ETHICAL HACKING AND SECURITY AGAINST CYBER CRIME

By

NEERAJ RATHORE

Assistant Professor, Department of Computer Science and Engineering, Jaypee University of Engineering and Technology, Guna, Madhya Pradesh, India.

ABSTRACT

This paper explores the fast growing Cyber world and its components over the internet. The fast growing Internet has benefited the modern society in the form of e-commerce, e-mail, online banking or system, advertising, vast stores of reference material, etc. But, there is also a dark side, where internet becomes a common and easy tool for the criminal activity using a weak link and vulnerability of internet. In this paper, the author concentrated over several hacking activity that come under Cyber crime. It also highlights the role of ethical hacker to evacuate from the culprits and cyber crime and illustrate on proactive approach to minimize the threat of hacking and Cyber crime.

Keywords: Hacking, Security, Cyber Crime, Ethical, Threat, Vulnerability.

INTRODUCTION

"Security is a state of well being of information and infrastructure in which the possibility of successful yet undetected theft, tempering and disruption of information and services are kept to low tolerable." [1]

- *Network Security:*

Protecting a network and data, computer program, other computer system assets from unwanted intruders, and unauthorized user [1-2].

- *Information Security:*

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

There are following security services issues as given below [3-5].

- Confidentiality
- Authentication
- Integrity
- No repudiation
- Access control
- Availability
- Authorization.

1. Hacking

The word "Hacking" term refers to the hobby/profession of working with computers. It describes the rapid development of a new program or reverse engineering of the existing software to make code better and efficient. Hacking divided into two terms: [6-8]

- Ethical Hacking
- Unethical Hacking

1.1 Ethical Hacking

The practice of breaking into computers without malicious intent, simply to find security hazards and report them to the people responsible. Ethical hacker refers to security professional who apply their hacking skills for defensive purpose and constructive purpose [9-12].

1.2 Unethical Hacking

Unethical Hacking is "cracking". Cracking activities is breaking the computer security without authorization or using technology, or tools (usually weak links of a computer, phone system or network) for vandalism, credit card fraud, identity theft, piracy, or other types of illegal activity. So, cracker refers to person who uses hacking skills or computer system knowledge for an offensive purpose [13-15].

2. What is Cyber Crime?

Cyber crime is the leveraging of a target's computer and information, particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure. According to Kevin G. Coleman at al., Cyber crime is defined as "The premeditated use of

disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

3. Importance of Ethical Hacking and How to Minimize The Security Threats

Ethical Hacker is a network and computer security professional who apply their knowledge and skills for a defensive purpose. Roles of an ethical hacker are followed [16-18]:

- Evaluate the Weak links of network and computer system.
- Find out the malicious contents from the network traffic.
- Trace out the cyber culprits by using some tools like tracing tools etc.
- Shutdown all the doors of network and operating system and information system for security pirates.
- Ethical hacker work as a security advisor of network and the computer system.
- Diagnose the security threat of the system.

  Restricts the unauthorized access of network or system by installing advanced security or IDS system.
- Protect the information system or network from Penetrating the Testing.

4. Major Disaster of Unethical Hacking

Unethical hacking is a cyber crime and being used as a prominent arm to make crime and cause million harms every day [19-21].

4.1 9/11 Demolition:

Most cruel face of this unethical hacking, are to hack the account, identity, penetrating in unauthorized network or system and sniffing the data, etc., not only for money but also to spread terrorism. 9/11 demolition is example of such kind of hacking which shocked the whole world and challenged the USA's network security. In this terrorist attack, all information are transferred over network using a new technique called stenography through which, all the encoded textual information was hidden into funny images by advanced program [22].

4.2 Virus Attack

The damage was not done to a person, but to the masses is the case of the Melissa virus. The Melissa virus first appeared on the internet in March 1999. It spread rapidly throughout the computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars damage to the computers worldwide [23].

5. Social Awareness and Precaution During Net Surfing

- Should not click any hyperlink if you are not sure about the link [24].
- Should not create unnecessarily many email accounts.
- Should not use an anonymous user id and password for net surfing.
- System should be password protected and should automatically lock when the system is idle for a long time.
- Destroy all the important material related to system, network, or id so that dumpster diving cannot be done.
- User id and password should be strong with special character and should be change periodically.
- We should not provide your personal information unnecessarily to unknown sites or we are not sure about the sites credibility.
- Use encryption and digital signature etc. techniques to transfer the important data.
- We should always avoid checking unknown greetings, downloading screen savers, or free software.
- We should avoid using pirated software.
- Vendor-supplied software should be free from bugs, missing operating system patches, vulnerable services, and insecure choices for default configurations.

6. Some System and Devices for Network Security

6.1 Intrusion Detection Systems (IDS)

An IDS monitors network traffic for any suspicious activity and alerts the system or the network administrator. IDS

may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. There are Network based (NIDS) and Host based (HIDS) Intrusion Detection Systems. Host Intrusion Detections Systems (HIDS) run on individual hosts or devices on the network and Network Intrusion Detection systems (NIDS) are placed at a strategic point within the network to monitor traffic to and from all devices on the network [25].

6.2 Firewall:

A firewall is a system that is set up to control traffic flow between two networks. Firewall is an effective means of protecting the network system from the threats and a single choke point that keeps an unauthorized user out of the protected network, and also prohibits potentially vulnerable services from entering and leaving the services [26].

6.3 Packet Filtering Firewall

A packet filtering firewall applies a set of rules to each incoming packets and then, forwarding or discarding them. These rules are based on source IP, port no, UDP, TCP, etc., [27].

6.4 Port Scanning:

A port scanner is a program which attempts to determine a list or range of open TCP, UDP, etc., ports on a list or range of IP addresses. Port scanners are used for network mapping and network security assessments. So, we have knowledge to disable (close) all doors (port) to prohibit the pirates for entering into the network [28].

6.5 IPSec

IPSec is a protocol suite which is used to secure communication at the network layer between two peers. When end-to-end security is required, it is recommended that, additional security mechanisms such as IPSec or TLS, can be used inside the tunnel, in addition to L2TP tunnel security [14].

6.6 ISAKMP

"Internet Security Association and Key Management Protocol (ISAKMP) " is a protocol for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques, and threat mitigation e.g. denial of service and replay attacks [12][13].

7. Network Security Essentials and Tools

7.1 Network Auditing

Network auditing software is an important security tool. It provides the IT administrators with a two-pronged approach to network security. First, it provides an accurate view of the entire network and subnets, making it easier to spot any open ports, unaccounted for components or other discrepancies. Second, it allows a prompt action to protect against any open vulnerability. Network security is not just about protecting an individual computer; it is also about identifying and correcting the vulnerabilities found in the entire network. Network auditing is fast indispensable tool in the maintenance of a healthy network [17].

7.2 Network Scanning Strengths

A network-based scanning assessment might detect extremely critical vulnerabilities such as, miss configured firewalls or vulnerable web servers in a DMZ that could provide a stepping stone to an intruder and allow them to quickly compromise an organization's security. Network scanners provide a comprehensive view of all operating systems and services running and available on the network [16].

7.3 Host-based Scanners

Host-based scanners detect signs that an intruder has already infiltrated a system. These hacker traces include suspicious file names, unexpected new files, or device files found in unexpected places. Network and host-based scanning technologies provides the best vulnerability assessment for measuring an organization's security risks [15].

7.4 DMZ (Demilitarized Zone)

DMZ is a firewall configuration for securing LAN. DMZ is a buffered zone that is placed between the trusted network (LAN) and un-trusted network (WAN or Internet). This is

considered as a Screened subnet or a separate network. DMZ is an additional firewall rule, meaning that, incoming requests reach the firewall directly. In a true DMZ, incoming requests must first pass through a DMZ computer before reaching the firewall. So, DMZ is a technique to protect the web server, data server, mail server and also the network from pirates [10],[11].

8. Wi-Fi Network Security

802.11 wireless LAN protocols (i.e. Wi-Fi protocol) have become the most popular protocol for wireless networking. So Wi-Fi network are most vulnerable, if the network administrator is completely aware about the security issues. So hacker can penetrate into the network by hiding their identity. Two WEP and WPA protocols are used to protect the wi-fi network. WEP (Wireless Equivalent Privacy) is an optional encryption standard for Wi-Fi network, implemented in the MAC layer. WEP uses a secret 40 or 64-bit key to encrypt and decrypt datagram. Wi-Fi Protected Access (WPA) is a certification (Authentication) program created by the Wi-Fi Alliance. WPA improves on the authentication and encryption features of WEP. One of the key technologies behind, WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP [8][9].

Conclusion

Internet is serving the modern society in several ways. But, It has several security breaches. These security breaches can be misused by black hats for offensive purposes. So, it is mandatory to determine the vulnerable points of the information system. There are various tools like firewall, gateways, IPSec, DMZ, network auditing, etc., evaluating the breaches and mitigating them by using tools and taking proactive action against them for averting from disaster. Few precautions and proactive actions can eliminate the hazard and cyber terrorism.

References

[1]. Rathore, Neeraj, and Inderveer Chana, (2014). "Job migration with fault tolerance based QoS scheduling using hash table functionality in social Grid computing". *Journal of Intelligent and Fuzzy Systems*, Vol. 27 No. 6, pp.2821-2833.

[2]. Rathore, Neeraj, and Inderveer Chana, (2015). "Variable threshold-based hierarchical load balancing technique in Grid". *Engineering with Computers*, Vol. 31 No.3, PP.597-615.

[3]. Rathore, Neeraj, and Inderveer Chana, (2014). "Load balancing and job migration techniques in grid: a survey of recent trends". *Wireless Personal Communications*, Vol.79 No.3, pp.2089-2125.

[4]. Rathore, Neeraj (2015). "Efficient Agent Based Priority Scheduling and Load Balancing Using Fuzzy Logic in Grid Computing". *i-manager's Journal on Computer Science*, Vol.3 No.3, PP. 11.

[5]. Rathore, Neeraj (2015). "Map Reduce Architecture for Grid". *i-manager's Journal on Software Engineering,* Vol.10, No.1, pp.21.

[6]. Sharma, Vishal, Rajesh Kumar, and Neeraj Rathore, (2015). "Topological Broadcasting Using Parameter Sensitivity-Based Logical Proximity Graphs in Coordinated Ground-Flying Ad Hoc Networks". *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol.6 No.3, pp.54-72.

[7]. Rathore, Neeraj, and Inderveer Chana, (2013). "Report on hierarchal load balancing technique in grid environment", *i-manager's Journal on Information Technology*, Vol.2 No.4, pp.21.

[8]. Rathore, Neeraj Kumar, and Inderveer Channa, (2010). "Check pointing Algorithm in Alchemi .NET". *ims Journal on Information Technology*. http://www.iuu.ac/pragyaan/Pragyaan_IT_June10.pdf.

[9]. Rathore, N. K., and I. Chana (2011). "A cogitative analysis of load balancing technique with job migration in grid environment", *IEEE Proceedings Paper*, Vol.77, No.82.

[10]. Rathore, Neeraj. and Inderveer Chana, (2013). "A sender initiate based hierarchical load balancing technique for grid using variable threshold value". *Signal Processing, Computing and Control (ISPCC), IEEE International Conference on IEEE*.

[11]. Neeraj Kumar Rathore and Inderveer Chana, (2008), "Comparative Analysis of Checkpointing". *PIMR Third National IT Conference*, IT Enabled Practices and Emerging Management Paradigm book and category is

Communication Technologies and Security Issues, pp.32-35, Topic No/Name-46, Prestige Management and Research, Indore, (MP) India, 2008.

[12]. Neeraj Rathore, "Implementing Checkpointing Algorithm in Alchemi.NET". ME Thesis, Thapar University, Patiala. Retrieved from http://hdl.handle.net/10266/658 http://dspace.thapar.edu:8080/dspace/bitstream/10266/658/3/T658.pdf

[13]. Neeraj Kumar Rathore and Inderveer Chana (2010). "Check pointing Algorithm in Alchemi.NET". Lambert Academic Publication House (LBA), Germany ISBN-10: 3843361371, ISBN-13:978-3843361378, Retrieved from https://www.lap-publishing.com/catalog/details/store/gb/book/978-3-8433-6137-8/checkpointing-algorithm-for-alchemi-net-in-grid

[14]. Neeraj Kumar Rathore and Anuradha Sharma (2015). "Efficient Dynamic Distributed Load Balancing Technique". Lambert Academic Publication House, Germany, Project ID: 127478, ISBN no-978-3-659-78288-6,retrieved from https://www.lap-publishing.com/catalog/details//store/gb/book/978-3-659-78288-6/efficient-dynamic-distributed-load-balancing-technique, http://www.amazon.com/Efficient-Dynamic-Distributed-Balancing-Technique/dp/3659782882.

[15]. Neeraj Kumar Rathore, (2015). "Load Balancing Algorithm for Grid" in *30th M.P. Young Scientist Congress*, Bhopal, M.P., pp-56.

[16]. Neeraj Kumar Rathore (2014). "An Efficient Hierarchical Load Balancing Technique for Grid". *29th M.P. Young Scientist Congress*, Bhopal, M.P., pp.55.

[17]. Rohini Chouhan and Neeraj Kumar Rathore (2012). "Comparison of Load Balancing Technique in Grid". *17th Annual Conference of Gwalior Academy of Mathematical Science and National Symposium on Computational Mathematics & Information Technology*, JUET, Guna, M.P., pp.7-9.

[18]. Neeraj Kumar Rathore and Inderveer Chana, (2010). "Fault Tolerance Algorithm in Alchemi.NET Middleware". *National Conference on Education & Research (ConFR10), Third CSI National Conference of CSI Division V*, Bhopal Chapter, IEEE Bombay, and MPCST Bhopal, organized by JUIT, India.

[19]. Neeraj Kumar Rathore and Inderveer Chana (2009), "Checkpointing Algorithm in Alchemi.NET", *Annual Conference of Vijnana Parishad of India and National Symposium Recent Development in Applied Mathematics & Information Technology*, JUET, Guna, M.P.

[20]. William Stallings. *Network Security Essentials*.

[21]. Cheng, P.et al., "A security Architecture for Internet Protocol", *IBM System Journal*.

[22]. Manidar Singh. Network Security notes, Thapar University, Patiala.

[23]. Biono Paul,. *Evaluation of Security Risks associated with Networked Information System,* RMIT University.

[24]. Chunk Semeria, *Internet Firewall Security.* Retrieved from http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html.

[25]. N. Ferguson and B. Schnier, A Cryptographic Evaluation of Ipsec. Retrieved from http://www.schneier.com/paperipsec.html.

[26] ISS Internet Security System. *Network and Host Based Vulnerability.*

[27] Christian Barnes, (2002). *"Hack Proofing of Wireless Network"*.

[28] Halil Ebrahim, Ihsan, Batmaz. *Wireless Network Security Comparison of WEP Mechanism,* WPA and RSN security protocols".

ABOUT THE AUTHOR

Dr. Neeraj joined the Department of Computer Science and Engineering at Jaypee University, Guna, M.P., India, in 2010 and is presently serving as an Assistant Professor in the Department. He has over 8 years experience of teaching, research as well as industrial experience of IT Industry (Computer Sciences Corporation) with the role of Software Engineer. He obtained his Ph.D. in Computer Science with specialization in Grid Computing (2014) and M.E. in Computer Engineering (2008) from Thapar University and B.E. in Computer Science and Engineering (2006). His areas of interests include Parallel and Distributed Computing, Grid Computing, DBMS and Data Structure. He has over 25 publications in International Journals and Conferences and books of repute. Under his supervision, 06 Master theses have been awarded and 1 PhD thesis is on-going.