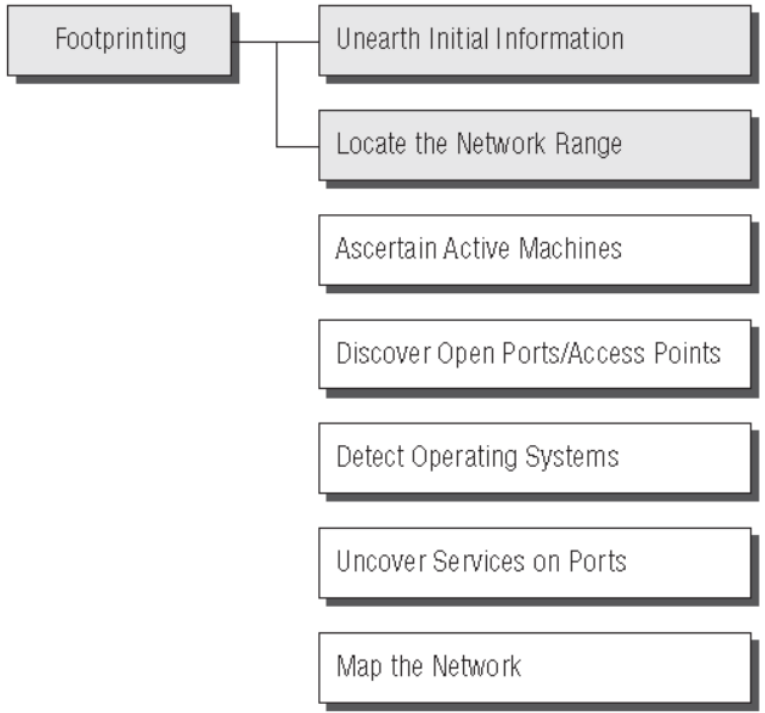
To use the KeywordSpy online tool to gather competitive intelligence information:

1. Go to the www.keywordspy.com website and enter the website address of the target in the search field:

2. Review the report and determine valuable keywords, links, or other information.

Information Gathering Methodology

Seven steps of information gathering



FOOT PRINTING

- ***Footprinting is defined as the process of creating a blueprint or map of an organization's* network and systems.**
- Footprinting 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 nonintrusive methods.
- For example, the organization's own **web page may provide a personnel directory or a list of employee bios,** which may prove useful if the hacker needs to use a social-engineering attack to reach the objective.
- 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:

FOOTPRINTING

- 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
- Once this information is compiled, it can give a hacker better insight into the organization, where valuable information is stored, and how it can be accessed.

Tools in Footprinting

- Domain name lookup
- Whois
- NSlookup
- Sam Spade
- **In google to Gather 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.

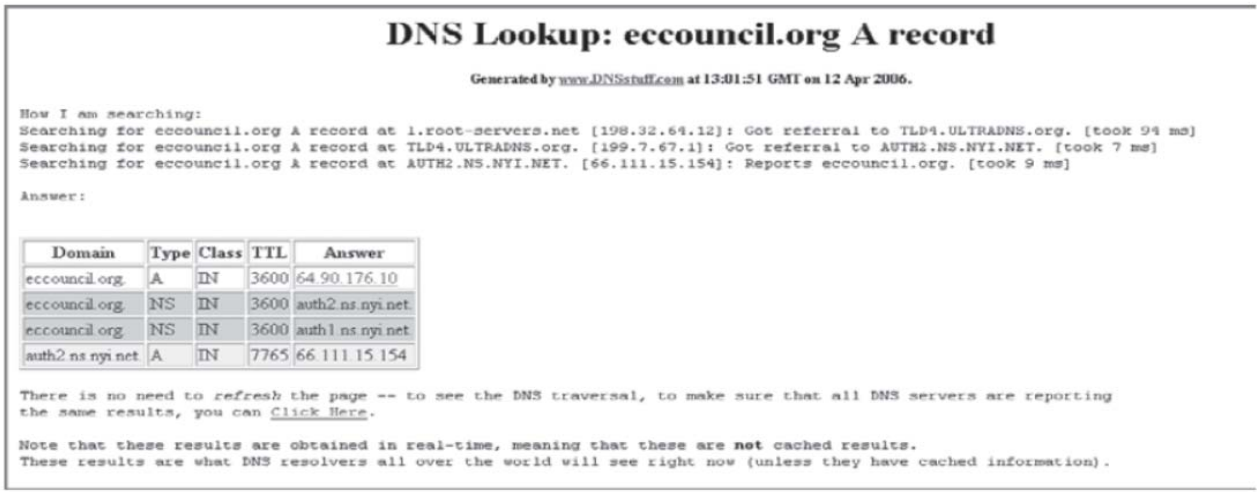
cache Identifies the version of a web page. Supply the URL of the site after the colon.

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.

UNDERSTANDING DNS ENUMERATIONS

- *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



DNS Lookup: eccouncil.org A record

Generated by www.DNSstuff.com at 13:01:51 GMT on 12 Apr 2006.

```
How I am searching:
Searching for eccouncil.org A record at l.root-servers.net [198.32.64.12]: Got referral to TLD4.ULTRADNS.org. [took 94 ms]
Searching for eccouncil.org A record at TLD4.ULTRADNS.org. [199.7.67.1]: Got referral to AUTH2.NS.NYI.NET. [took 7 ms]
Searching for eccouncil.org A record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports eccouncil.org. [took 9 ms]

Answer:
```

Domain	Type	Class	TTL	Answer
eccouncil.org.	A	IN	3600	64.90.176.10
eccouncil.org.	NS	IN	3600	auth2.ns.nyi.net.
eccouncil.org.	NS	IN	3600	auth1.ns.nyi.net.
auth2.ns.nyi.net.	A	IN	7765	66.111.15.154

There is no need to *refresh* the page -- to see the DNS traversal, to make sure that all DNS servers are reporting the same results, you can Click Here.

Note that these results are obtained in real-time, meaning that these are **not** cached results.
These results are what DNS resolvers all over the world will see right now (unless they have cached information).

U NS

Domain Information

Domain:	pvpsiddhartha.ac.in
Registrar:	ERNET India
Registered On:	2005-03-04
Expires On:	2030-03-04
Updated On:	2021-08-12
Status:	OK
Name Servers:	margot.ns.cloudflare.com osmar.ns.cloudflare.com

Registrant Contact

Organization:	Prasad V Potluri Siddhartha Institute of technology
Country:	IN
Email:	Please contact the Registrar listed above

Identifying types of DNS records

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 trace root in Footprinting

- 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 traceroute 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.

Using trace root in Footprinting

- NeoTrace, VisualRoute, and VisualLookout are all packet-tracking tools with a GUI or visual interface. They plot the path the packets travel on a map and can visually identify the locations of routers and other internetworking devices.
- These tools operate similarly to traceroute and perform the same information gathering; however, they provide a visual representation of the results.

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.**
- Visualware's eMailTrackerPro (www.emailtrackerpro.com/) and MailTracking (http:// mailtracking.com/) are tools that allow an ethical hacker to track email messages.
- When you use these tools to send an email, forward an email, reply to an email, or modify an email, the resulting actions and tracks of the original email are logged. The sender is notified of all actions performed on the tracked email by an automatically generated email.

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.