Azure Skynet Solutions Pvt. Ltd.
M-4, 1st Floor, Old DLF Colony Sector 14
Gurgaon – 122001,
Haryana, India

Tital: "Project Report on Ethical Hacking".

Divyanshu kumar

divyanshukumar29042004@gmail.com

Acknowledgment:

- A section to thank those who have helped you in completing the project.

Content/Index:

A table of contents listing the sections and corresponding page numbers.

Project Content Details:

1. Project Name:

❖. "Project Report on ETHICAL HACKING".

2. Aim/Objective:

Aim:

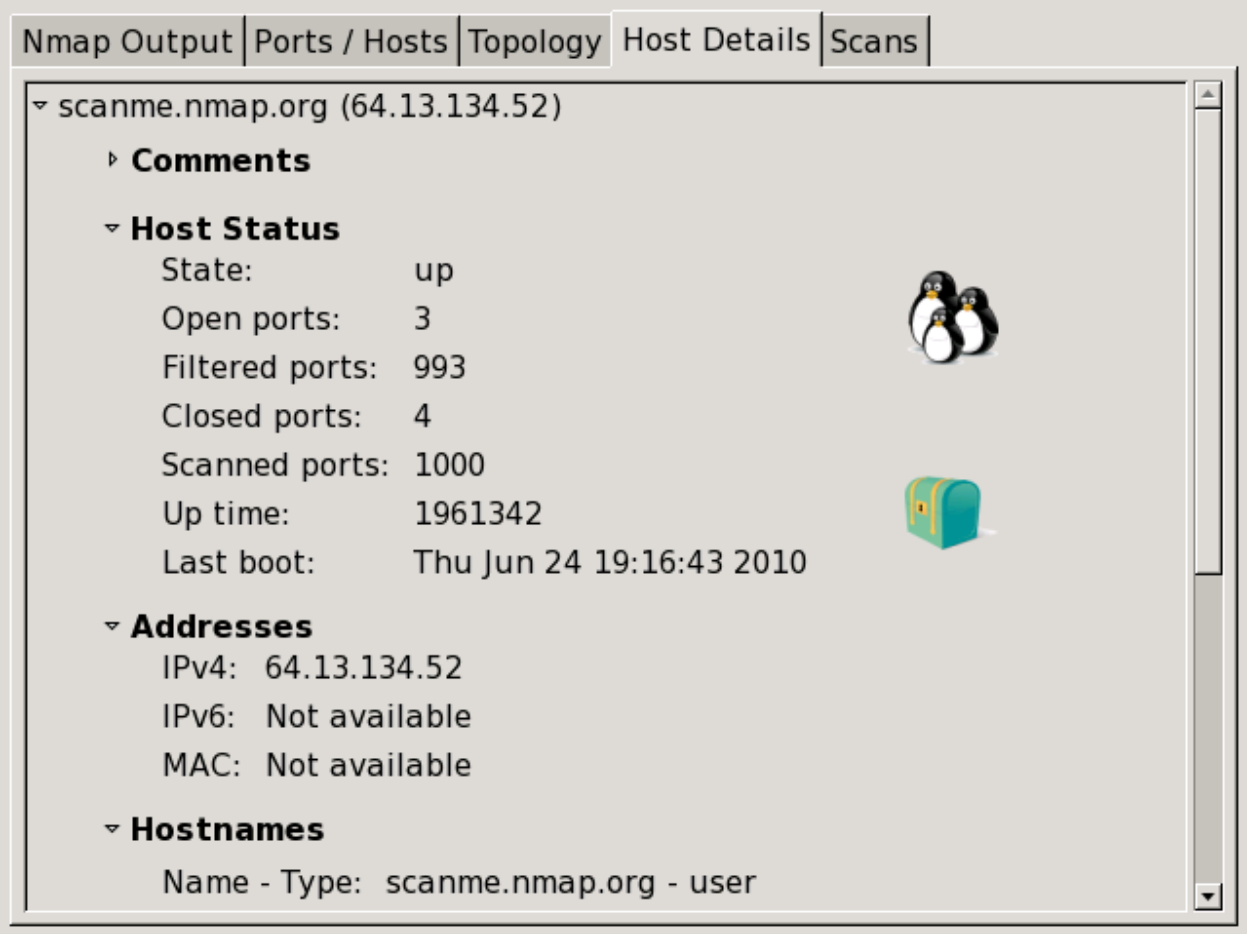
The aim of ethical hacking is to identify and rectify potential security vulnerabilities in computer systems, networks, or web applications by simulating potential attacks. This proactive approach helps organizations to strengthen their security posture and protect sensitive information from malicious hackers.

Objectives:

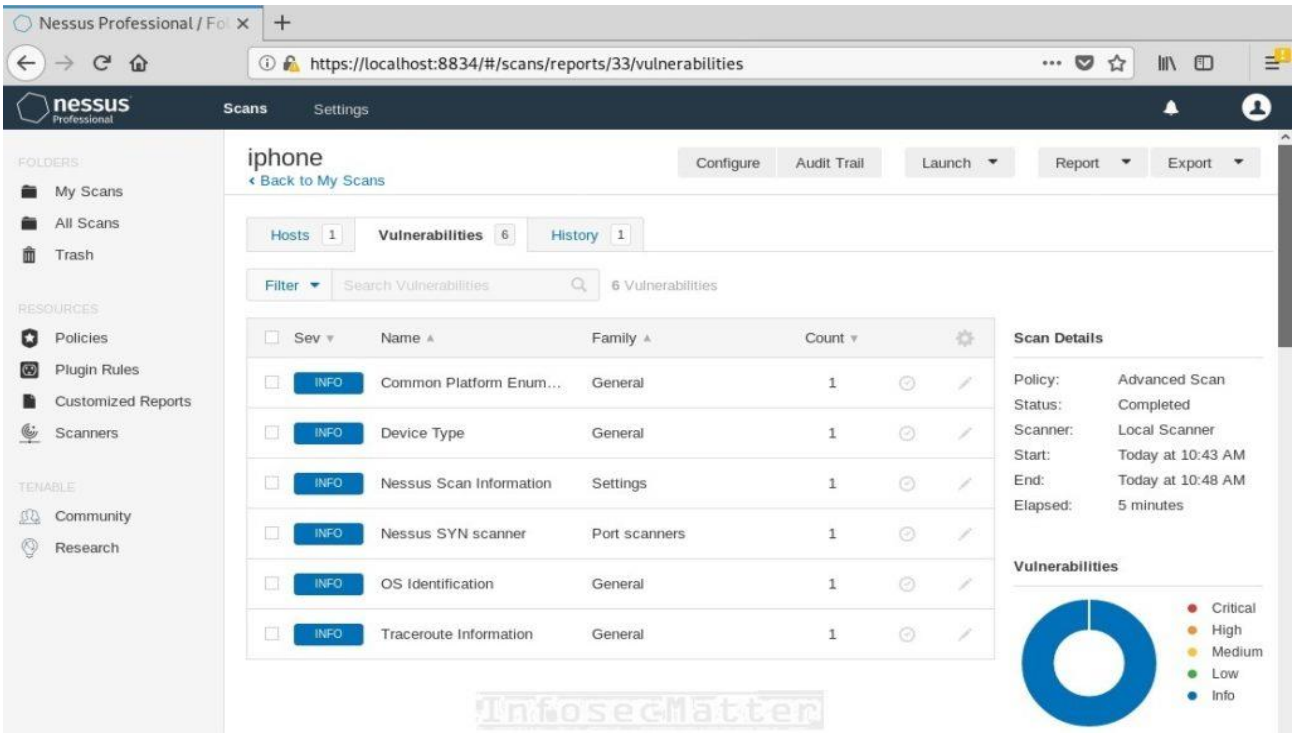
1. **Identify Security Weaknesses**:
   - Discover vulnerabilities in the system that could be exploited by attackers.
2. **Evaluate Security Measures:**
   - Assess the effectiveness of current security policies and controls.
3. **Prevent Data Breaches:**
   - Implement solutions to protect against unauthorized access and data breaches.
4. **Enhance Security Awareness:**
   - Educate stakeholders about potential threats and the importance of cybersecurity practices.
5. **Ensure Compliance:**
   - Ensure that the organization meets industry standards and regulatory requirements related to cybersecurity.

3. Steps Performed:

1. Reconnaissance: This is the first phase where the Hacker tries to collect information about the target. It may include Identifying the Target, finding out the target's IP Address Range, Network, DNS records, etc. Let's assume that an attacker is about to hack a websites' contacts.



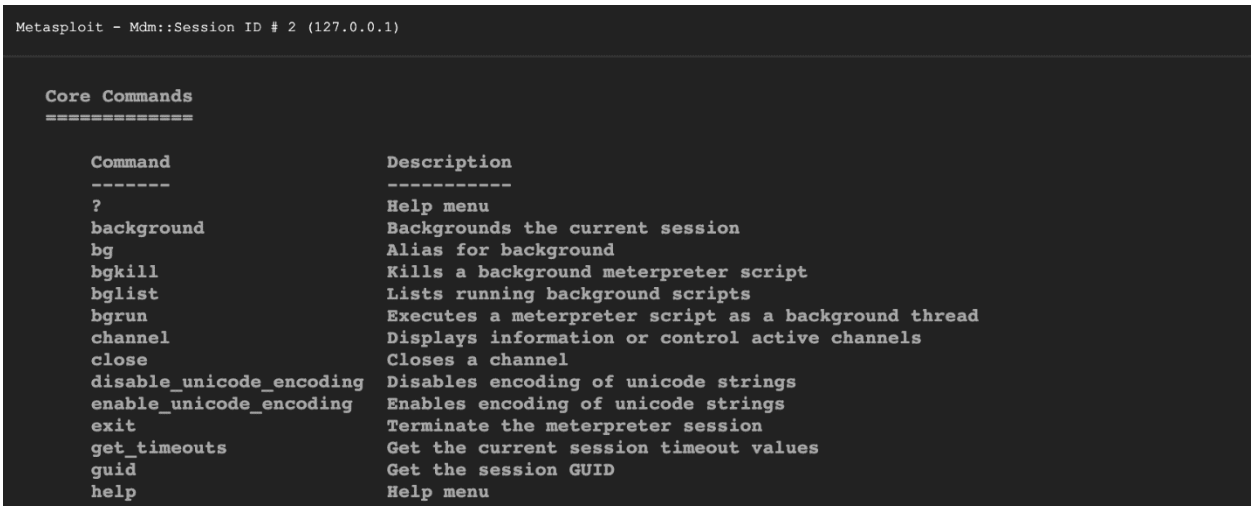
2. Scanning: This phase includes the usage of tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners to scan data. Hackers are now probably seeking any information that can help them perpetrate attacks such as computer names, IP addresses, and user accounts. The hacker decides to use a couple of methods for this end to help map the network (i.e. Kali Linux, Maltego and find an email to contact to see what email server is being used).



3. Gaining Access: In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and scanning the network and now decides that they have some options to gain access to the network.

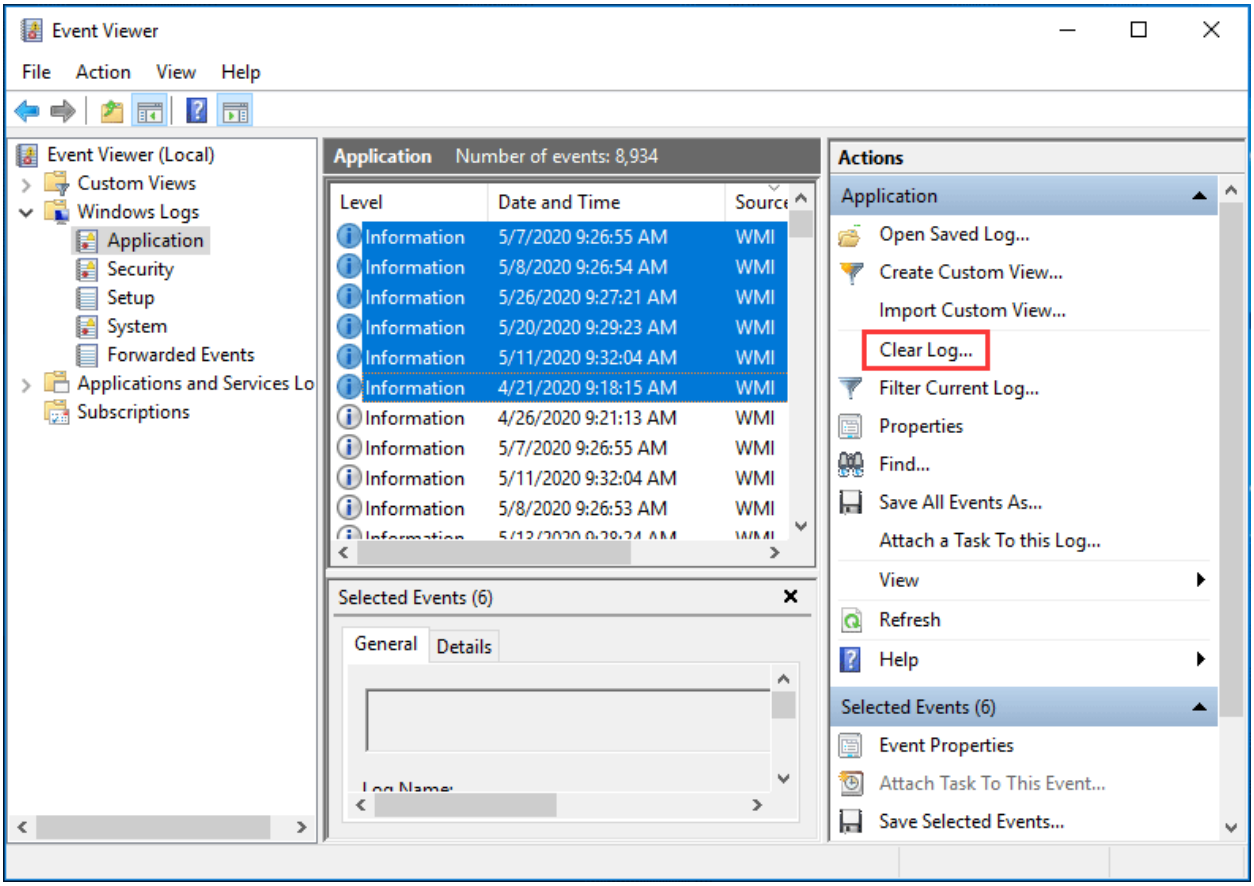
4. Maintaining Access: Once a hacker has gained access, they want to keep that access for future exploitation and attacks. Once the hacker owns the system, they can use it as a base to launch additional

attacks. The hacker may also send out emails to other users with an exploited file such as a PDF with a reverse shell in order to extend their possible access. No overt exploitation or attacks will occur at this time. If there is no evidence of detection, a waiting game is played letting the victim think that nothing was disturbed.



5. Clearing Tracks: Prior to the attack, the attacker would change their MAC address and run the attacking machine through at least one VPN to help cover their identity. They will not deliver a direct attack or any scanning technique that would be deemed “noisy”.
This includes clearing out Sent emails, clearing server logs, temp files, etc. The hacker will also look for indications of the email provider alerting the user or possible unauthorized logins under their account.

Most of the time is spent on the Reconnaissance process. Time spend gets reduced in upcoming phases. The inverted triangle in the diagram represents a time to spend in subsequent phases that get reduced



.

4. Project Output:

❖ Summary of Findings and Security Posture of the Target System.

Summary of Findings:

1. **Vulnerabilities Identified:**
    - Critical Vulnerabilities
    - High-Risk Vulnerabilities
    - Medium-Risk Vulnerabilities
    - Low-Risk Vulnerabilities

2.Exploits Performed:

- Successfully exploited the SQL injection vulnerability to retrieve sensitive data from the database.
- Gained remote access to the web server through an unpatched software vulnerability.
- Used weak passwords to gain unauthorized access to network devices.

3.Access and Persistence:

- Established a persistent backdoor on the compromised web server for ongoing access.
- Created unauthorized user accounts on network devices for future access.

4.Logs and Tracks:

- Cleared system logs to remove evidence of the attack.
- Used stealth techniques to maintain a low profile and avoid detection.

Security Posture:

1.Overall Security Rating:

- Current Security Posture: Poor
- Security Rating: C (on a scale of A to F)

2.Strengths:

- Basic firewall configuration in place.

- Some level of network segmentation to isolate critical systems.
- Use of HTTPS for secure communication.

3.Weaknesses:

- Numerous critical and high-risk vulnerabilities present.
- Inadequate patch management and software updates.
- Weak password policies and lack of multi-factor authentication.
- Insufficient monitoring and logging capabilities.
- Lack of comprehensive security policies and employee training.

4.Recommended Mitigations:

- Patch Management:
- Enhance Authentication
- Improve Configuration
- Security Monitoring
- Employee Training
- Vulnerability Management

5.Conclusion:

The target system has significant security weaknesses that could be exploited by malicious actors. Immediate action is required to address the identified vulnerabilities and improve the overall security posture. By implementing the recommended mitigations, the organization can significantly enhance its defenses and reduce the risk of cyber attacks.

6.References Taken:

❖ List of sources and tools used during the assessment.

1. Sources:

- Books:
- Articles and Papers:
- Online Resources:
- Training and Tutorials:

2. Tools Used:

- Reconnaissance:
- Scanning:
- Exploitation:
- Maintaining Access:
- Covering Tracks:

7.Bibliography:

Books

1. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2nd ed.). Wiley.
2. Erickson, J. (2008). Hacking: The Art of Exploitation (2nd ed.). No Starch Press.
3. Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

4. McClure, S., Scambray, J., & Kurtz, G. (2009). Hacking Exposed.
5. Skoudis, E., & Liston, T. (2006). Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall.

Articles and Papers

1. OWASP Foundation. (2021). OWASP Top Ten Web Application Security Risks.
2. Mandiant. (2013). Understanding the Advanced Persistent Threat.
3. Symantec. (2017). An In-depth Analysis of the WannaCry Ransomware Attack.

Online Resources

1. OWASP (Open Web Application Security Project). OWASP Website.
2. Exploit Database. Exploit-DB Website.
3. SANS Institute. Whitepapers and Research.

Training and Tutorials

1. Offensive Security. Penetration Testing with Kali Linux (PWK).
2. Coursera. Cybersecurity Specialization.
3. Cybrary. Ethical Hacking Courses.