www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 4 April 2018, Page No. 23860-23865
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i4.10

Blended Extensibility of Cyber Forensics

Nikunj Pansari [1], Vijay Kumar Mall [2], Dhruwal Kushwaha [3]

[1,3]Information and technology,kiet group of institution,ghaziabad
[2]Electrical and electronics engineering,kiet group of institution,ghaziabad

Abstract
For today's attack-prone and vigorously developing world, network security is as important as eating food. This is because any pinch of vulnerable source (whether self or by-attacker) could adversely affect the end-user data, information as well as all useful assets. Cyber Forensics proves to be an advantage in presenting the evidence, against the court of law, if required, in defence of an attack. This can also help the end-user become more cautious and secure to repress against any kind of vulnerabilities. Generally, not many people are aware about it, which is the strongest reason for an attacker to commit the attack again.

***Keywords*-**attacker, attack-prone, cyber-forensics, network security, vulnerabilities, a victim, etc.

Introduction

Cyber Forensics (Computer Forensics) aims at investigation and analysis using various techniques to collect information and gather evidence about a particular computing device which makes it reasonable enough to defined against law, if required. It focuses on finding out the reasons and solutions behind a vulnerability or attack occurred.[7]
Forensic investigators have long been following defined methods called procedures. The first step of the process is the physical isolation which is done by the investigators. They make a digital copy of the storage media of the device, so that a copy is still in backup, within proximity, if any part of data gets lost. Duplication of original copy ensures that the investigation is done on that copy, so that the future prospects are safe in the original copy.[7]

There are various software and techniques used by the investigators, searching for unallocated space and hidden folders.
For any legal proceedings, verification of the digital copies is performed rigorously.[7]

This is the official website of cyber forensics which provides all the help, features and support in case of any cybercrime, cyber theft or any kind of problems related to any phishing attack. Cyber forensics has become an area of importance for all range of users, as it also provides coursework and certification, embedded with in-built security.[7]
Cyber forensics and Ethical hacking can certainly not go hand-in-hand. But, Ethical Hacking certainly provides end-user to know the consequences and major threats very closely, thus can work on to make the system, more secure and less vulnerable to attack.[7]

"No System/web app can be ideally called as fully secured."

Ethical Hacking

We often consider hacking as a crime, rather than regarding it as ethical. Hacking, as the term defines, is an activity which hackers use to play with the computer systems and networks. Now, it can be viewed as both Ethical or as a crime.[1]

Ethical hacker is someone who finds or identify the potential threats on a computer or network. An Ethical hacker aims to bypass the system security and exploit all the vulnerabilities.
Organisations usually employ hackers to maintain the security of their system, as well as identify and eliminate all weaknesses.
If the hacker uses the information, data or personal credentials in an unauthorized manner, in-order to harm the end-user directly, the it is considered to be an unethical hacking and is regarded as a crime in such cases.[1][2][5]

Domains of Hacking

a) Website Hacking
b) Network Hacking
c) Email Hacking
d) Ethical Hacking
e) Password Hacking
f) Computer Hacking[1][2][5]

Types Of Hacking

1)White hat hacker- They are referred to as good guys or ethical hackers of the hacking world as their major task is to remove vulnerabilities or faults from a system for a company.
They are known to have a recognized degree such as CEH (Certified Ethical Hacker) from the EC-Council.

2)Grey hat hacker- These are the hackers, which act upon situations, and cover large portions of hacking world. Their work can involve not stealing any information or money (may involve playing with a website or two, but unintentionally), and at the same time, not providing any help to the people, if required.[2][5]

3)Black hat hacker- These are the real hackers or so-called crackers. Their task is to ensure unauthorized access to any personal or useful information, that can be further used for any destructive purposes. They generally employ some simple hacking techniques for usage.[2][5]

4)Script Kiddie- They are the learners of the hacking world, as they usually replicate the codes and use it as a tool to attack, and, can usually attack through SQLinjection.
They basically use some software to ensure the attacks like DOS AND DDOS, by flooding an IP with excess Information.
These hackers are usually recognized by an anonymous group of hacker's communities.

5)Green hat Hacker-Babies of the hacking world. They are known to know just a brief about hacking, and often retaliated by the hacker's community for asking some fundamental queries. They listen to the answers, with the curiosity of a child.

considering the smallest 6)Blue hat Hacker-These are so called revenge taker (Script Kiddie) for their loss. They seek to extract their work from anyone who, they might think to be aggressive to them. Generally, employ multiple varieties of methods for forcing an attack onto the cracker. They don't have any zeal to learn. [

7)Red hat Hacker-They attack the cracker, by uploading viruses attack and leveraging system vulnerabilities, thus loophole to attack. They are not must worried about the businesses.

Network Security

Network Security is important to ensure that there is no unauthorized access of any kind of data, information or network components. It is ensured to maintain the efficient working of a healthy vulnerability free network. Network Security or Cyber Security also mainly focuses on fulfilling the three basic criteria-
a) Confidentiality
b) Integrity
c) Authenticity
One has to keep these in mind, while, looking for loopholes or defining system or network security.
Some of the important and useful concepts while dealing with network security are-

1)Cryptography-It basically follows the encryption mechanism, in which the plaintext is converted into cipher text and vice-versa. It involves maintaining the authenticity of the information. It can be Symmetric key cryptography or public key cryptography.

2)Firewalls-They act as a shield for a network, by providing a secure layer or filter to allow only required information to seep through, thus preventing the other useless or space consuming information to be denied. It can take place within a large set of networks.
These can be two types as listed:

a) Application-level: works at the application level to identify and protect the application.

b) Packet-filtering: works at the networking level. Used to filter packets being sent, to ensure that it doesn't contain the malicious information. [3]

3)Intrusion Detection System(IDS)-It is basically a software that is used to monitor, analyse and maintain all the network configurations of the system. It is designed to support all kinds of system requirements, and also facilitates for finding out any kind of malicious activity or work that might pertain the system to be hacked.

4)Digital Signatures-These are the verifiable and non-forgeable signatures or hand-written work, which is used for authentication of an individual or organisation. It inculcates cryptographic techniques to analyse and identify the signatures. Used nowadays, as a source of identification, in case of any attack.

There are various encryption and hashing algorithms being used to identify and fix loopholes in any website, system or network. Some of the most commonly and popularly known hashing algorithms are MD5, SHA1, SHA2, etc. These algorithms basically focus on the techniques to understand the logic behind any attack like password cracking or finding vulnerabilities.

Network Security as a branch can be very useful for the learners also, as it ultimately pertains in you the required skillset to protect the network and the system. It involves various keys for encryption and decryption, which makes it easier for the sender and receiver for communication.There are various types of network security as:

a) Firewalls
b) Access Control Mechanism
c) E-mail security
d) IDS
e) Antivirus and anti-malware system
f) Data loss prevention [8]

Investigation Methodologies-
O-Obtain information
S-make proper strategies
C-collect evidences
A-analyse
R-report
[3]

S.NO.	THREATS	DESCRIPTION	COUNTER MEAUSRES
(1)	DOS/DDOS	It basically involves flooding of useless and malicious generated packets to make the network system inappropriate for use/Multiple coordinated sources 'swamp' receiver.	a) filter out the flooded packets. b) traceback to source of the flood.
(2)	mapping	Using **ping** to identify the services of the network. Port Scanning to identify the attackable ports.	a) analysing-record the traffic entering the network. b) scan for IP addresses and ports
(3)	Packet Sniffing	Used for broadcast media, capable enough to read all the unencrypted data(promiscuous NIC mode)	a) checking, if the host is in promiscuous mode b) one host per segment of broadcast media.
(4)	IP Spoofing	Sending floods of IPs to disturb the flow of network communication	Ingress Filtering can be a useful option.
(5)	Password Cracking	Using various hashing algorithms to crack the passwords.	Secure the passwords by making it long, with using different set of characters.
(6)	Social Engineering	Psychological involvement of people into revealing some confidential information.	Protect the personal information wisely.
(7)	Phishing	**Attempt to identify some useful and confidential information of any website, individual or organisation by disguising or misleading them to** fake sites.	**Always attempt to think for a minute before clicking on any unknown** sources(websites).

Internet Security Threats-
There are varieties of Internet Security threats that one needs to be aware of, and thus protect the system, network from being hacked. These takes place basically because most of the people don't know about such attacks. People need to be aware of such vulnerabilities and loophole to curb the spreading of malicious viruses and attacks.[9]

Client/Server- Side Attacks
There are various tools which can be used for server-side or client-side attacks, classified under several domains.
Some Commonly used tools (penetration testing tools) are:

a) HTTrack-tool built for replicating the contents of a website such as the pages, its styles, and all the files in a controlled environment.
Command-
sudo apt-get install httrack[2][11]

b) DIG (Domain Information Groper)-It is a popularly known and used DNS Reconnaissance tool, which gives information about the system and the sub-domain.
Using it, specific DNS server can be used to queried directly. [2]

c)Fierce-It basically scans for non-contiguous IP and host names for various sub-domains. Works to

locate useful targets within and outside the network. It is available as a tool within Kali Linux or any other testing OS.

d)nmap-It is a security scanner, used to configure the network within the reach of the system. It involves host discovery, port scanning and OS detection also. Habitual to network features like congestion and latency, while scanning. In brief, it used as a medium to gather all useful information about a network.

Password Cracking Tools-

a) John-The Ripper-Attempts cracking passwords using sets or combinations of dictionary words. Appending or pre-pending of alphanumeric characters could be done to match the passwords.
Commands-
tr A-Z, a-z<CustomWordFile> All Lower-Case file
sort -u<AllLowerCasefile>No Duplicates or Uppercase
wc -l <No Duplicates or Uppercase>
(where tr-translate, sort-sorting the characters and wc -denotes the count of lines)[10]

b) Hydra-inculcates brute-force attack to test against different protocols. Ideal for an attack towards an e-mail server, since, Hydra targets the IP and the protocols used by e-mail systems like POP3 and SMTP.

Command-
hydra –l /usr/share/wordlists/metasploit/user -P /usr/share/wordlists/metasploit/ passwords ftp://(ip address) –V

-V: username and password(assumed)[9]

c)Rainbowcrack-Rainbow lookup table is used for cracking the hashes. This table
contains the files stored on disks. This tool is easily available in 'password attacks' in Kali Linux.

Command-
rcrack path (rainbow table) -f path (password hash) [10]

d)SQLdict-This tool uses SQL Server, by computing dictionary attack. Basic and easy to be used. Uses Target's IP address and Target's Account (Username) to initiate the attack.[10]

e) Johnny- It is a GUI version of the parent 'John-The Ripper' password cracking tool.
Generally, employed to crack weak passwords. Easy to work and implement interface. [10]

OTHER TOOLS-

a) Perl-based testing tool, works mostly on all the OS. Used to find out and identify the vulnerabilities of a web application, easily and effectively. Employs comprehensive tests on the web servers to detect malicious vulnerabilities.[10]

b) Nessus: Has to obtain a registration code from Tenable to use this tool. Used as a tool to scan a particular target device. It scans a maximum of 16 IP addresses and uses port no: 8834.
Available as a HomeFeed option or for a Professional use.
If we want to scan more IP, then Professional Pack should be used which is paid, but also delimits other limitations which were there in HomeFeed pack.[10]

c)Owasp-Zap: Also referred to as Zap Proxy. It is an intercept proxy defined for testing securely web applications employ SSL encryption mechanisms for functioning.
Also, been given flagship status.[10]

d)Metasploit: Used by the penetration testers for invoking unauthorised attack or exploitation of systems. postgressssql service is a pre-requisite for this tool to work.
It provides an ease to exploit known vulnerabilities in OS, network systems and web applications. Its framework can be used to design other testing tools.[10]

e) Wireshark: It is an open-source and free packet analyser, used for troubleshooting, analysis and maintenance of the network system. It is cross-platform but has a graphical front-end. It invokes offline facility and live capture. Output can be exported to an XML, CSV or plaintext format.[10]

f) Skipfish: Uses recursive crawls and dictionary-based probes for detection of vulnerabilities in a web app. Prepares an interactive sitemap for the target. It is fast, efficient and secured.[10]

g) WebSlayer: It is a brute-force tool used for getting the FORM, GET and POST parameters. Firefox often employ a plugin called 'Http Headers'. Basically, two formal parameters are necessary for it:
a) User-agent

b) Login Credentials[10]

Conclusion

Network Security is by far an important ingredient of the cyber world, as can be easily illustrated through growing demand of cyber security. One has to be at the edge to identify and improve all the loopholes of an existing leveraging system. Cyber forensics, in the coming era, would define the structure of the way, in which the network system is viewed at. Cyber Security and Cyber forensics are wholly inter-dependent on each other, thus catering the needs to maintain a vulnerability free system or network.[4][5]

A famous quote always stands still," Whenever**, you get something free, take it with a pinch of salt.**"

Acknowledgement

We would like to express our heartiest gratitude to all the preceding papers authors. These papers and references provided us with all the appropriate knowledge and determination for all our sincere efforts. Also, it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them.

Our family members were the most important sort of encouragement for us to define this paper. We would like to thank our parents, for their love and guidance in whatever fields we choose to pursue. They are our ultimate role models.

References

[1] Ethical Hacking by Ajinkya A. Farsole, Amruta G. Kashikar and Apurva Zunzunwala.

[2] Basics of Ethical Hacking by Chenchu Lakshmi S P I Basarkod

[3] IEEE journals and proceeding papers

[4] Ethical Hacking Techniques with Penetration Testing by K. Bala Chowdappa, S.Subba Lakshmi, P.N.V.S.Pavan Kumar .

[5] Comprehensive Study on Ethical Hacking by Er. Anjali Passi, Er. Priyanka Sharma.

[6] Ethical Hacking: A Security Technique by Sonal Beniwal, Sneha .

[7] http://www.cyberforensics.in/

[8] https://www.cybrary.it/

[9] https://www.cisco.com/c/en/us/products/security/index.html

[10] https://tools.kali.org/

[11] https://en.wikipedia.org/wiki/Kali_Linux

Nikunj Pansari

Nikunj Pansari is currently pursuing his Bachelor's degree of Technology in Information Techmology from KIET GROUP OF INSTITUTIONS, GHAZIABAD(affiliated to Dr. Abdul Kalam Technical University) .

He has his eyes set on becoming a Certified Ethical Hacker and a Licensed Penetration Tester, and is working hard in that direction. His other passions include learning about new technologies and is very passionate about Cricket as a sport.

vijay kumar mall

vijay kumar mall is currently pursuing his Bachelor's degree of Technology in Information Techmology from KIET GROUP OF INSTITUTIONS, GHAZIABAD(affiliated to Dr. Abdul Kalam Technical University) .

He is working on several projects based on embedded systems. And looking forward to do his

m.s in robotics and automation.

Dhruwal Kushwaha

Dhruwal Kushwaha is currently pursuing his Bachelor's degree of Technology in Information Technology from KIET GROUP OF INSTITUTIONS, GHAZIABAD(affiliated to Dr. Abdul Kalam Technical University).

He wants to pursue his Master's in Computer Science in the near future. An avid reader, he likes non-fiction works. His other interests include Chess and Automobiles.