Advanced Infrastructure Hacking

Get Certified Today!

Check Point SOFTWARE TECHNOLOGIES LTD

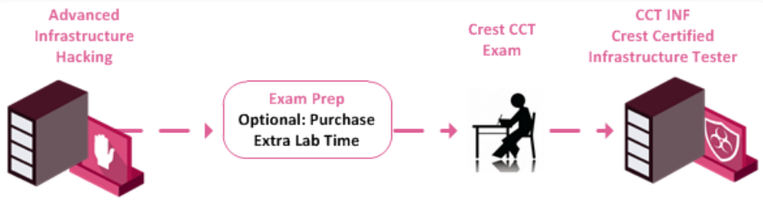
5 DAY CLASS | ADVANCED TRACK | PART OF HACKINGPOINT

Whether you are penetration testing, Red Teaming or trying to get a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques is critical. This course covers a wide variety of neat, new and ridiculous techniques to compromise modern Operating Systems and networking devices. While prior pentest experience is not a strict requirement, familiarity with both Linux and Windows command line syntax will be greatly beneficial.

STUDENT REQUIREMENTS

The only requirement for this class is that you bring your own laptop and have admin/root access. During the class, we will give you VPN access to our state-of-the-art Hacklab which is hosted at our Datacenter in the UK. Once you are connected to the lab, you will find all the relevant tools and VMs there.

We also provide a dedicated Kali VM to each attendee at the Hacklab, so you don't have to bring any VMs. All you need is admin access to install the VPN client and when you are connected, you're good to go!



WHO SHOULD TAKE THIS CLASS?

- System administrators, SOC analysts, penetration testers, network engineers, security enthusiasts, and anyone who wants to take their skills to the next level.

Requirement: Bring a laptop with admin/root access

Understanding Advanced Hacking techniques for infrastructure devices and systems, is critical for penetration testing, red teaming, and managing vulnerabilities in your environment.

Students will become familiar with hacking techniques for common operating systems and networking devices.

Experience with common hacking tools such as Metaspoit is recommended, but not a requirement.

Day 1

- IPv4/IPv6 basics
- Host discovery & enumeration
- Advanced OSINT & asset discovery
- Mastering Metaspoit
- Hacking application and CI servers
- Hacking third-party applications (Wordpress, Joomla)
- Hacking databases
- Windows enumeration and configuration issues

In collaboration with

NOT SO SECURE
A Claranet Group Company

Day 2

- Windows desktop *Breakout* and *AppLocker* bypass techniques (Win 10)
- Local privilege escalation
- A/V & AMSI bypass techniques
- Offensive PowerShell tools and techniques
- Post-exploitation tips, tools, and methodology
- Active Directory delegation reviews and Pwnage (Win 2012 server)
- Pass the Hash/Ticket
- Pivoting, port-forwarding and lateral movement techniques

Day 3

- Linux vulnerabilities and configuration issues
- User/service enumeration
- File share hacks
- SSH hacks
- X11 vulnerabilities
- TTY issues, SSH reverse tunneling
- Restricted shells breakouts
- Breaking hardened webservers
- Local privilege escalation
- Post-exploitation

Day 4

- Breaking and abusing Docker Kubernetes vulnerabilities
- Explointing insecure VPN configuration
- VLAN hopping
- Hacking VoIP
- B33r 101