

Forum:[Hack Forums](#)

Thread: [Introduction to Ethical Hacking](#)

obtainhigh - July 4, 2024, 2:40 am

Introduction to Ethical Hacking

Ethical hacking involves testing computer systems, networks, or web applications to find security vulnerabilities that could be exploited by malicious hackers. This tutorial will cover the basics and guide you through the initial steps of becoming an ethical hacker.

1. Understanding the Basics

What is Hacking? Hacking: Unauthorized access to data in a system or computer.

Ethical Hacking: Authorized practice of bypassing system security to identify potential data breaches and threats in a network.

Types of Hackers White Hat: Ethical hackers who work to protect systems.

Black Hat: Malicious hackers who exploit vulnerabilities.

Gray Hat: A mix of both; may break the law but not for malicious intent.

2. Setting Up Your Environment

Tools and Operating Systems Kali Linux: A popular Linux distribution for penetration testing.

Virtual Machines (VMs): Use software like VirtualBox or VMware to run different operating systems.

Network Scanners: Tools like Nmap for network discovery and security auditing.

Installing Kali Linux

Download Kali Linux: [Kali Linux Download](#)

Install VirtualBox/VMware:

[VirtualBox Download](#)

[VMware Download](#)

Create a New VM:

Open VirtualBox/VMware and create a new virtual machine.

Allocate resources (RAM, CPU).

Attach the Kali Linux ISO and install the OS.

3. Learning Basic Commands

Linux Commands Navigating Directories:

`ls` – List directory contents.

`cd` – Change directory.

`pwd` – Print working directory.

File Operations:

`cp` – Copy files.

`mv` – Move or rename files.

`rm` – Remove files.

Networking Commands `ifconfig` – Display network configuration.

`ping` – Test network connectivity.

`netstat` – Network statistics.

4. Basic Network Scanning

Using Nmap Introduction to Nmap: Network Mapper used for network discovery and security auditing.

Basic Scanning:

`nmap <target IP>` – Basic scan.

`nmap -sS <target IP>` – Stealth scan.

`nmap -A <target IP>` – Comprehensive scan with OS detection.

5. Vulnerability Scanning

Using OpenVAS

Install OpenVAS:

```
`sudo apt-get install openvas`
```

```
`sudo openvas-setup`
```

Access OpenVAS:

Open a web browser and navigate to ``https://<your-kali-ip>:9392``.

Login with the credentials set during setup.

Running a Scan:

Create a new target.

Configure and start the scan.

Analyze the results to identify vulnerabilities.

6. Exploitation Basics

Using Metasploit

Install Metasploit:

```
`sudo apt-get install metasploit-framework`
```

Start Metasploit:

```
`msfconsole`
```

Basic Exploitation:

```
`search exploit <service>` – Find exploits for a service.
```

```
`use <exploit path>` – Use a specific exploit.
```

```
`set RHOST <target IP>` – Set the target IP.
```

```
`set PAYLOAD <payload>` – Set the payload.
```

```
`exploit` – Run the exploit.
```

7. Password Cracking

Using Hydra

Install Hydra:

```
`sudo apt-get install hydra`
```

Basic Usage:

```
`hydra -l <username> -P <password list> <target IP> <service>`
```

Using John the Ripper

Install John the Ripper:

```
`sudo apt-get install john`
```

Basic Usage:

```
`john <password file>`
```

8. Web Application Testing

Using Burp Suite

Install Burp Suite:

```
`sudo apt-get install burpsuite`
```

Configuring Burp Suite:

Configure your browser to use Burp Suite as a proxy.

Basic Web Testing:

Intercept and modify HTTP requests.

Scan for vulnerabilities.

9. Reporting

Documenting Findings Create a Report: Use tools like Dradis to organize your findings.

Include Details:

- Description of each vulnerability.

- Steps to reproduce.

- Potential impact.

- Remediation recommendations.

10. Continuous Learning

Online Courses: Platforms like Coursera, Udemy (warez disallowed), and Cybrary offer courses on ethical hacking.

Books: "The Web Application Hacker's Handbook," "Hacking: The Art of Exploitation."

Certifications: CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional).

BlackSoulZN5006 - July 7, 2024, 9:27 pm

Excellent Thread you posted for sure to starting out