SIDDHI S. KOTRE
ROLL NO: 50

Ethical Hacking Lab

Assignment 8

Penetration Testing using Metasploit and Metasploitable.

Practical 1. Aim: Penetration Testing - Explanation of penetration testing using Metasploit and Metasploitable.

Theory:

Penetration Testing (often referred to as "pen testing") is a simulated cyber attack against a computer system, network, or web application to identify vulnerabilities that an attacker could exploit. The goal is to evaluate the security of the system and discover any weaknesses that could be exploited by malicious actors. This process typically involves several phases, including planning, scanning, gaining access, maintaining access, and reporting.

Metasploit is one of the most widely used penetration testing tools. It provides a suite of tools for developing and executing exploit code against a remote target machine. Key features of Metasploit include:

- **Exploits**: Pre-written code that takes advantage of known vulnerabilities in systems or applications.
- **Payloads**: Code that runs on the target machine after exploiting a vulnerability (e.g., creating a shell).
- **Encoders**: Tools to obfuscate payloads to evade detection by security tools.
- **Post-exploitation modules**: Tools for tasks that can be performed after gaining access, such as privilege escalation or data extraction.

Metasploitable is a deliberately vulnerable virtual machine created for testing and educational purposes. It contains a variety of exploitable applications and services, making it an ideal target for penetration testing exercises.

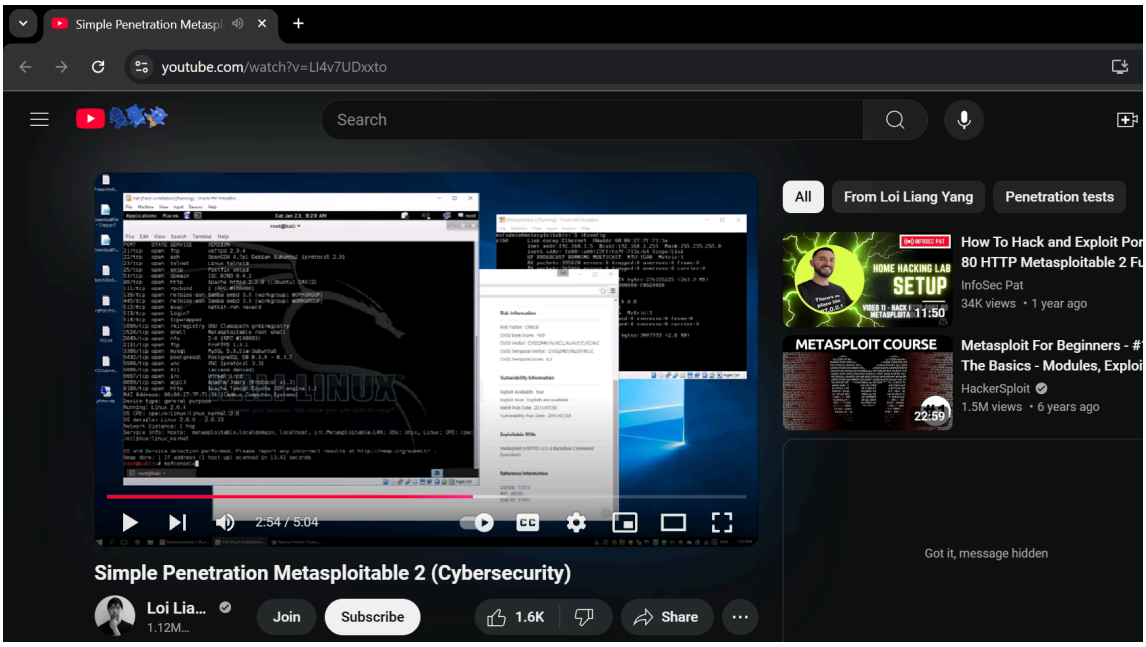
Materials Required:

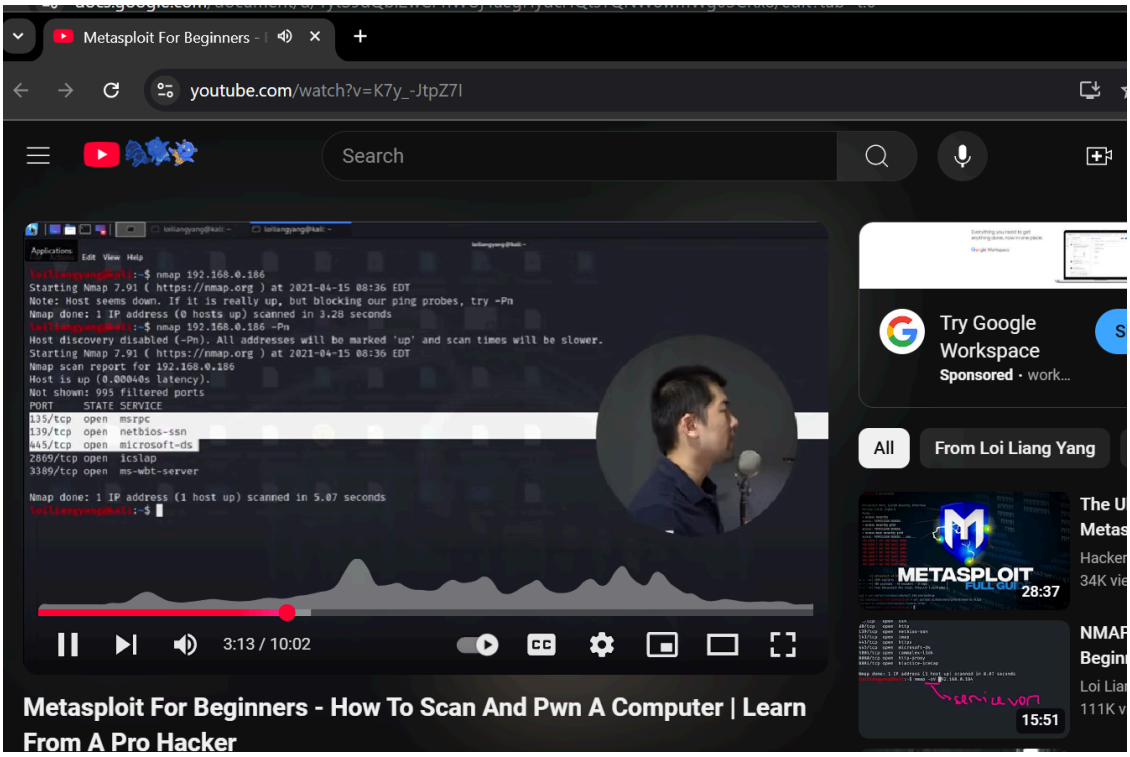
- A virtual machine running Metasploitable 2 (for a vulnerable testing environment)
- Metasploit Framework installed on a separate system or VM (e.g., Kali Linux)

Procedure:

1. Setting Up the Environment
   - Download and install the Metasploitable VM.
   - Ensure that Metasploit is installed and operational on a separate system or virtual machine.
   - Configure both VMs to be on the same network to allow Metasploit to scan and interact with Metasploitable.
2. Conducting the Penetration Test
   - Open the Metasploit console on the Metasploit system.
   - Perform a network scan to detect the Metasploitable machine using commands like nmap.
   - Identify open ports and services on the target machine.
   - Search for available Metasploit modules related to the identified vulnerabilities on Metasploitable.
   - Select an appropriate exploit module in Metasploit and configure it with the target details.
   - Execute the exploit and attempt to gain unauthorized access to the Metasploitable machine.
3. Documentation
   - Note each step and command used.
   - Document any successful exploitation and the level of access gained.

Output:


Simple Penetration Metasp
youtube.com/watch?v=Ll4v7UDxxto
Search
All
From Loi Liang Yang
Penetration tests
How To Hack and Exploit Por
80 HTTP Metasploitable 2 Fu
InfoSec Pat
34K views • 1 year ago
HOME HACKING LAB
SETUP
11:50
METASPLOIT COURSE
22:59
Metasploit For Beginners - #
The Basics - Modules, Exploi
HackerSploit
1.5M views • 6 years ago
2:54 / 5:04
Got it, message hidden
Simple Penetration Metasploitable 2 (Cybersecurity)
Loi Lia...
1.12M...
Join
Subscribe
1.6K
Share


Metasploit For Beginners -
youtube.com/watch?v=K7y_-JtpZ7I
Search
lolliangyang@kali:~$ nmap 192.168.0.186
Starting Nmap 7.91 (https://nmap.org) at 2021-04-15 08:36 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds
lolliangyang@kali:~$ nmap 192.168.0.186 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 (https://nmap.org) at 2021-04-15 08:36 EDT
Nmap scan report for 192.168.0.186
Host is up (0.00040s latency).
Not shown: 995 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
2869/tcp open icslap
3389/tcp open ms-wbt-server
Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
lolliangyang@kali:~$
3:13 / 10:02
Metasploit For Beginners - How To Scan And Pwn A Computer | Learn From A Pro Hacker
Try Google Workspace
Sponsored • work...
All
From Loi Liang Yang
METASPLOIT
28:37
15:51

Practical 2. Cyber Law Under the IT Act 2000: Sections 43, 65, 66A, 66B, 66C, 66D, 66E, 66F, 67A, 67B, 71, 73, and 74

For each of the following sections under the IT Act 2000, provide:

- Description of each section
- Penalty or punishment
- Real-life cases associated with each section
- Preventive measures for each type of cybercrime, if applicable
- Section 65: Tampering with Computer Source Documents
    - Penalty: Imprisonment for up to 3 years, or a fine of up to 5 lakh rupees (Rs. 500,000), or both.
    - Real-life Example: In October 1995, the Economic Offences Wing of the Mumbai Crime Branch seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These were allegedly prepared using Desktop Publishing Systems. Abdul Kareem Telgi, along with several others, was convicted in India for counterfeiting stamp papers and postage stamps totaling billions of rupees.

Aim: To understand the key sections under the IT Act 2000 related to cybercrime, including descriptions, penalties, real-life cases, and preventive measures

Theory:

The Information Technology (IT) Act, 2000, was enacted in India to provide a legal framework for electronic governance and address cybercrime. This Act includes various sections covering offenses such as unauthorized access, data theft, and digital fraud, among others. Understanding these sections is crucial to preventing and responding to cybercrimes.

Sections Under the IT Act 2000:

Section 43: Penalty for Damage to Computer, Computer System, etc.

Description: This section addresses unauthorized access to a computer system or network, causing damage or destruction to data or programs. It also covers the introduction of viruses and the disruption of services.

Penalty/Punishment:

- Penalty of up to ₹1 crore for damages to the affected party.

Real-life Cases:

- The case of **Chetan B. Ranjit vs. State of Karnataka** involved unauthorized access to a computer network.

Preventive Measures:

- Use of firewalls and antivirus software to protect systems from unauthorized access.
- Regular system audits and updates to software and security protocols.

Section 65: Hacking with Computer System

Description: This section penalizes the act of tampering with computer source code or data without the consent of the owner.

Penalty/Punishment:

- Imprisonment of up to three years or a fine of up to ₹2 lakh, or both.

Real-life Cases:

- The **2014 hacking incident involving the Delhi University**, where student data was tampered with.

Preventive Measures:

- Implementing strict access controls and encryption of sensitive data.
- Regularly training employees on cybersecurity awareness.

Section 66A: Sending Offensive Messages through Communication Service

Description: This section penalizes sending offensive messages through communication services or platforms.

Penalty/Punishment:

- Imprisonment of up to three years and/or a fine.

Real-life Cases:

- The **2012 arrest of two girls in Mumbai** for posting a comment on Facebook regarding the shutdown of Mumbai.

Preventive Measures:

- Educating users about responsible online behavior and the consequences of offensive communication.
- Implementing moderation mechanisms on online platforms.

Section 66B: Punishment for Receiving Stolen Computer Resources

Description: This section penalizes anyone who receives or retains stolen computer resources.

Penalty/Punishment:

- Imprisonment of up to three years or a fine of up to ₹1 lakh, or both.

Real-life Cases:

- Various cases involving the possession of stolen credit card data or hacking tools.

Preventive Measures:

- Ensuring proper tracking of computer resources and auditing for theft.
- Educating users on the importance of obtaining software and hardware from reputable sources.

Section 66C: Identity Theft

Description: This section deals with identity theft, including the use of someone else's password or personal details without their consent.

Penalty/Punishment:

- Imprisonment of up to three years or a fine of up to ₹1 lakh, or both.

Real-life Cases:

- Numerous instances of identity theft related to financial fraud.

Preventive Measures:

- Using strong, unique passwords and enabling two-factor authentication.
- Regularly monitoring financial statements and credit reports.

Section 66D: Cheating by Personation using Computer Resource

Description: This section penalizes cheating by impersonation through computer resources.

Penalty/Punishment:

- Imprisonment of up to three years or a fine of up to ₹1 lakh, or both.

Real-life Cases:

- Cases of online fraud where individuals impersonate others to obtain money or information.

Preventive Measures:

- Educating users on recognizing phishing attempts and verifying the identity of individuals in digital transactions.

Section 66E: Violation of Privacy

Description: This section penalizes the violation of the privacy of an individual through the capture or disclosure of images or information without consent.

Penalty/Punishment:

- Imprisonment of up to three years or a fine of up to ₹2 lakh, or both.

Real-life Cases:

- The case of **Rekha Sharma vs. State of Haryana**, where private images were shared without consent.

Preventive Measures:

- Encouraging individuals to use privacy settings on social media and be cautious about sharing personal information.

Section 66F: Cyber Terrorism

Description: This section addresses acts of cyber terrorism that threaten the unity, integrity, security, or sovereignty of India.

Penalty/Punishment:

- Imprisonment for life.

Real-life Cases:

- Cases involving hacking of critical infrastructure systems or threats to national security.

Preventive Measures:

- Implementing robust cybersecurity measures for critical infrastructure.
- Conducting regular threat assessments and training for personnel.

Section 67A: Publishing or Transmitting Obscene Material in Electronic Form

Description: This section penalizes the publishing or transmitting of material that is sexually explicit or obscene in electronic form.

Penalty/Punishment:

- Imprisonment of up to five years and a fine of up to ₹10 lakh for first-time offenders; increased penalties for repeat offenders.

Real-life Cases:

- Cases involving the distribution of obscene content through social media platforms.

Preventive Measures:

- Establishing content moderation policies on digital platforms.
- Educating users about responsible content sharing.

Section 67B: Publishing or Transmitting Material Depicting Children in Obscene or Sexual Acts

Description: This section penalizes the publication or transmission of material depicting children in obscene or sexual acts.

Penalty/Punishment:

- Imprisonment of five to seven years and a fine.

Real-life Cases:

- Various child exploitation cases involving the distribution of child pornography.

Preventive Measures:

- Collaborating with law enforcement to report and track child exploitation materials.
- Implementing strict policies for content management on platforms used by minors.

Section 71: Misrepresentation

Description: This section penalizes any person who misrepresents themselves or their services related to a computer resource.

Penalty/Punishment:

- Imprisonment of up to two years or a fine of up to ₹1 lakh, or both.

Real-life Cases:

- Instances of companies misrepresenting their data protection services.

Preventive Measures:

- Ensuring transparency in service offerings and certifications.
- Regular audits and compliance checks for service providers.

Section 73: Publishing Information which is False or Misleading in Electronic Form

Description: This section deals with publishing misleading information in electronic form.

Penalty/Punishment:

- Imprisonment of up to two years or a fine.

Real-life Cases:

- Instances of false news and misinformation spread via social media.

Preventive Measures:

- Promoting media literacy and fact-checking.
- Implementing reporting mechanisms on social media platforms.

Section 74: Publication for Fraudulent Purposes

Description: This section penalizes the publication of information for fraudulent purposes.

Penalty/Punishment:

- Imprisonment of up to three years and/or a fine.

Real-life Cases:

- Cases involving fraudulent online businesses or scams.

Preventive Measures:

- Educating users about recognizing fraudulent schemes.
- Reporting and taking action against fraudulent websites or individuals.

Output: