International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

Cyber Security: The Study on Information Gathering

Varun Verma, Saurabh Kumar Dubey, Tajwar Khan, Prem, Himanshu Pandey
Department of CSE,
Lovely Professional University, Jalandhar, India
varun2awesome@gmail.com, dubeysaurabh592@gmail.com, tajwarkhan2@gmail.com, Premy1325@gmail.com

***Abstract*- Internet-wide network scanning has numerous security applications, including exposing new vulnerabilities and tracking the adoption of defensive mechanisms, but probing the entire public address space with existing tools is both difficult and slow. We introduce GRABIN - An automated Cyber Security tool by which we can gather the information about the particular target like we can gather the information about domains, subdomains, users, user emails, open ports, their IP addresses and much more. Also, we are able to find web App vulnerabilities in the proper CVE format, and we are able to hash the values and we can encrypt and decrypt out messages by using the tool. We present the scanner architecture, experimentally characterize its performance and accuracy, and explore the security implications of high speed Internet-scale network surveys, both offensive and defensive. We also discuss best practices for good Internet citizenship when performing Internet-wide surveys, informed by our own experiences conducting a long-term research survey.**

***Keywords*- Information gathering, cyber security, penetration testing.**

I.INTRODUCTION

Information gathering is the associated art of gathering data regarding your target. Before hacking into websites or Systems you have got to achieve the maximum amount of data as doable regarding your target.

Gathering data is very vital. If the number of knowledge collected isn't comfortable, or as an alternative, if the target is tightly defended, no attacks are launched.

If the knowledge gathered shows a poorly defended computer system, associate attacks are launched, and unauthorized access is gained. However, if the target is very protected, the hacker can turn over before making an attempt to interrupt in. it'll be dependent upon the tools and systems that shield the target. Again, the key here is the quantity of data he has gathered beforehand.

II. BACKGROUND

From the 40s to the current, discoveries however cybersecurity have developed to become what we all know now a days.

This race has been occurring since the Nineteen Fifties, and this explains the evolution of cyberattacks and security solutions.

- **1940s:** The time before crime
- **1950s:** The phone phreaks
- **1960s:** All quiet on the Western Front
- **1970s:** Cyber security is born
- **1980s:** From ARPANET to net
- **1990s:** The globe goes on-line
- **2000s:** Threats diversify and multiply
- **2010s:** Next generation

1. >1940s: The time before crime:
For nearly 20 years when the creation of the world's initial electronic computer in 1943, finishing up cyberattacks was tough. Access to the enormous electronic machines was restricted to little numbers of individuals and that they weren't networked – a very number of people knew a way to work them therefore almost no threat was in existence. Interestingly, the idea underlying viruses was initially made public in 1949, once pioneer John von Neumann speculated that programs may reproduce.

2. >1950s: The phone phreaks:
The technological and subcultural roots of hacking are mainly related to the maximum amount of early telephones as they're to computers.

In the late 50s, 'phone phreaking' emerged. The term captures many strategies that 'phreaks' – individuals with a selected interest within the workings of phones – accustomed to hijack the protocols that allowed telecoms engineers to keep their work continue on the network remotely to form free calls and avoid long-distance tolls.

Sadly for the phone corporations, they can't find any method of stopping the phreaks, though that eventually died in the 80s.The phreaks had become a community, even issue newsletters, and enclosed technological trailblazers like Apple's founders Steve Wozniak and Steve Jobs. The mildew was set for digital technology.

3. >1960s: All quiet on the Western Front:

© 2021 IJSRET

International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

The first-ever reference of malicious hacking was within the Massachusetts Institute of Technology's student newspaper.

Even by the mid-1960s, most computers were immense mainframes, kept away in secure temperature-controlled rooms. These machines were terribly pricey, therefore access – even to programmers – remained very limited.
However, there have been early forays into hacking by a number of those with access, usually students. At this stage, the attacks had no economical, commercial or geo-political advantages. Most hackers were curious mischief-makers or people who sought-after to enhance existing systems by creating them to work a lot quickly or expeditiously.

In 1967, IBM invited youngsters mainly school kids to give them an opportunity to try their latest computers. When done exploring the accessible elements of the system, the kids worked to probe deeper, learning the system's language, and gaining access to alternative elements of the system. This was a valuable lesson to the corporate and that they acknowledged their gratitude to "a variety of school students for his or her compulsion to bomb the system", that resulted within the development of defensive measures – and presumably the defensive attitude that might prove essential to developers from then on. Ethical hacking is still being practiced nowadays.

As computers began to cut back in size and value, several giant corporations invested in technologies to store and manage information and systems. Storing them locked and key became redundant as a lot of folks required access to them and passwords began to be used.

4. >1970s: cybersecurity is born:
The proper beginning of cybersecurity was with a research project ARPANET [Advanced Research Project Agency Network] in 1972. it was a precursor to the internet.

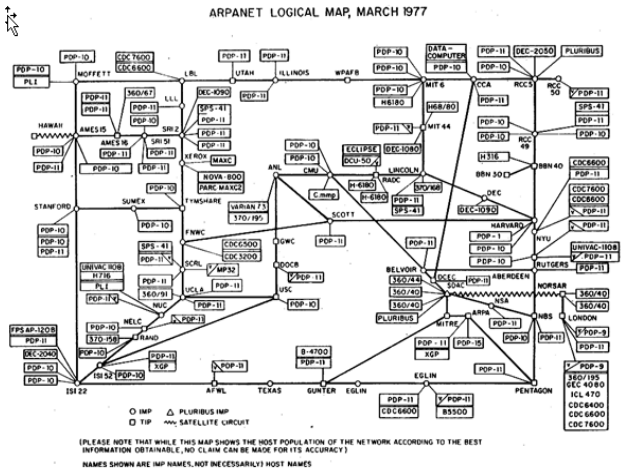

Fig 1. (This Diagram depicts the protocols developed by ARPANET for remote computer networking.)

A researcher Bob Thomas created a program named Creeper that could easily move across ARPANET's network and also was leaving a breadcrumb trail in its back from wherever it passed. The trail and message it was leaving says that "'I'm the creeper, catch me if you can".

Ray Tomlinson – the discoverer of email – wrote the program Reaper, which pursued and deleted Creeper. Reaper wasn't solely an initial example of an antivirus program, however it had been conjointly the primary self-replicating program and also was the first-ever PC worm.

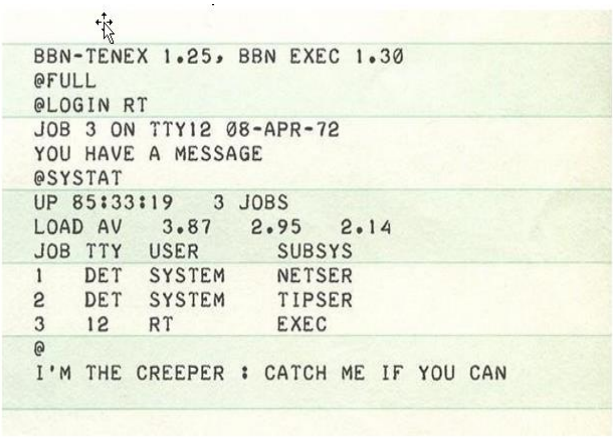

Fig 2. Ray Tomlinson

The above image depicts a very good example of creeper's taunting message.Challenging the vulnerabilities in these rising technologies became very necessary as many organizations were setting out to use the telephone to establish remote networks. Each and every new connected hardware piece presented a new entry point for which protection is required. As dependencies on computers accumulated and networking grew, it became much and much clear to governments that security was essential, and unauthorized access to databases and systems might be dangerous. From 1972 to 1974 a markable increment in discussion towards computer security was done and that was mainly by papers (academics).

Creation of computer security in early time was undertaken by ESD and ARPA with the U.S. Air Force and different organizations that worked in cooperation to design and develop a security kernel for the Honeywell Multics (HIS level 68) system. UCLA and also the Stanford Institute of research worked on the same project.
ARPA's Protection Analysis project explored software package security; characterise, wherever possible, auto matable techniques for police investigation vulnerabilities in packages. By the mid-1970s, the definition of cyber security was maturing. In 1976 software package Structures to Support Security and Reliable package stated: "Security has been playing a vital and difficult goal within the architecture of systems."

© 2021 IJSRET

In 1979, 16-year-old Kevin Mitnick magnificently hacked into The Ark – the computer system at the Digital equipment Corporation used for developing OS – and created copies of the package. He was arrested and confined for what would be the primary of many cyberattacks he conducted over consecutive few decades. These days he runs Mitnick Security Consulting.

5. >1980s: From ARPANET To Global Internet:

The 80s brought a rise in high-profile attacks, as well as those at National CSS, AT&T, and Los Alamos National Laboratory. The motion picture War Games, during which a scoundrel worm takes over nuclear missile systems beneath the story of a game, was launched in 1983. This was a similar year when the terms Trojan Horse and Computer Virus were introduced.

During the cold war conflict, the threat of cyber spying evolved. In 1985, The United state Department of Defense released the trustworthy computer system evaluation Criteria globally known as The Orange Book that provided steerage on:

- Assessing the degree of trust which will be placed in code that processes classified or sensitive info.
- What security measures makers required to follow during the building of their commercial product.

Despite this, in 1986, German hacker Marcus Hess used an online gateway in Berkeley, CA, to piggyback onto the ARPANET. He hacked four hundred military computers, as well as mainframes at the Pentagon, desiring to sell info to the Soviet KGB.

Security began to be taken a lot seriously. Savvy users quickly learned about monitoring of the command.com file size, having detected that a rise in size was the primary sign of potential infection. Cybersecurity measures incorporated this thinking, and an abrupt reduction in free operable memory remains a signal of attack this day.

6. 1987: The birth of cyber security:

1987 was the year when commercial antivirus were born,though there were competitor claims for the innovation of the initial antivirus product.

- Andreas Lüning and Kai Figge launched their 1st antivirus product for the Atari ST – that conjointly saw the launch of ultimate Virus Killer (UVK).
- The first version of NOD antivirus was created by three Czechoslovakians.
- In the USA, McAfee was founded and launched by John McAfee. it was a part of intel security at that time.

One of the earliest documented 'in the wild' shows thatGerman Bernd Fix was used to perform virus removals when he neutralized the infamous Vienna virus.(it was a malware that spreads and corrupts files.)

The encrypted Cascade virus that infected. COM files, 1st appeared .A year later, Cascade caused a major incident in IBM's Belgian branch and served impetus for IBM's antivirus development.Before this, any antivirus solutions developed at IBM had been meant only for internal use.

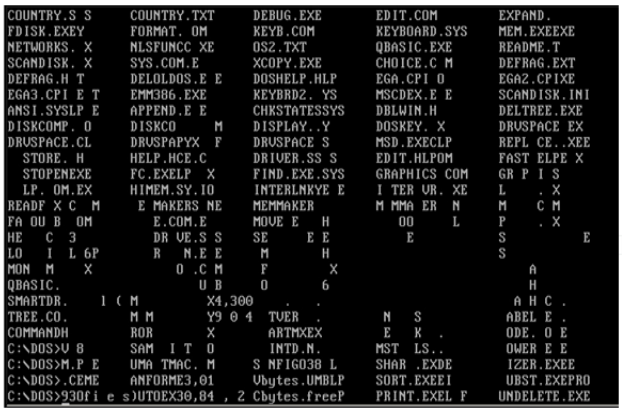

Fig 3. **Text Here your Fig Title.**

This picture depicts text falling to the bottom of the screen and was an effect of cascade virus.

By 1988, several antivirus corporations had been established round the world Early antivirus software systems consisted of straightforward scanners that performed context searches to notice distinctive virus code sequences. several of those scanners additionally enclosed 'immunizers' that changed programs to form viruses assume the pc was already infected and not attack them. because the variety of viruses raised into a whole bunch, immunizers quickly became ineffective.

It was additionally turning into clear to antivirus corporations that they might solely react to existing attacks, and an absence of a universal and omnipresent network (the internet) created updates exhausting to deploy.

As the world slowly began to notice pc viruses, 1988 additionally witnessed the primary electronic forum dedicated to antivirus security – Virus-L – on the Usenet network. The last decade additionally saw the birth of the antivirus press: UK-based Sophos-sponsored Virus Bulletin and Dr. Solomon's Virus Fax International.

The decade closed with a lot of additions to the cybersecurity market, as well as F-Prot, ThunderBYTE, and Norman Virus management. In 1989, IBM finally commercialized their internal antivirus project and IBM Virscan for MS-DOS went on sale for $35.

7. >1990s: the globe goes on-line 1990 was quite an year:

- The first polymorphic viruses were created (code that mutates whereas keeping the first algorithmic program intact to avoid detection).

© 2021 IJSRET

- British magazine pc today launched edition with a free disc that 'accidentally' contained the DiskKiller virus, infecting tens of thousands of computers.
- EICAR (European Institute for Computer Antivirus Research) was established.

Early antivirus was totally signature-based, comparing binaries on a system with databases related to virus 'signatures'. This meant that early antivirus created several false positives and used loads of procedure power – that makes a user frustrated as productivity slowed. As more and more antivirus scanners hit the market, cybercriminals were responding and in 1992 the 1st anti-antivirus program appeared.

By 1996, several viruses used new techniques and innovative strategies, as well as concealment capability, polymorphism, and 'macro viruses', leading to a whole new set of challenges for antivirus vendors to develop new detection and removal capabilities. New virus and malware numbers exploded during the 90s, from tens of thousands early within the decade growing to five million per annum by 2007. By the mid-'90s, it had been clear that cybersecurity had to be a part of mass production in order to keep the general public safe.

One NASA research worker developed the 1st firewall program, modeling it on the physical structures that stops the spread of actual files in the system.

In the late 90s they were additionally marked by conflict and friction between antivirus developers:

- McAfee accused Dr. Solomon of cheating so testing of clean discs showed sensible speed results and therefore the scan tests of virus collections showed sensible detection results. Dr. Solomon's filed suit in response
- Taiwanese developer Trend Micro accused McAfee and Symantec of violating its patent on virus scan-checking technology via the net and piece of email. Symantec then accused McAfee of mistreatment code from Symantec's Norton AntiVirus.

Heuristic detection additionally emerged as a brand new methodology to tackle the large variety of virus variants. Antivirus scanners began to use generic signatures – typically containing non-contiguous code and mis treatment wildcard characters – to discover viruses even though the threat had been 'hidden' within purposeless code.

Email: a blessing and a curse Towards the tip of the 90s, email was proliferating and whereas it was secure to revolutionize communication, it became a brand new entry point for viruses.

In 1999,Melissa virus appeared. It entered the user's pc via a Word document and so emailed copies of itself to the 1st fifty email addresses in Microsoft Outlook. It remains the one of the max spreading viruses and therefore the harm value was around $80 million.

8. >2000s: Threats diversify and multiply:

With the web offered in additional homes and offices across the world, cybercriminals had a lot of devices and package vulnerabilities to take advantage of than ever before. And, as a lot of information was being unbroken digitally, there was a lot of to plunder.

In 2001, a replacement infection technique appeared: users not required to transfer files – visiting infected websites was enough as dangerous actors replaced clean pages with infected ones or hid malware on legitimate webpages. Instant messaging services conjointly began to urge attacks, and worms designed to propagate via IRC (Internet Chat Relay) channel conjointly arrived.

The development of zero-day attacks, that take advantage and use of 'holes' in security measures for new packages and applications, meant that antivirus was being less effective – you can't check code against existing attack signatures unless the virus already exists within the database. pc magazine c't found that detection rates for zero-day threats had decreased from 40-50% in 2006 to solely 20-30% in 2007.

A key challenge of antivirus is that it will typically slow a computer's performance. One answer to the present was to maneuver the code off the pc and into the cloud. In 2007, Panda Security combined cloud technology with threat intelligence in their Antivirus product – an industry-first. McAfee Labs followed suit in 2008, adding cloud-based anti-malware practicality to VirusScan. In the subsequent year, the Anti-Malware Testing Standards Organization (AMTSO) was created and began operating shortly once on a way of testing cloud products.

Another innovation this decade was OS security – cybersecurity that's engineered into the OS, providing an extra layer of protection. This typically includes performing regular OS patch updates, installation of updated antivirus engines and code, firewalls, and secure accounts with user management. With the proliferation of smartphones, antivirus is needed and developed in the windows and android phone world.

9. >2010s: Next generation:

- The 2010s saw several high-profile breaches and attacks getting down to impact the national security of several nations and cost businesses millions.
- **2012:** Saudi hacker 0XOMAR publishes sensitive details of quite four millions credit cards on the internet.
- **2013:** Former CIA worker for the Edward Snowden traced and leaked classified info from the National Security Agency (NSA).
- **2013-2014:** Malicious hackers broke into Yahoo, compromising the accounts and private info of its three

© 2021 IJSRET

billion users. Yahoo was later penalised $35 million for failing to disclose the news.

- **2017:** WannaCry ransomware infects 230,000 computers.
- **2019:** New Zealand's stock market forced to close due to Multiple DDoS attacks.

The increasing connectedness and the ongoing digitization of many aspects of life continued to offer cybercriminals new opportunities to exploit. Cybersecurity tailored specifically to the needs of businesses became more prominent and in 2011, Avast launched its first business product.

As cybersecurity developed to tackle the expanding range of attack types, criminals responded with their own innovations: multi-vector attacks and social engineering. Attackers were becoming smarter and antivirus was forced to shift away from signature-based methods of detection to 'next generation' innovations. Next-gen cybersecurity uses different approaches to increase detection of new and unprecedented threats, while also reducing the number of false positives.

It typically involves: Multi-factor authentication (MFA).

- Network Behavioural Analysis (NBA)–identifying malicious files based on behavioral deviations or anomalies Threat intelligence and update automation
- Real-time protection–also referred to as on-access scanning, background guard, resident shield and auto-protect
- Sandboxing – creating an isolated test environment where you can execute a suspicious file or URL
- Forensics – replaying attacks to help security teams better mitigate future breachesBack-up and mirroring
- Web application firewalls (WAF) – protecting against cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.

III. IMPORTANT OF INFORMATION GATHERING

Gathering information is that the beginning wherever a hacker tries to induce data regarding the target. Hackers use completely different sources and tools to induce additional data, and a few of them square measure shortly explained here. This information is helpful for you to become associated with Nursing moral hackers. The purpose of data gathering is to support the look of your organization's work to become a lot of totally inclusive.

- It is vital to appear at out there facts -- objective data, together with demographics and best practices.
- It is additionally important to appear at neutral views subjective data, together with the opinions of your purchasers, potential purchasers, staff, board members, donors, etc. concerning the work that you just do and the way you are doing it.

Security may be a broad and invasive domain within the computer network. The foremost important step in Security to solve any drawback is "Information Gathering."

Many of the protection vulnerabilities discovered were a result of operation. Even the oldest of the protocol has some flaws, only on through learning the planning & implementation they will be discovered. Isn't this what we have a tendency to decide operations? Let's take Associate in Nursing analogy from the real world. A patient goes to a doctor with some issues. The doctor collects the importance of the patients and suggests tests if needed. This diagnosis is an operation. To cure any problem the doctor learns from literature and alternative doctors, that is additionally a method of knowledge Gathering.

Similarly, is that the cyber world. to try to do any task, information concerning the task is required. The background concerning the task is additionally important, to solve it. This background includes literature and documentation of tools, protocols and far a lot of. however things work ought to additionally not be neglected. of these areas a method of knowledge Gathering. over and over individuals new security forget this step and cause damage not solely to others, however additionally to themselves. So, do preparation of knowledge Gathering before diving into finding a security drawback or a hack, else you'll be associated with this culture as expected.

Critical Thinking starts with gathering information. the majority skip this step and go right to the choice creating method that sends them down the incorrect path right from the beginning. You have already got some data supporting your own data and experiences.Your past experiences will assist you to form selections concerning current things. However, so as to urge the most effective outcome, it's necessary that you simply have all of the knowledge associated with this state of affairs. Gathering data is the most significant part of the important thinking method. obtaining all of the knowledge you wish to form a call can continuously cause the most effective outcome.

Depending on the depth of your information-gathering method, compiling the knowledge you collected is also straightforward or a lot of complicated:

If you have got resources, you'd like to save lots of time by hiring somebody to compile the knowledge. If you do not have resources to rent somebody, establish somebody in your organization UN agency has comfort and talent with basic program usage to assist with this as a part of the inclusiveness initiative. Or, you'll need to use a volunteer like a college boy UN agency is curious about the topic of inclusiveness. so as to separate up the work, you'll choose

© 2021 IJSRET

one individual to compile the prevailing information and another to figure with neutral perceptions.

Researching, or gathering information, is trying unless you've got a method in place. There are such a large amount of resources obtainable it is laborious to understand wherever to start out. Here ar 5 steps to follow to change the method of gathering information:

- Ask the proper queries
- Find information sources
- Notice the information you would like from your sources
- Apply your own knowledge and experiences
- Contemplate several sources

IV. TECHNICS OF INFORMATION GATHERING

Information Gathering is that the act of gathering completely different styles of info against the targeted victim or system. it's the primary step or the start stage of moral Hacking, wherever the penetration testers or hackers (both black hat or white hat) performed this stage; this can be a necessary and crucial step to be performed. The additional the data gathered concerning the target, the additional the likelihood to get relevant results.

Operation isn't simply a section of security testing; it's associate degree art that each penetration-tester (pen-tester) and hacker ought to master for a much better expertise in penetration testing.

There are varied tools, techniques, and websites, as well as public sources like Whois, nslookup which will facilitate hackers gather info. This step is important as a result of you would like any info (such as his hypocorism, best friend's name, age, or signaling to perform word dead reckoning attack or different kinds of attacks) whereas performing arts attacks on any target.

Information gathering can be classified into three major categories:

- Footprinting
- Scanning
- Enumeration

1. Footprinting: Footprinting is the technique to gather the maximum amount of data as potential regarding the targeted network/victim/system. It helps hackers in numerous ways to get in an associate organization's system. This method also determines the protection postures of the target. Footprinting will be active moreover as passive.

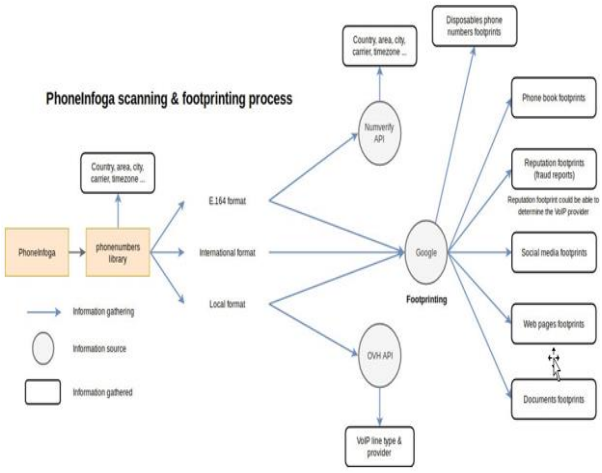

Fig 4. Footing Printing.

Passive footprinting/pseudonymous footprinting involves grouping knowledge while not the owner, knowing that hackers gather his/her knowledge. In distinction, active footprints square measure created once personal knowledge gets free consciously and by choice or by the owner's direct contact. Other than kinds of footprinting, some branches of footprinting a learner ought to apprehend before gathering information.

- Open-Source Footprinting.
- Network-based Footprinting.
- DNS Interrogation.

2. Who is? Who is could be a known net record listing tool to spot UN agency owns a site or UN agency registers for that individual domain along with their contact details. The web Corporation for appointed Names and Numbers (ICANN) regulates domain registration and possession details. Whois records have tried very helpful and have developed into a vital resource for maintaining the name registration and web site possession process's integrity.

3. Harvester: Harvester is additionally AN information-gathering tool that helps you extract the email address and subdomains of a specific target. Harvester is coded employing an easy python script that searches data from large search engines like Google, Yahoo, Bing, and far additional.

4. Metagoofil: Metagoofil is another operation or footprinting tool used for extracting data or knowledge that is publicly offered on the web happiness to the corporate

5. Netifera: Netifera is a potent tool that provides a whole platform to assemble info relating to the targeted web site you wish to attack. It is a free tool that comes built-in with the UNIX operating system OS. This computer code can provide info like information processing address, the artificial language used for website development, the amount of internet sites hosted, DNS.

© 2021 IJSRET

We can gather information from alternative sources like social networking sites (Facebook, Twitter, LinkedIn, etc.) wherever general users share their personal information and extra information associated with them. Even search engines play a big role in gathering information.

Hackers may also gather information from varied monetary services of a couple of companies, like the value of a company's shares, company profile, competition details, etc.

Hackers can also collect information from the email header, which includes:

- Address from which message was sent.
- Sender's email server.
- Sender's IP address.
- Date and time received by the originator's email server.
- The sender's mail server uses the authentication system.
- Sender's full name.

6. Objective of footprinting:

6.1 Collect Network Information:- like name, Internal domain names, science addresses of the accessible systems, rascal websites/private websites inside the domain, Access management Mechanisms, protocols used, existing VPNs, analog and digital phone numbers, authentication mechanisms, and system enumeration.

6.2 Collect System Information:- like users and cluster names, system banners, routing tables, and also the routing protocols it's exploitation, SNMP data, system design, software package used, remote system sort, username, and passwords.

6.3 Collect Organizations' Information:- like worker details, organization's web site, company directory, native details, address and phone numbers, comments in HTML ASCII text file at intervals associate organization's web site, security policies enforced, internet server links relevant to the organization, news articles and announcement.

2. Scanning:

Scanning is another essential step that is important, and it refers to the package of techniques and procedures accustomed to determine hosts, ports, and various services at intervals in a network.

Network scanning is one among the parts of intelligence gathering and knowledge retrieving mechanism Associate in Nursing assaulter accustomed to produce an summary situation of the target organization (target organization: suggests that the cluster of individuals or organization that falls within the prey of the Hacker).

Vulnerability scanning is performed by pen-testers to sight the likelihood of network security attacks. This system junction rectifier hackers to spot vulnerabilities like missing patches, supererogatory services, weak authentication, or weak coding algorithms.

Thus a pen-tester Associate in Nursing moral hacker lists down all such vulnerabilities found in an organization's network.

Scanning is of three types:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Tools which will ar accustomed scan networks and ports are:

2.1 Nmap: extract information like live hosts on the network, services, form of packet filters/firewalls, operating systems, and OS versions.

```
root@bt:~# nmap -Pn -sS -A 172.16.32.131
Nmap scan report for 172.16.32.131
Host is up (0.0035s latency).
Not shown: 993 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
```

2.2 Angry IP Scanner: scans for systems on the market during a given input vary.

2.3 Hping2/Hping3: It is command-line packet crafting and network scanning tools used for TCP/IP protocols.

2.4 Superscan: It is another powerful tool developed by Mcafee, that may be a protocol port scanner, also used for pinging.

2.5 ZenMap: It is another terribly powerful Graphical programme (GUI) tool to notice the sort of OS, OS version, ping sweep, port scanning, etc.

2.6 Net Scan Tool Suite Pack: It may be an assortment of various kinds of tools which will perform a port scan, flooding, webrippers, mass mailers; and This tool may be a trial version, however paid versions are on the market.

Wireshark and Omnipeek are 2 powerful and celebrated tools that hear network traffic and act as network analyzers.

Names of different celebrated PCs tools are Advanced Port Scanner, Net Tools, MegaPing, CurrPorts, PRTG Network Monitor, SoftPerfect Network Scanner, Network Inventory somebody, etc.

There are numerous different scanners on the market free and inherent in Kali UNIX operating system OS.

© 2021 IJSRET

Tools and software systems that are employed in mobiles as scanners embody the names like Umit Network Scanner, Fing, IP network Scanner, PortDroid network Analysis, Pamn IP Scanner, Nessus Vulnerability Scanner, Shadow Sec Scanner, etc.

V. TYPES OF INFORMATION GATHERING

Information gathering i.e, pre-attack phase is of two types.

- Passive Information gathering
- Active Information gathering

1. Passive Information Gathering:
In This type of information gathering, the attacker collects the publicly available information of the target. Passive information gathering has extremely low chances to get detected because there is no direct establishment between attacker and the target, Some tools for passive information gathering are whois, web spiders, Netcraft, google, maltego etc.

- We can extract these information from passive information gathering.
- Subdomains and public ip addresses.
- Leaked credentials.
- Publicly available sensitive documents and files.
- Directory listing.
- Usernames and passwords

2. Active Information Gathering:
In this type of information gathering the attacker is directly engaged with the target organization, with active information gathering an attacker can collect information related to operating system, portss, Dns information and many sensitive information.

In active information gathering there is a great chance to be detected by target IDS or IPS or Blocked by firewall. Tools related to active information gathering are Nmap/ Zenmap, dnsenum used for dns enumeration, Netcat (which is also known as swiss army knife), The harvester, Metagoofil, and many more tools which can collect tons of information about the target.

VI. CONCLUSION

The relevance of the information gathering is clear from the research point of view. This subject has been widely targeted by researchers of testing and safety, mainly because the number of flaws and vulnerabilities has increased in the last years. This paper focused on mapping the information gathering, identifying the application scenarios, usual tools and methodologies in different contexts, the main contributions and related challenges.

It was possible to draw some conclusions on how tools or methodologies are used for information gathering, network scanning, pre-invasion, post-invasion, and web analytics. From that, the results can help testers to define, within their testing scope, which tools or methodologies are indicated depending on the context or scope they will be applied. it would be important to have a set of recommendations aimed to improve and/or complement information gathering.

This set of recommendations can be based on the existing methodologies. Thus, a proposed set of recommendations /tools would address the strengths and limitations of the models and also would provide a flexible, dynamic, and many activities choices, steps, and other aspects inherent to an information gathering. Some preliminary results on a new methodology for information gathering that can be applied in different target scenarios.

VII. ACKNOWLEDGMENT

This research was supported by Lovely Professional University. We thank our colleagues from Lovely Professional University who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank Ms. Pawandeep kaur for guiding us throughout the research study, also her views that greatly improved the manuscript.

We would like to show our gratitude to her for sharing her pearls of wisdom with us during the course of this research, and we thank 3 “anonymous” reviewers for their so-called insights. We are also immensely grateful to our friends and family for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

[1] Wang, S., Wang, J., Feng, C., & Pan, Z. (2016). Wireless Network Penetration Testing and Security Auditing. ITM Web of Conferences, 7, 03001.
[2] Goel, J. N., & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber DefenceTechnology. Procedia Computer Science, 57, 710-715.
[3] B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016). Penetration Testing using Linux Tools: Attacks and Defense Strategies. International Journal of Engineering Research andTechnology, V5(12), 153-158.
[4] M. Reddy and P. Yalla, "Mathematical Analysis of Penetration Testing and Vulnerability Counter measures," IEEE International Conference on Engineering and Technology (ICETECH), pp. 1-5, 2016.

© 2021 IJSRET

[5] A. Bacudio, X. Yuan, B. Bill Chu and M. Jones, "An Overview of Penetration Testing," International Journal of Network Security & Its Applications (IJNSA, vol. 3, no. 6, pp. 19-38, 2011.
[6] B. Shivayogimath, "An Overview of Network Penetration Testing," International Journal of Research in Engineering and Technology, vol. 3, no. 7, pp. 408-413, 2014.
[7] "Open Information Systems Security Group", Information systems security assessment framework, 2006.
[8] Pentest-standard.org. (2018). The Penetration Testing Execution Standard. [online] Available at: http:// www.pentest-standard.org/index.php/Main_Page [Accessed 31 Mar. 2018].

© 2021 IJSRET