ADVANCED PENETRATION TESTING

CODEC NETWORKS

Decoding Threats, Coding Solutions

Proposed by Codec Networks Pvt Ltd
www.codecnetworks.com | mktg@codecnetworks.com

TABLE OF CONTENTS

INTRODUCTION

Overview

There are good penetration testers and then there are great penetration testers.

Unless you are bent on being nothing other than the best in penetration testing, don't bother registering for this program, as you are probably not cut out for it.

You will be required to make knowledgeable decisions under immense pressure at critical stages while selecting your approach and exploits.

As you progress along these levels, you will need to maneuver web application, network, and host penetration testing tools and tricks in an internal and external context to ultimately pawn the hosts and exfiltrate data required for the completion of the challenges.

This course is designed for security professionals who want to take a serious and meaningful step into the world of professional penetration testing. This includes – pentesters seeking an industry-leading certification, security professionals, network administrators and other technology professionals.

Objective

- Using Information gathering techniques to identify and enumerate targets running various operating systems and services
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling and porting public exploit code
- Conducting both remote and client-side attacks
- Identifying and exploiting XSS, SQL infection and file inclusion vulnerabilities in web applications
- Deploying tunneling techniques to bypass firewalls
- Creative problem solving and lateral thinking skills

Pre-requisites

- Solid understanding of TCP/IP networking
- Reasonable understanding of Linux
- Familiarity of Bash scripting with basic Python or Perl a plus

Course Duration

40 Hours (8 hours/day)

TOPICS

Essential Tool for Penetration Testing

- Wireshark to analyze the network traffic
- Tcpdump to filtering traffic
- Netcat in Enumeration
- Netcat to Transfer File
- Netcat to take a reverse shell

Passive Information Gathering

- Netcraft for information gathering
- Recon-ng for information gathering
- Maltego for information gathering

Active Information Gathering

- DNS lookup
- Perform zone transfer using dig
- Nmap port scanning technique
- Use tool like nslookup, snmpenum, snmpwalk

Buffer Overflow

- Fuzzing.
- How to Control the EIP?
- Checking and removing of bad characters.
- Improve the old exploits.
- DEP and ASLR protection and how to bypass them.

Working with Exploit

- Search for exploit according to the version info.
- Finding exploits at different sources.
- Customize the prebuild exploit.

Privilege Escalation

- Abusing sudo rights based privilege escalation
- SUID bit based privilege escalation
- Kernel exploit based privilege escalation
- Path variable based privilege escal**ation**
- Mysql based privilege escalation
- Crontab based privilege escalation
- Wildcard injection based privilege escalation
- Buffer overflow based privilege escalation

Web application attacks

- OWASP top 10

Port Redirection and Tunneling

- Port Forwarding/Redirection
- SSH tunneling
- HTTP tunneling Redirection and Tunneling
- Port Forwarding

Bypass Antivirus Software

- Encoding payload with metasploit
- Custom Encoders

ADVANCE LABS

Easy CTF's

Nibbles

Description: Nibbles is a recently retired CTF challenge VM on Hack the Box with Easy difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.75.

It is based on Sudo privilege escalation.

Poison

Description: Poison is a recently retired CTF challenge VM on Hack the Box with Easy difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.84

It is based on SSH privilege escalation.

Sunday

Description: Sunday is a recently retired CTF challenge VM on Hack the Box with easy difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.76

It is based on SUID based privilege escalation.

Jerry

Description: Jerry is a recently retired CTF challenge VM on Hack the Box with easy difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.95

It is based on Native vulnerability based privilege escalation.

Blue

Description: Blue is a recently retired CTF challenge VM on Hack the Box with easy difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.40

Medium CTF's

Bashed

Description: Bashed is a recently retired CTF challenge VM on Hack the Box with Medium difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.68

It is based on cron file privilege escalation.

Sense

Description: Sense is a recently retired CTF challenge VM on Hack the Box with Medium difficulty level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.60

Node

Description: FriendZone is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of FriendZone is 10.10.10.58.

It is based on user privilege escalation.

Valentine

Description: Valtentine is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Valtentine is 10.10.10.79

It is based on suid based privilege escalation.

Cronos

Description: Cronos is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Cronos is 10.10.10.13

It is misconfiguration based privilege escalation.

Nineveh

Description: Nineveh is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Nineveh is 10.10.10.43

It is database based privilege escalation

Solidstate

Description: Solidstate is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Solidstate is 10.10.10.51

It is native vulnerability privilege escalation

Optimum

Description: Optimum is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Optimum is 10.10.10.8

It is database based privilege escalation

Davel

Description: Davel is a recently retired CTF VM on Hack the Box with the objective – Capture the user and root flag. Since these labs are online available, therefore, they have a static IP. The IP of Davel is 10.10.10.5

It is native vulnerability based privilege escalation

Bounty

Description: Bounty is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.93

It is native vulnerability based privilege escalation

Jeeves

Description: Jeeves is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.63

It is misconfiguration based privilege escalation

Hard CTF's

BrainFuck

Description: Brainfuck is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.17

It is based on wordpress plugin issue privilege escalation.

Kotarak

Description: Vault Kotarak is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.55

It is based on wget native vulnerability based privilege escalation.

TartarSauce

Description: Vault TartarSauce is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.88

It is misconfigure backup file based privilege escalation.

Silo

Description: Silo is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.82

It is native vulnerability based privilege escalation.

Bart

Description: Bart is a recently retired CTF challenge VM on Hack the Box with Intermediate level and the objective remains the same– Capture the root flag. Since these labs are online available, therefore, they have a static IP. The IP of Help is 10.10.10.81

It is native vulnerability based privilege escalation.