Advanced Infrastructure Hacking

Learn via: **Classroom/Virtual**

Duration: **5 Days**

Overview

An Advanced Infrastructure Hacking class, new for 2017, 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. 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).

IISP Skills Alignment

This course is aligned to the following Institute of Information Security Professionals (IISP) Skills. More details on the IISP skills framework can be found here.

- D2, E3, C2

Continuous Professional Development (CPD)

CPD points can be claimed for GCT accredited courses at the rate of 1 point per hour of training for GCHQ accredited courses (up to a maximum of 15 points).

Prerequisites

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. The Advanced Infrastructure class will get the attendees familiarised with a wealth of hacking techniques for common Operating Systems and networking devices. We recommend the delegates have completed the Art of Hacking course (QATAOH) before attending this course. 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. Solid Linux skills and Windows OS knowledge is essential.

This course will be suitable for delegates interested in the SANS Institute course SEC560: Network Penetration Testing & Ethical Hacking.

Who Should Attend

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 skillset.

Outline

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.