Manoj Saha, 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Reconnaissance for Ethical Hacking

PG Student Manoj Saha, Professor Vijayakumar Adaickalam
School of Computer Science and Information Technology,
Jain Deemed-to-be University,
Bengaluru, India
Email: sahamanoj96@gmail.com, vijay.pattukkottai@gmail.com

Abstract-As technology approach the new era of cyber security, Internet user witnessed the flexible growth of using cyber security tools in 5 years. The fundamental challenges that professional faced today is evolving technologies and human beings. In these digital environments, where online communication and the Internet have become essential but we always fear our security and privacy. As a normal Internet user, they are not aware of the cyber security tool that is used to protect our security and privacy or the tools which help cyber security professionals to figure out the cyber-incident. So, let's talk about the cyber security tool, LINUX and PARROT Operating system but it's a completely different environment for average Internet users. It very important to know about cyber security fundamentals and ethical hacking ethics which will provide cyber security knowledge and behavior pattern. Adversaries are frequently capable of penetrating networks and compromising structures through exploiting vulnerabilities in human beings and information systems. The key to the fulfilment of those attacks is statistics that adversaries gather during the levels of the cyber kill chain. We summarize and examine the methods, tactics, and gear that adversaries use to behavior reconnaissance activities in the course of the attack process. It is important to talk about what types of information adversaries seek, and how and when they could gain this information..

Keywords- Cyber security, Information Gathering, Foot-printing, and Reconnaissance.

I. INTRODUCTION

In 2021, indicated that failure in the use of fundamental security features in safeguarding the corporation information could make agencies prone to cyber-attacks.

Cyber security refers back to the collection of tools, first-class practices, guidelines, policies, safety concepts, and safety safeguards, procedures to danger management, education actions, warranty and technology usable in protective cyber environment, the enterprise and the property of person.

Cyber security assures that the enterprise attains and keeps its safety houses and person property in opposition to safety dangers inside cyber environment.

In this regard, cyber security and moral safety hacking strategies may be carried out via way of means of enterprise in lowering cyber dangers and capability impact at the recognition of enterprise and its information. Ethical hacking can maintain digital privacy of users.

At the equal time, the enterprise can foresee capability cyber attacks and preclude their occurrence. Hence, the implementation of cyber security and moral hacking strategies can facilitate enterprise in keeping its virtual property.

Chances are you've got observed a trend here - the CIA Triad is all about facts.

1. Confidentiality:
It means that the data is only available to permission granted parties.

2.Integrity:
It refers to the certainty that the data is not tampered with or degraded during or after submission.

3. Availability:
The information is available to permission granted users when it is needed.

While that is taken into consideration the core thing of the majority of IT security, it promotes a constrained view of the safety that ignores different crucial factors. For example, despite the fact that availability may serve to make sure you don't lose access to assets had to offer facts while it's far needed, considering facts protection in itself doesn't assure that someone else hasn't used your hardware resources without authorization.

It's crucial to recognize what the CIA Triad is, how it's far used to plan and additionally to implement a first-class protection coverage whilst expertise the diverse ideas behind it. It's additionally crucial to recognize the restrictions it presents.

When you're informed, you may make use of the CIA Triad for what it has to provide and keep away from the outcomes that could come along by not understanding it.

II. LITERATURE SURVEY ON ETHICAL HACKING

Wojciech Mazurczyk and Luca Caviglione (1) stated that in general, reconnaissance relies upon a composite set of techniques and processes and has not to be considered limited to information characterizing the target at a technological level, such as, the used hardware or the version of software components.

Attackers also aim at collecting details related to the physical location of the victim, phone numbers, names of the people working in the targeted organizations and their email addresses. In fact, any bit of knowledge may be used to develop a software exploit or to reveal weaknesses in the defensive systems.

For the better understanding of cyber security and ethical hacking, I have studied more than 10 research and survey paper dated from 2021 to 2017.

Notable paper from the above-mentioned:
Wojciech Mazurczyk and Luca Caviglione (1) have proposed that it has focused on the reconnaissance phase, which is the basis for the totality of cyber security attacks. Engineer a new-wave of reconnaissance-proof-by design services, for instance, by minimizing the impact of the addressing scheme, the use of IoT and the exposition to scanning services like Shodan and re-think the concept of privacy in a broader manner to also include protection mechanisms against advanced and malicious data gathering campaigns.

Shanto Roy, NaziaSharmin, Jamie C. Acosta, Christopher Kiekintveld and Aron Laszk (2) have proposed one of the main lessons is the overall scope and diversity of the problem of adversarial reconnaissance in cyber security. The variety of types of information that could potentially be useful to an attacker is vast, as is the number of tools and specific techniques for obtaining it. This is also a moving target, as the types of information that are relevant and the tools will naturally evolve over time with technology.

Danda B. Rawat (3) have proposed that the cyber defense teams to leverage data-driven techniques with AI for cyber security, where AI learns and enhances its knowledge base more quickly to better detect, predict and respond to cyber-attacks. The results have revealed that the probability of cyber-attack decreases as the education and income level of victim increases. It is believed that cyber-crime units will use the proposed model. It will also facilitate the detection of cyber-attacks and make the fight against these attacks easier and more effective in near future.

Abdulkadir Bilen and Ahmet Bedri Azur (4) proposed that, it analyses the cyber-crimes in two different models with machine-learning concept and predicted the effect of the defined features on the detection of the cyber-attack methods and the perpetrator behavior and actions.

Ahmad Mtair AL Hawamleh, AlorfiAlmuhannadSulaiman M, Jassim Ahmad Al-Gasawneh, and Ghada Al-Rawashdeh (5) proposed about the importance of cyber security and the use of ethical hacking techniques for user data protection through the characterization of globally established standards and techniques for

organizations to apply, in the prevention of likely cyber threats while assuring user data protection.

Rohit Kalakuntla, AnveshBabuVanamala and Ranjith Reddy Kolipyaka (6) proposed about the motivation, behaviour and countermeasure behind the cyber security and cyber terrorism. Cyber Security accepts a vigorous role in the area of information technology. Safeguarding the information has become an enormous problem in the current day. The cyber security the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings

IdimadakalaNagaraju (7) proposed about the ethics of using cyber security tool and understanding the true intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and people are encountering tools that are beneficial to them. If these tools fall into the wrong hands they can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues highlighted by the media always reporting some type of cyber-crime, a study showing that nearly 93% of attacks happened inside of the organization raising concerns of how easy it is to be working inside to be able to infiltrate attacks.

Saloni Khurana (8) proposed about the exploration on how cybercrime has become a serious threat in our lives and it highlight are some of the different security methods that are being used in malicious approaches, techniques and attack and their various loopholes.

Pavan Kumar and K. Pranathi (9) proposed that the entire world is moving toward technological advancements and increasing digitization of real-world operations, which raises the risk of security. The workings of malicious hackers or crackers, on the one hand, who try to illegally break into security, and white hat hackers or ethical hackers, on the other hand, who try to preserve security and trying harden the security configuration and patching critical vulnerabilities.

Brijesh Kumar Pandey, Alok Singh and Lovely lakhmaniBalani (10) have proposed about the concepts of system security, hacking, hacker, ethical hacking aka pen testing. Then in next section it discussed about various tools, techniques and approaches which are normally constitutes weaponry of a seasoned hacker and their behavioral mindset.

It also explains it has explained how ethical hacking is a continuous and dynamic process, and then it discussed various opportunities available to an ethical hacker as a professional.

III. ETHICAL HACKING

Ethical Hacking: It is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization.

1. Types of Hackers:

A hacker is someone who solves a technical difficulty through the usage of a computer, networking, or maybe different abilities. Anyone who makes use of their abilities to gain access to a device or networks in utility to break legal guidelines is known as a hacker.

There are distinct varieties of hackers:

1.1 White Hat Hackers: On the dark web, those are the proper folks that come to our aid. White hat hackers additionally referred to as ethical hackers, are cyber security professionals who help the authorities and companies through performing penetration trying out and figuring out protection flaws. Ethical hackers use quite a few strategies to defend themselves from black hat hackers and different cybercriminals. They spoil into our device with the best goal of locating vulnerabilities and helping you in eliminating viruses and malware.

1.2 Grey Hat Hackers: Grey Hat Hackers fall in among white and black hat hackers. Grey hat hackers might not use their competencies for non-public advantage; they could however have both excellent and horrific intentions. For instance, a hacker who hacks into an enterprise and unearths a few vulnerabilities may also leak it over the internet or tell the enterprise approximately it. Nevertheless, as quickly as hackers use their hacking competencies for the non-public advantage they end up black hat hackers.

1.3 Black Hat Hackers: These days, black hat hackers are the primary perpetrators of cybercrime. The

majority of the time, the schedule of a black hat hacker is monetary. These hackers search for flaws in personal computer systems in companies and banking systems. They can hack into your community and gain access to your non-public, business, and monetary data by exploiting any loopholes they find.

2. The five phases of ethical hacking are:

2.1 Reconnaissance: Reconnaissance is an important section of ethical hacking. It facilitates the discover of attacks can be launched and to collect as much of data as possible.

2.2 Scanning: The second step in the ethical hacking methodology is scanning, where attackerlooks for information such as user accounts, credentials, IP addresses, etc.

2.3 Gaining Access: The next step in ethical hacking is gaining access where an attacker can usevarious tools and methods to gain access and enter a system.

2.4 Maintaining Access: In this stage, the attacker manages to access the target's system, they trytheir best to maintain that access.

2.5 Clearing Track: The last phase of ethical hacking ensures that the attackers leave no clues or evidence behind that could be traced back.

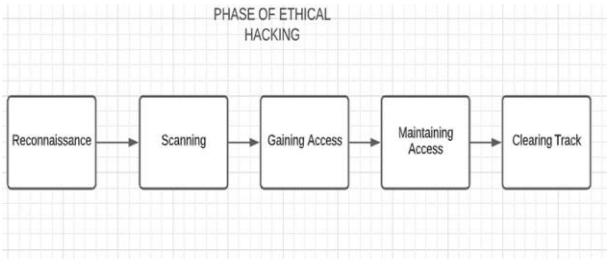

Fig 1. Phase of Ethical Hacking.

3. Why Ethical Hacking is Necessary:

The upward push in malicious activates, cybercrimes, and appearance of different styles of superior assaults require to need of penetration tester who penetrate the safety of device and networks to be determined, prepare and take precaution and remediation movement towards those competitive assaults.

These competitive and superior assaults include: -

- Identity Theft
- Vandalism
- Credit Card theft
- Denial-of-Services Attacks
- Theft of Services
- Manipulation of data
- Piracy

Increase in those form of assaults, hacking cases, and cyber assaults, due to the fact of growth of the use of online transactions and online offerings with inside the last decade. It turns into greater appeal for hackers and attackers to tempt to thieve financial information. Computer or Cybercrime regulation has bogged down prank activities only, while actual assaults and cybercrimes upward push. It specializes in the requirement of Pentester, a shortened shape of Penetration tester for the hunt for vulnerabilities and flaws inside a device earlier than watching for an assault.

If you need to overcome the attacker and hacker, we need to be clever sufficient to suppose like them and act like them. As we know, hackers are skilled, with great know-how of hardware, software, and exploration capabilities. It guarantees the want and significance of moral hacking which lets the ethical hacker counter the assault from malicious hackers via way of means of looking ahead to methods.

Another primary gain and want for ethical hacking are to discover the vulnerabilities in structures and protection deployments to do so to secure them earlier than they may be utilized by a hacker to breach protection.

4. Limitations of Ethical Hacking:

Ethical Hacking is an essential and important issue of threat assessment, auditing, and counter frauds. Ethical hacking is extensively used as penetration trying out to pick out the vulnerabilities, threats, and spotlight the holes to take remedial moves towards attacks. However, there may be additionally a few barriers in which ethical hacking isn't enough, or simply through ethical hacking, the problem ought to not resolve. An enterprise needs to first recognize what it is seeking out earlier than hiring an outside pentester.

It enables attention to the desire to acquire and keep time. The testing group was committed to troubleshooting the real trouble in resolving the issues. The ethical hacker additionally enables to apprehend the safety gadget of an enterprise better. It is as much as the enterprise to take encouraged movements through the Pentester and put into

effect safety regulations over the machine and network.

Information Gathering and learning about the target systems is the primary procedure in ethical hacking. Reconnaissance is a fixed set of approaches and techniques (Foot printing, Scanning & Enumeration) used to covertly find out and gather records about a target system. During reconnaissance, an ethical hacker tries to acquire a whole lot of records about a target device as possible, following the seven steps indexed below – Gather preliminary records Determine the network system and ranges.

Identify active machines Discover open ports and get admission access to points Fingerprint the running system Uncover offerings on ports Project the network Reconnaissance takes parts in two areas – Active reconnaissance and Passive reconnaissance.

5. Scope:

Reconnaissance is performed not only by the adversaries (black/gray hat hackers) but additionally by cyber-security researchers (white hat hackers, blue teams, etc.) for protection testing purposes. In this survey, we speak reconnaissance from the hacker's angle in particular, and we do not consider styles of reconnaissance which can be used most effectively by cyber- security researchers or network administrators.

IV. BACKGROUND OF RECONNAISSANCE

Reconnaissance involves the discovery of information, usually public information, about an organization to better understand how it operates and is used to identify people or potential points of compromise that can be used to successfully exploit an organization. Reconnaissance is a prerequisite of each next step that adversaries try and execute in an attack.

The foot printing section permits the attacker to accumulate the records concerning the inner and outside safety of security-based architecture. Collection of records additionally enables one to become aware of the vulnerabilities inside a system, which exploits, to benefit access. Getting deep records approximately target reduces the point of interest area & carries the attacker in the direction of the goal. The attacker focuses the goal via way of means of the range of IP to deal with what he has to go through, to hack the target or concerning area information or else.

Foot printing is part of reconnaissance wherein the hackers try and collect the target device data in active and passive ways. Reconnaissance is a technique of collecting data about the machine.

It includes 3 steps:

- Foot printing
- Scanning
- Enumeration

During reconnaissance, an ethical hacker tries to accumulate a lot of fact about a targetmachine, following the seven steps mentioned below –

- Gather preliminary facts
- Determine the network architecture range
- Identify lively machines
- Discover open ports and get entry to points
- Fingerprint the working system
- Uncover offerings on ports
- Map the network

Reconnaissance is of two types – Active reconnaissance and Passive reconnaissance.

1. Active Reconnaissance:

In this procedure, you may immediately engage with the pc device to benefit from facts. These facts may be applicable and accurate. But there may be a risk of having detected in case you are making plans for active reconnaissance without permission. If you're detected, the device admin can take intense movement towards you and path your next activities.

- Querying posted call servers of the target
- Extracting metadata of posted files and files
- Gathering records thru e-mail tracking
- Performing Whois lookup
- Extracting DNS records
- Performing trace route analysis

2. Passive Reconnaissance:

In this procedure, you may now no longer be immediately linked to a pc device. This procedure is used to acquire important facts without ever interacting with the goal systems.

- Finding Information through search engines domain.
- Finding Top-level Domains (TLDs) and sub-domain names of a goal via net services.

International Journal of Science, Engineering and Technology

An Open Access Journal

- Collecting vicinity facts at the goal via net services
- Performing people search using social networking web-sites and those seek services
- Gathering monetary facts approximately about the goal via economic services
- Gathering infrastructure information of the target employer via process websites
- Monitoring target usage alert services
- Collecting facts via social engineering on social networking websites.

V. APPROACHES

The first step to ethical hacking is Foot printing. Foot printing is the series of each feasible record concerning the target and target network community. This series of records facilitates in figuring out distinct feasible methods to enter into the target network community. This series of records might also additionally have gathered via publicly- to be had private records and touchy records from any mystery supply.

Typically, footprinting & reconnaissance is performed by social engineering attacks, gadget or network attack, or via some other technique. Active and passive strategies of reconnaissance are also famous for gaining records of goals immediately or indirectly. The overall reason for this section is to maintain interplay with the target to benefit records with no detection or alerting.

1. Pseudonymous Foot printing:
Pseudonymous foot printing consists of foot printing via online sources. In Pseudonymous foot printing records approximately a target is shared through posting with an assumed name. This kind of record is shared with the real credential to keep away from hint to a real supply of records.

2. Internet Foot printing:
Internet Foot printing consists of Foot printing and reconnaissance strategies for gaining records via the internet. In Internet Foot printing, approaches include Google Hacking, Google Search, Google Application inclusive of search engines apart from Google as well.

3. Objectives of Foot printing:
The fundamental targets of Foot printing are: -

- To recognize security posture
- To lessen recognition area
- Identify vulnerabilities
- Draw community network map

VI. METHDOLOGY AND TECHNIQUES

It isn't a massive deal to get records concerning each person because the internet, social media, reliable websites, and different sources have a lot of records about their customers which aren't sensitive, however, a group of records can also additionally fulfill the necessities of an attacker and attacker can acquire sufficient records via way of means of a bit effort.

Below are extra frequently strategies utilized by hackers: -

1. Foot printing via Search Engines:
The primary choice that is very responsive as properly is Foot printing through search engines. Search engines extract the records of approximately an entity you have looked for from the internet. You can open an internet browser and throughany search engine like Google, DuckDuckGo and Bing, look for any organization. The end result collects each available record on the internet.

2. Foot printing via Advanced Google Hacking Techniques:
Some superior alternatives may be used to look for a particular subject matter the usage of search engines. These Advance search operators made the looking more suitable and centered on a sure subject matter.

Advanced search engine operators by Google are: -

2.1 Site: Search for the bring about the given domain
2.2 Related: Search for Similar internet pages
2.3 Cache: Display the internet pages saved in Cache
2.4 Link: List the websites having a hyperlink to a particular internet page
2.5 Allintext: Search for websites containing a particular keyword
2.6 Intext: Search for files containing a particular keyword
2.7 Allintitle: Search for websites containing a particular key-word within side the title
2.8 Intitle: Search for files containing a particular key-word within side the title
2.9 Allinurl: Search for websites containing a particular key-word in URL

2.10 Inurl: Search for files containing a particular keyword in URL

2.11 The syntax where it can be used: https://www.google.com/advanced_search

3. Foot printing via Social Networking Sites:

Social Networking is one of the best information sources among other sources. The different popular and most widely used social networking site has made it quite easy to find someone, get to know someone, including its basic personal information as well as some sensitive information as well. Advanced features on these social networking sites also provide up-to-date information.

An Example of gathering information through social networking sites can be finding someone on Facebook, Twitter, LinkedIn, Instagram, and much more.

4. Foot printing via Websites:

Website Foot printing process involves tracking and investigating the target organization's reliable internet site for gaining records inclusive of Software running, variations of those software programs, working systems, Sub-directories, database, scripting records, and different details. These records can be accrued through on-line offerings as described in advance like netcraft.com or through using software program inclusive of Burp Suite, Zaproxy, Website Informer, Firebug, and others. This equipment can carry records like connection kind and standing and last amendment records. By getting this kind of records, an attacker can observe supply code, developer's details, document machine structure, and scripting.

5. Foot printing via Email:

Email performs an essential function in going for walks an organization's business. Email is one of the maximum popular, broadly used expert approaches of conversation that is utilized by each organization. Communicating with the business partners, employees, competitor, contractors and different kinds of human beings which are worried in going for walks an organization. Content or frame of Email is hence essential, extraordinarily treasured to attackers.

This content material may also include hardware and software program facts, consumer credentials, community and security gadgets facts, economic facts that is treasured for penetration testers and attackers. Polite Mail is a totally beneficial device for Email foot printing. Polite Mail tracks e-mail conversation with Microsoft Outlook. Using this device, with a listing of e-mail addresses of a focused organization, the malicious hyperlink may be dispatched and hint the character event.

Tracing an e-mail, the usage of e-mail header can display the following facts:

- Destination address
- Sender's IP address
- Sender's Mail server
- Time & Date facts
- Authentication device facts of sender's mail server

6. Foot printing via Competitive Intelligence:

Competitive Intelligence accumulating is a way of gathering records, reading and accumulating records concerning the competitors. Competitive the intelligence accumulating system is non-interfering as its miles the system of series of records thru the unique resources.

Some primary sources of aggressive intelligence are:

- Official Websites
- Job Advertisements
- Press releases
- Annual reports
- Product catalogs
- Analysis reports
- Regulatory reports

7. Foot printing via WHOIS:

"WHOIS" allows to advantage records concerning area name, ownership records. IP Address, Netblock data, Domain Name Servers, and other records. Regional Internet Registries (RIR) keep the WHOIS database. WHOIS research allows discovering who's at the back of the goal area name.

8. Foot printing via DNS:

DNS lookup statistics are beneficial to discover a bunch inside a targeted network. There are numerous tools to be had on the internet which carry out DNS lookup.

9. Foot printing via Network:

One of the crucial kinds of foot printing is network foot printing. Fortunately, there are numerous tools to be had which may be used for community foot

International Journal of Science, Engineering and Technology

An Open Access Journal

printing to benefit statistics approximately the target network. Using that software, a statistics seeker can create a map of the focused network.

Using those tools, you may extract statistics such as:-

- Network address ranges
- Hostnames
- Exposed hosts
- OS and alertness model statistics
- Patch state of the host and the programs
- Structure of the programs and back-end servers

10. Foot printing via Social Engineering:

In foot printing, one of the simplest aspects to hack is a human being itself. We can accumulate statistics from a human quite easily without difficulty than fetching statistics from systems.

Using Social Engineering, a few primary social engineering strategies are: -

- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Impersonation

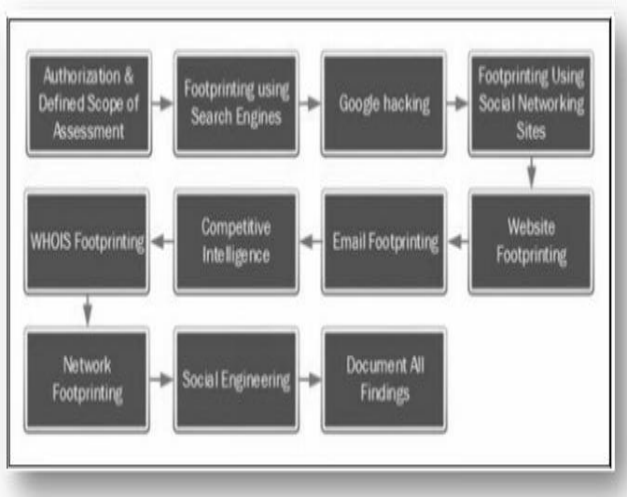

Fig 2. Overall Method Roadmap for Reconnaissance.

The following is a listing of key strategies and sub-strategies

Active Scanning

- Port Scanning
- Vulnerability scanning
- Website Directory brute-force Search Open Technical Databases
- Search Engines
- Social Networks

Search Open Website/Domains

- Who is records
- DNS records
- Sub domain enumeration
- Discover web technologies and stacks utilized
- Identify vulnerabilities

Gather Victim Identity Information.

- Emails
- Credentials
- Employee Names

Gather Victim Network Information

- Domain properties
- DNS
- Third-parties' domains
- Network topology
- IP addresses
- Security infrastructure

The strategies mentioned above will fall beneath passive or lively recon primarily based totally on the kind of statistics we can be accumulating and the character of our engagement with the goal organization's virtual infrastructure.

Passive reconnaissance includes utilizing publicly to be had statistics sources like search engines and databases to locate and pick out statistics approximately our goal domain or organization.

Gathering Domain IP/DNS records:

The first step on this technique is to discover the IP deal with and DNS statistics of your goal area, this may be achieved via way of means of utilizing the subsequent tools:

- **Host utility software:** We can use the host software on Linux/Unix structures to decide the IP deal with our goal area
- **Nslookup:** We can use the Nslookup software to pick out the IP deal with our goal area
- **DNSRecon:**DNSRecon is an exceptionally beneficial software that comes pre-packaged with Kali Linux and may be used to enumerate the DNS statistics for a selected area, this statistic can monitor MX (Mail) server addresses in addition to different beneficial DNS statistics that may enlarge our know-how of the goal's infrastructure
- **Dig:** We also can make use of the DNS research software dig, to pick out the goal area.

International Journal of Science, Engineering and Technology

An Open Access Journal

VII. VULNERABILITIES, ATTACKS AND COUNTERMEASURE

Reconnaissance attacks purpose to find out records about a network, inclusive of the following:

1. Active Targets Attack:
An active attack might be a network exploit at some point in which the attackers will alter or modify the content material and affect the device resource. It'll cause damages to the end-user. The attackers can carry out passive attacks to acquire data earlier than they start playacting an energetic attack.

The attackers try to disrupt and forced the entry of the device. The victims can get knowledgeable regarding the energetic attack. This kind of attack can threaten their integrity and accessibility. A lively attack is more difficult to carry out in comparison to a passive assault.

2. Network Services Attack:
Network attacks are unauthorized moves at the virtual property inside an organizational community. Malicious events generally execute network attacks to alter, destroy, or steal personal information. Perpetrators in network attacks generally tend to target community perimeter networks to benefit access to inner systems.

There are fundamental forms of network attacks: passive and active. In passive network attacks, malicious events benefit unauthorized access to networks, monitor, and steal personal statistics without making any alterations. Active network assaults contain modifying, encrypting, or unfavorable statistics.

Upon infiltration, malicious events can also additionally leverage different hacking activities, inclusive of malware and endpoint assaults, to assault an organizational community. With extra groups adopting faraway working, networks have grown to be extra susceptible to statistics robbery and destruction.

3. Operating system platform vulnerabilities attack:
The working device's strategies and kernel do the specific mission as instructed. If person software made those strategies do malicious tasks, then it's far called Program Threats. One of the not unusual place examples of a software hazard is software set up in a pc which can save and ship person credentials through community to a few hackers.

Following is the listing of a few famous software threats.

- Trojan Horse − Such a software traps person login credentials and shops them to ship to the malicious person who can afterward login to a pc and might get entry to device resources.
- Trap Door − If a software this is designed to paintings as required, has a protection hollow in its code and plays unlawful motion without the understanding of the person then it's far known as to have a lure door.
- Logic Bomb − A common sense bomb is a state of affairs whilst a software misbehaves simplest whilst sure situations are met in any other case it really works as an actual software. It is tougher to detect.
- Virus − Virus because the call shows can reflect themselves on a pc device. They are exceptionally risky and might modify/delete person files, crash systems. A virus is typically a small code embedded in a software. The person accesses the software, the virus begins off evolved getting embedded in different files/ packages and might make the device unusable for the person

4. File Permission Attack:
Adversaries might also additionally alter report or listing permissions/attributes to evade access control lists (ACLs) and get admission to covered documents. File and listing permissions are usually controlled via way of means of ACLs configured via way of means of the report or listing owner, or customers with the correct permissions. File and listing ACL implementations range via way of means of the platform, however usually explicitly designate which customers or businesses can carry out which actions (read, write, execute, etc.).

Modifications might also additionally consist of converting precise get admission to rights, which might also additionally require taking possession of a report or listing and/or multiplied permissions relying on the report or listing's current permissions. This might also additionally permit malicious interest along with modifying, changing, or deleting precise documents or directories. Specific report and listing changes can be a required step for lots techniques,

along with organizing Persistence through Accessibility Features, Boot or Login Initialization Scripts, Unix Shell Configuration Modification, or tainting/hijacking different instrumental binary/configuration documents through Hijack Execution Flow.

5. Information Disclosure Attack:

Information disclosure also known as information leakage is when an internet site by accident exhibits critical records to its users. Depending on the context, websites may also leak all forms of records to a capability attacker, including:

- Data approximately different users, consisting of usernames or economic records.
- Sensitive business or commercial enterprise data
- Technical information about the internet site and its infrastructure

As web application technology evolves, strong safety features should observe suit. Threats to internet app protection are a truth and going on throughout the globe. Standard measures are not enough to guard towards evolving threats. Fortunately, apps do now no longer must stay vulnerable, ready to be exploited via way of means of terrible actors. There are strong safety features and practices that may be hired to guard this ever-developing assault surface.

The top 10 most common application vulnerabilities include:

- Injection: An injection happens when a bad actor sends invalid data to the web appto make it operate differently from the intended purpose of the application.
- Broken Authentication: A broken authentication vulnerability allows a bad actor togain control over an account within a system or the entire system.
- Sensitive Data Exposure: Sensitive data exposure means data is vulnerable to being exploited by a bad actor when it should have been protected.
- XML External Entities (XXE): A type of attack against an application that parses XML input and occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.
- Broken Access Control: When components of a web application are accessible instead of being protected like they should be, leaving them vulnerable to data breaches.
- Security Misconfigurations: Incorrectly mis-configuring a web application provides bad actors with an easy way in to exploit sensitive information.
- Cross Site Scripting (XSS): An XSS attack means a bad actor injects malicious client- side scripts into a web application.
- Insecure De-serialization: Bad actors will exploit anything that interacts with a web application—from URLs to serialized objects—to gain access.
- Using Components with Known Vulnerabilities: Instances such as missed software and update change logs can serve as big tip-offs for bad actors looking for ins into a web application. Disregarding updates can allow a known vulnerability to survive within a system.
- Insufficient Logging and Monitoring: Lack of efficient logging and monitoring processes increases the chances of a web app being compromised.

"Cyber Kill Chain" term coined by Lockheed Martin maps to detection and mitigation actions for cyber security attacks. Because the Kill Chain makes use of an attacker's viewpoint, the Kill Chain is threat-primarily based totally. It permits agencies to plan, the use of their assets and investments intelligently. The framework nature of the Kill Chain promotes flexibility and subsequently can adapt to almost any form of threat.

The Kill Chain idea considers that an assault isn't a single occasion however is a chain of phases (or levels) that construct upon one another. Interrupting at a single degree is to disrupt the complete assault.

6. Reconnaissance:

In any other case called target selection and spying. An attacker both enters this level with a deliberate target already established, or the attacker searches for a goal primarily based totally on suitability and susceptibility. Gathering as an awful lot of statistics approximately about the target as viable is their purpose, starting with passive and transferring in the direction of greater competitive active reconnaissance.

The attacker develops a listing of potential end-user with a slender purpose in mind (e.g., extracting economic information from POS machines), and conducts reconnaissance to isolate the one's maximum prone to attack.

International Journal of Science, Engineering and Technology

An Open Access Journal

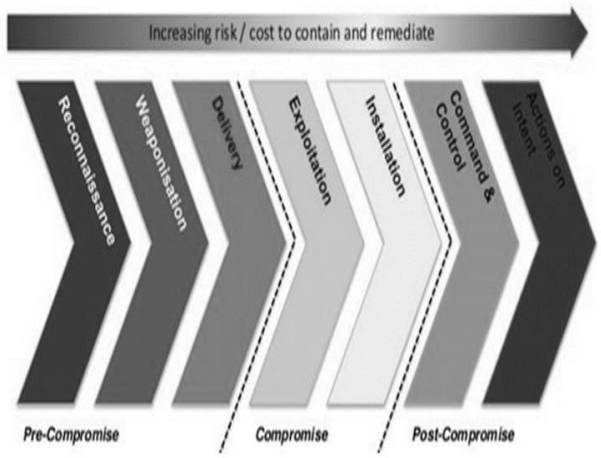

Fig 3. Cyber Kill Chain.

7. Countermeasures against reconnaissance Phase

- Education about the basics of cyber security do and don't
- Interrupt the attack at one of the levels of progression
- Training towards Social Engineering
- Consider protection plan for SDLC
- Implement Application protection Programs
- Ensure Vendors and third-party software
- Implement Security Best Practices
- Layered, ringed defenses

Privilege escalation and lateral movement in system:
The lateral movement refers back to the strategies that a cyber attacker uses, after gaining preliminary get admission, to transport deeper right into a network looking for critical records and different high-priced assets. After coming into the network, the attacker continues ongoing access through shifting via the compromised surroundings and acquiring extended privileges through the use of diverse tools.

For an attacker, privilege escalation isn't a standalone measure. It is usually a part of a method referred to as lateral movement, which takes a region following the compromise of an endpoint. The attacker will usually integrate privilege escalation with a try and circulate laterally throughout the networks to compromise extra machines and accounts.

8. Valuable countermeasure for Privilege Escalation and Lateral Movement?

The following are some vital nice practices that may lessen the danger of a hit privilege escalation and lateral movement attacks.

- End-user strong password policy.
- Mandatory have Privilege Access Management Policies and Tools.
- Have Strong Firewall Policies / No permit any – any Policies / Allow individual what is wanted or Close unused ports and restriction record get admission to
- Secure, Record, Audit System Admin, databases and sanitize end-user inputs and force
- Keep your machine and programs patched and updated. Checking the system with Patching and Vulnerability Scanning tools.

VIII. CONCLUSION

In this survey paper it mainly describes how reconnaissance phase works and their methodology along with techniques against attacks and vulnerabilities. Reconnaissance is a primary and beginning segment of any cyber-attack so if any solution for detecting cyber reconnaissance may be an excellent fulfillment in the direction of improvement on powerful early warning system.

It is necessary to understand about the intentions, mentality and working of hacker, ethical hacker and cyber security tools which is very crucial in order to protect the data available in public domains. The benefits of better knowledge about cyber security tools can identify and prevents lot of attacks surfacing applications and as well as web applications or anything which have IP address.

Reconnaissance is an essential first phase of cyber security which speed up the process of information gathering against the target or hacker using open source tools.

Since the technology's advancement, day by day lots of vulnerabilities are been discovered surfacing over application software and web application. It is an early warning to all the cyber security professional, researcher and students throughout the worldwide to work hard in finding the effective solutions for upcoming threats and existing threats.

REFERENCES

[1] Wojciech Mazurczyk, Luca Caviglione, Cyber Reconnaissance Techniques, Communications of the ACM, Vol. 64 No. 3, Pages 86-95 10.1145/3418293, March 2021

International Journal of Science, Engineering and Technology

An Open Access Journal

[2] Shanto Roy, NaziaSharmin, Jamie C. Acosta, Christopher Kiekintveld, Aron Laszka, Survey and Taxonomy of Adversarial Reconnaissance Technique, arXiv:2105.04749v1 [cs.CR], May 2021.

[3] Danda B. Rawat, Journal on Cyber security and Privacy, Journal of Cyber security and Privacy: A New Open Access Journal, 2021.

[4] Abdulkadir Bilen and Ahmet BedriAzur, Cyber-attack method and perpetrator prediction using machine learning algorithms, s. PeerJComput. Sci. 7: e475 DOI 10.7717/peerj-cs.475, 2021.

[5] Ahmad Mtair AL Hawamleh, AlorfiAlmuhannadSulaiman M, Jassim Ahmad Al-Gasawneh, Ghada Al-Rawashdeh, Cyber Security and Ethical Hacking: The Importance of Protecting User Data Solid State Technology, Volume: 63 Issue: 5, 2020

[6] Rohit Kalakuntla, AnveshBabuVanamala, Ranjith Reddy Kolipyaka, Cyber Security, 2019, HOLISTICA Vol 10, Issue 2, pp. 115-128, 2019.

[7] IdimadakalaNagaraju , Ethics in Ethical Hacking , International Journal of Scientific & Engineering Research, Volume 4, Issue 10,ISSN 2229-5518, 2018.

[8] Saloni Khurana, A Review Paper on Cyber Security International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org, VIMPACT - 2017 Conference Proceedings, 2017.

[9] Pavan Kumar, K. Pranathi, A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime. JAC: A Journal of Composition Theory Volume XIV, Issue IV, APRIL 2021 ISSN: 0731-6755,2017.

[10] Brijesh Kumar Pandey, Alok Singh and Lovely lakhmaniBalani, ETHICAL HACKING (Tools, Techniques and Approaches, Conference Paper • January 2017(CAIM-International Conference on Advancement in IT and Management At: Thakur Institute of Management Studies Career Development and Research Thakur Village Kandivali East Mumbai),2017

[11] Victor-Valeriu Patriciu and Adrian Constantin Furtuna, Guide for Designing Cyber Security Exercises recent advances in e-activities, information security and privacy (ISSN: 1790-5117 ISBN: 978-960-474-143-4), 2016

[12] https://owasp.org/www-project-top-ten/: Vulnerabilities in web applicationsWorkshops, certification and training on cyber security.

[13] https://www.eccouncil.org/ethical-hacking/: Ethical Hacking learning's