Advanced Infrastructure Hacking

5 DAY CLASS

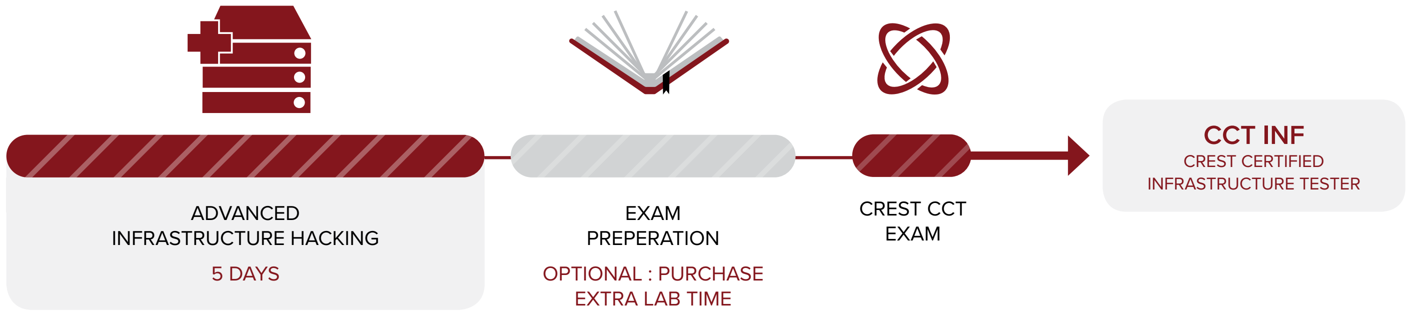
ADVANCED TRACK

Latest exploits, highly relevant

Teaching a wide variety of offensive hacking techniques

Written by real pen testers with a world conference reputation (BlackHat, AppSec, OWASP, Defcon etc)

This Advanced Infrastructure Hacking class is designed for those who wish to push their knowledge. The fast-paced class teaches the audience a wealth of hacking techniques to compromise various operating systems and networking devices. The class will cover advanced penetration techniques to achieve exploitation and will familiarise you with hacking of common operating systems, networking devices and much more. From hacking domain controllers to local root, VLAN hopping to VoIP hacking, we have got everything covered.

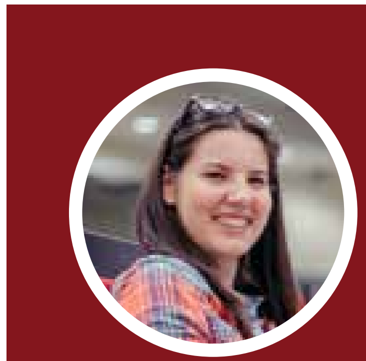


ADVANCED INFRASTRUCTURE HACKING
5 DAYS

EXAM PREPERATION
OPTIONAL : PURCHASE EXTRA LAB TIME

CREST CCT EXAM

CCT INF
CREST CERTIFIED INFRASTRUCTURE TESTER



This course was exactly as described. It delivered good, solid information on the current state of infrastructure hacking at the rapid pace promised. This was a great way to get back into this area after years away from it.

Delegate, Black Hat USA

NOT SO SECURE

WHO SHOULD TAKE THIS CLASS?

The class is ideal for those preparing for CREST CCT (ICE), CHECK (CTL), TIGER SST and other similar industry certifications, as well as those who perform penetration testing on infrastructure as a day job and wish to add to their existing skill set.

Whether you are penetration testing, red teaming, or hoping to gain a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques for infrastructure devices and systems is critical.

This Advanced Infrastructure Hacking class will get the attendees familiarised with a wealth of hacking techniques for common operating systems and networking devices. While prior pen testing experience is not a strict requirement, a prior use of common hacking tools such as Metasploit is recommended for this class.

DAY 1

IPv4 and IPv6 refresher

Advanced topics in network scanning

Understanding and exploiting IPv6 targets

OSINT, DVCS exploitation

Advanced OSINT data gathering

Exploiting git and continuous integration (CI) servers.

Database servers

MySQL

Postgres

Oracle

Recent vulnerabilities

Heart-Bleed and Shell-Shock

PHP serialization exploit

Web-sphere Java exploits

DAY 2

Windows exploitation

Domain and user enumeration

AppLocker / GPO restriction bypass

Local privilege escalation

Post exploitation #1 (AMSI bypass & Mimikatz)

Post exploitation #2 (LSASecrets)

DAY 3

AD exploitation

Active directory delegation issues

WOW64

Pivoting and WinRM

Persistence (Golden Ticket and DCSync)

Lateral movement using WMIC

DAY 4

Linux exploitation

Port scanning and enumeration

FS + SSH

Privilege escalation

Rservices

Apache

X11 services

DAY 5

Container breakout

Docker breakout

VPN exploitation

VPN

VoIP exploitation

VoIP enumeration

VoIP exploitation

VLAN exploitation

VLAN concepts

VLAN hopping attacks.