

Ethical Hacker Pro (V1)

Competency Assessment Objectives

Prepare

Perform reconnaissance

- Perform reconnaissance with operating system tools
- Perform reconnaissance with hacking tools

Perform scanning

- Scan for network devices
- Discover wireless devices
- Scan for IoT devices
- Detect operating systems and applications
- Identify open ports
- Scan for vulnerabilities

Perform enumeration

- Enumerate network resources
- Enumerate users and groups
- Enumerate device information
- Enumerate services and applications
- Enumerate DNS

Gain Access

Obtain login credentials

- Crack passwords
- Use Social Engineering

Gain administrative access and escalate privileges

- Gain access through a backdoor
- Escalate privileges
- Hijack a web session

Gain access by cracking

- Obtain credentials through sniffing
- Crack Wi-Fi devices

Attack

Perform passive online attacks

- Examine hidden web form fields
- Conduct a man-in-the-middle attack
- Implement a replay attack

Perform active online attacks

- Perform an SQL injection
- Execute a DoS or DDoS attack

Perform infrastructure attacks

- Attack a web server
- Access wireless networks
- Attack mobile devices
- Access IoT
- Evade firewalls, IDSs, and honeypots

Cover up

Cover up access

- Disable auditing

- Clear logs
- Remove or hide files and folders
- Change MAC address

Defend a System

Defend systems and devices

- Hide a web server banner broadcast
- Configure rogue host protection
- Secure mobile devices
- Configure account policies and account control

Implement defensive systems

- Implement an Intrusion Detection System (IDS)
- Create a honeypot
- Prevent DNS zone transfer

Scan for vulnerabilities

- Scan for vulnerabilities on Windows or Linux systems
- Scan for vulnerabilities on servers, wireless devices, and appliances