NOT SO SECURE
A Claranet Group Company

claranet cyber security

Advanced Infrastructure Hacking

Our Advanced Infrastructure Hacking class is designed for those who wish to push their knowledge. 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 class teaches the audience a wealth of advanced penetration testing techniques, from the neat, to the new, to the ridiculous, to compromise modern Operating Systems, networking devices and Cloud environments. From hacking Domain Controllers to local root, to VLAN Hopping, to VoIP Hacking, to compromising Cloud account keys, we have got everything covered.

Class Outline

Module 1: IPv4 / IPv6 Refresher, Host Discovery, OSINT

Module 2: Exploiting DVCS / CI-CD & other web technologies

Module 3: MySQL, Postgres, Oracle & MongoDB

Module 4: Windows enumeration & Exploitation

- Configuration issues
- AppLocker bypass techniques
- AV & AMSI Bypass techniques

Module 5: Hacking AD Environment

- Active Directory Delegation
- Persistence and backdooring Techniques
- Lateral Movement

Module 6: Hacking *nix

- Unix Exploitation
- NFS Attacks
- Shell Escapes
- TTY hacks & SSH Tunneling
- Exploiting *nix misconfigurations
- Web Server Hacks
- X11 Hacks
- Privilege Escalation and credential harvesting

Module 7: Container Technologies (Docker & Kubernetes)

Module 8: VPN Hacking

Module 9: VoIP Hacking

Module 10: VLAN Hacking

Module 11: Cloud Pentesting

Who Should Attend

System Administrators, SOC Analysts, Penetration Testers, Network Engineers, security enthusiasts and anyone who wants to take their skills to next level.

While prior pen testing experience is not a strict requirement, familiarity with both Linux and Windows command line syntax will be greatly beneficial and a reasonable technical understanding of computers and networking in general is assumed. Some hands-on experience with tools commonly used by hackers, such as Nmap, NetCat, or Metasploit, will also be beneficial, although, less advanced users can work their way up during the 30 days of complimentary lab access provided as part of the 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.

On Completion of this class Attendees will be able to:

- Enumerate, investigate, target and exploit weaknesses in an organisation's network devices, online presence, and people.
- Understand complex vulnerabilities and chained exploitation processes in order to gain access and perform restriction bypasses, privilege escalation, data exfiltration and gain long term persistence in: Web facing services, databases, Windows, Active Directory, *nix, container-based, VPN, VLAN, VoIP and Cloud environments.
- Use compromised devices to pivot onto other private networks and/or access services protected by whitelisting or only accessible via the loopback interface

What Students Receive

Access to our hacking lab not just during the class but for 30 days after the class too. This gives students plenty of time to practice the concepts taught in the class. The lab contains a wide variety of challenges from local privilege escalation to VLAN hopping etc. Numerous scripts and tools will also be provided during the training, along with student handouts.

Prerequisites

The only requirement for this class is that you must bring your own laptop and have admin/root access on it. During the class, we will give you VPN access to our state-of-art Hacklab which is hosted in our data-center in the UK. Once you are connected to the lab, you will find all the relevant tools/VMs there. We also provide a dedicated Kali VM to each attendee on the hacklab, accessed using SSH. So, you don't need to bring any VMs with you. All you need is admin access to install the VPN client and once connected, you are good to go!

Attendees may optionally come prepared with an OpenVPN client (e.g. OpenVPN Client for Windows, we suggest Tunnelblick for Mac, the OpenVPN client is often included natively for Linux but may need installing/updating) and an SSH client (e.g. PuTTY for Windows, generally included natively for Linux/Mac) installed.

For more information contact
+44 1223 653193
contact@notsosecure.com