American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-5, Issue-5, pp-01-05
www.ajer.org
Research Paper Open Access

Vulnerability Assessments in Ethical Hacking

Ashiqur Rahman[1], Md. SarwarAlam Rasel[2], Asaduzzaman Noman[3], Shakh Md. Alimuzjaman Alim[4]
[1](M.Sc in Information Technology (IT), Jahangirnagar University, Bangladesh)
[2](CSE, Royal University of Dhaka, Bangladesh)
[3](CSE, Royal University of Dhaka, Bangladesh)
[4](EEE, Royal University of Dhaka, Bangladesh)

ABSTRACT: *Ethical hackers use the same methods and techniques to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security. The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerabilities to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems. It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.*
Keywords *–Ethical Hacker, black hat, CERT, Integrity, Vulnerabilities.*

I. INTRODUCTION

Ethical hacking is a proactive form of information security and is also known as penetration testing, intrusion testing and red teaming. An ethical hacker is sometimes called a legal or white hat hacker and its counterpart a black hat, a term that comes from old Western movies, where the "good guy" wore a white hat and the "bad guy" wore a black hat. The term "ethical hacker" is frowned upon by some security professionals who see it has a contradiction in terms and prefer the name "penetration tester." Before commissioning an organization or individual, it is considered a best practice to read their service-level and code of conduct agreements covering how testing will be carried out, and how the results will be handled, as they are likely to contain sensitive information about how the system tested. There have been instances of "ethical hackers" reporting vulnerabilities they have found while testing systems without the owner's express permission. Even the LulzSec black hat hacker group has claimed its motivations include drawing attention to computer security flaws and holes. This type of hacking is a criminal offence in most countries, even if the purported intentions were to improve system security. For hacking to be deemed ethical, the hacker must have the express permission from the owner to probe their network and attempt to identify potential security risks.
Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

II. WHAT ARE VULNERABILITY ASSESSMENTS?

Vulnerability analysis consists of several steps:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs.

If security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability, or a responsible industry body such as the Computer Emergency Readiness Team (CERT), may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly.

The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a white hat using ethical hacking techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

"Vulnerabilities are the gateways by which threats are manifested"
- As documented by SANS

In other words, a system compromise can occur through a weakness found in a system. A vulnerability assessment is a search for these weaknesses/exposures in order to apply a patch or fix to prevent a compromise.

III. KEY TERMINOLOGIES

Threat: A threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system.

Exploit: An exploit is a defined as a technique to breach the security of a network or information system in violation of security policy.

Target of Evaluation: A target of evaluation is an IT system, product, or component that is identified subjected to a required security evaluation. This kind of evaluation helps the evaluator understand the functioning, technology, and vulnerabilities of a particular system or product.

Zero Day Attack: In a **zero day** attack, attacker exploits the vulnerabilities in software that is unknown to the vendor. This security hole is exploited by hackers before the vendor becomes aware and fixes it.

A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and asses their security. White hat hacker's usetheir skills to improve security by exposing vulnerabilities before maliciousshackers (known as black hat hackers) can detect and exploit them.

A black hat hacker is an individual with extensive computer knowledge whose purpose is to breach or bypass internet security. Black hat hackers are also known as crackers or dark side hackers.

The term "grey hat" or "gray hat" in Internet slang refers to a computer hacker or computer security expert whose ethical standards fall somewhere between purely altruistic and purely malicious.

IV. INFORMATION SECURITY

Fig: Information Security Algorithm

Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Confidentiality: Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

Integrity: To preserve the integrity of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it.

Availability: Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this standard, assets include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorized entities when they need to access or use them.

Authenticity: refers to characteristic of a communication, document, or any data that ensures the quality of being genuine or not corrupted from the original. The major roles of authentication include confirming that the user is who he or she claims to be and ensuring the message is authentic and not altered or forged. Biometrics, smart cards, and digital certificates are used to ensure authenticity of data, transactions, communications, or documents.

Non Repudiation: Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated. It is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

V. INFORMATION SECURITY THREAT'S

Natural threats: Natural disasters, Floods, Earthquakes, Hurricanes, Natural threats include above mentioned threats which cannot be stopped. Information damage or lost due to these type of threats cannot be prevented, hence safeguards against such threats should be taken by adopting disaster recovery plans and contingency plans.

Physical Security Threats: Damage of system resource, physical intrusion, Sabotage, espionage and errors Physical threats may include loss or damage of system resources through fire, water, theft, and physicalimpact. Physical impact on resources can be due to a collision or other damage, either intentionally or unintentionally. Sometimes, power may also damage hardware used to store information.

Human Threats: Hackers, Insiders, Social Engineering, Lack of awareness human threats include threats of attacks performed by both insiders and outsiders. Insider attacks refer to attacks performed by disgruntled or malicious employees. Outsider attacks refer to attacks performed by malicious people not within the organization. Insider attackers can be the biggest threat to information system as they may know the security posture of the information system, while outsider attackers apply many tricks such as social engineering to learn the security posture of the information system.

Based on the impact, Human threats can be classified into three types:

Network Threat: A network is defined as the collection of computers and other hardware connected by communication channels to share resources and information. As the information travels from one computer to the other through the communication channel, a malicious person may break into the communication channel and steal the information traveling over the network. The attacker can impose various threats on a target network:

1. Information gathering
2. Sniffing and eavesdropping
3. Spoofing
4. Session hijacking and man
5. SQL injection
6. ARP Poisoning
7. Password-based attacks

Host Threat: Host threats are directed at a particular system on which valuable information resides. Attackers try to breach the security of the information system resource. The following are possible threats to the host:

1. Malware attacks 5. Target Foot printing 8. Back door Attacks
2. Password attacks 6. Denial of service attacks 9. Privilege escalation
3. Arbitrary code execution 7. Unauthorized access
4. Physical security threats

VI. INFORMATION SECURITY THREAT'S

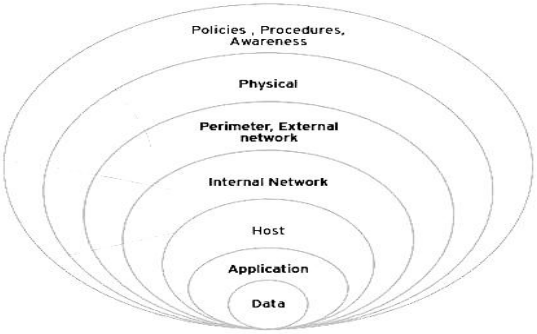

Fig 2: Information threat's

Perimeter, External Network Security: External, perimeter intrusive penetration testing should be carried out to simulate a destructive attack from the Internet, identifying system weaknesses and exploiting them to gain access to the organization's network and other confidential resources. These activities are aimed at testing the security configuration of the IT systems enabling Internet connectivity and controls.

Internal Network Security: An internal network scanning and attempts to gainaccess to the IT system from the internal networkwith no knowledge or limited prior knowledge of the computing environment which includes applications,database, operating systems and the networking technologies deployed.

Host Configuration review: A configuration review is undertaken on identifiednetwork components and servers configurations to determine mis-configurations.

Application Security: The application layer of the defense in depth model focuses on keeping applications on a host system and workstations secure. Applications are the software that manipulates the data, which is the ultimate attack target. Poorly protected applications can provide easy access to confidential data. These applications, such as customer relationship management and financial systems, can provide a target to individuals with malicious intent.

Data Security: The final layer in the Defense in Depth securitymodel protects the sensitive data itself. Protectingthis data is the end goal of almost all IT securitymeasures. Protection strategies at this layer shouldfocus on stored data as well as data in transit. Concepts like Data encryption, DLP and Backup should be understood and implemented.

VII. INTERNET CRIME RATE

Fig 3: Internet Crime Rate

In this year's GISS, Employees were seen as the most likely source of an attack. However, for the first time, we found that when the different types of external attacker were combined (criminal syndicates, state sponsored attackers, activists and lone wolf hackers) these threats were considered to be significantly more likely as arisk source. And nearly all our respondents have one or more external attackers included in their rating.

More than 1,800 respondents across all major industries and in 60 countries participated. For our survey, we invited CIOs, CISOs, CFOs,CEOs and other information security executives to takepart.

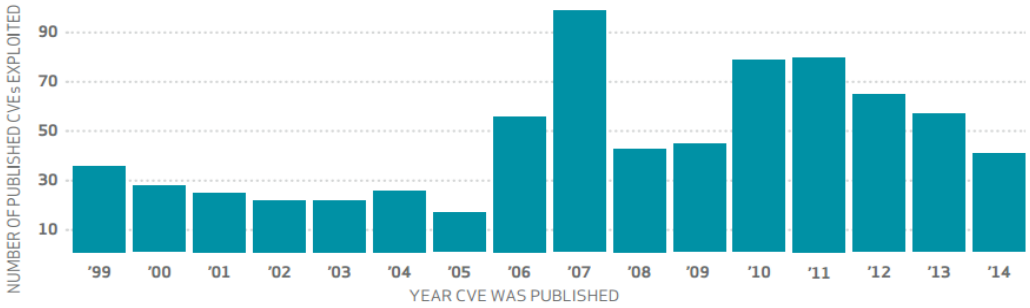

Fig 4: Security overview

99.9% of the exploited vulnerabilities had been compromised more than a year after the associated CVE was published. Known vulnerabilities are still being exploited.Looking at just the total number of malware events (around 170 million) across all organizations, five malware events occur every second.

VIII. CONCLUSION

Statistics show that the most devastating attacks are partly or completely committed by the company's own dissatisfied or angry employees, as they try to push an advantage that they believe to be rightful or just. Their intention is not necessarily to cause effective damage to company value. Curiosity often serves a great motivation as well - accessing sensitive information that should normally remain undisclosed holds out the promise of knowledge and power. We recommend an internal vulnerability assessment to all our clients who have sensitive information stored on their intranet or internal network, and prefer not to have them accessed by employees without proper roles or authorization. Assessment of Wi-Fi networks is closely related to the internal vulnerability assessment described earlier, as Wi-Fi networks are directly connected to the local area network (LAN). However, they have a much greater signal coverage than the physical area of the office itself. If a hacker ever successfully gained access to the Wi-Fi network, he would have the same set of rights as a registered internal company user does. He would then have the chance to implement transparent data mining, elevate his level of privilege, or carry on with taking over any of the devices found on the corporate network without anyone ever noticing. An internal vulnerability assessment takes place locally at the customer's office with a direct physical link to the LAN. Software functions and services are then picked up and examined to see if they can be exposed, and if so, which roles are affected (e.g. a guest account or an average employee).

IX. ACKNOWLEDGEMENTS

We are earnestly grateful to one our group member, Ashiqurrahman, Lecturer, Royal University of Dhaka. For providing us with his special advice and guidance for this project. Finally, we express our heartiest gratefulness to the Almighty and our parents who have courageous throughout our work of the project.

REFERENCES

[1] Berghel, H. &Uecker, J. (2004). Wireless infidelity II: Airjacking. ***Communications of the ACM,*** 47(12), 15-20.
[2] Berghel, H. &Uecker, J. (2005). WiFi attack vectors. ***Communications of the ACM.*** 48(8), 21-28.
[3] Canadian Institute of Chartered Accountants, the. (2003). Using an ethical hacking technique to assess information security Risk, 1-15.
[4] Chang, E.S. & Jain, A.K. & Slade, D.M. &Tsao, S.L. (1999). Managing Cyber Security Vulnerabilities in Large Networks. ***Bell Labs Technical Journal,*** 252-272.
[4] Clutterbuck, P. & Rowlands, T. &Seamons, O. (2007). Auditing the Data Confidentiality of Wireless Local Area Networks. ***The electronic Journal Information Systems Evaluation,*** 10(1), 45-56.
[5] Durst, R. & Champion, T. & Witten, B. & Miller, E. &Spagnuolo, L. (1999). Testing andEvaluating Computer Intrusion Detection Systems. ***Communications of the ACM,*** 42(7).
[6] Frost & Sullivan (2008). World Vulnerability Assessment Products Markets. Research and Markets.
Note that thesis title is set in italics and the university that granted the degree is listed along with location information