Advanced Infrastructure Hacking 5 Days

FAST TRACK AVAILABLE | 2020 EDITION

Our Advanced Infrastructure Hacking course is designed for those who wish to push their knowledge. Whether you are Pen Testing, Red Teaming or trying to get a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques is critical.

This course teaches the audience a wealth of advanced Pen 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.

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 course.

The course 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.

Delegates Receive

Access to our hacking lab not just during the course but for 30 days after the course too. This gives Delegates plenty of time to practice the concepts taught in the course. 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 course, along with Delegate handouts.

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.

Prerequisites

The only requirement for this course is that you must bring your own laptop and have admin/root access on it. During the course, 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.

Advanced Infrastructure Hacking 5 Days *Continued*

FAST TRACK AVAILABLE | 2020 EDITION

Course Outline

IPV4/IPV6 SCANNING, OSINT
- Advanced topics in network scanning
- Understanding & exploiting IPv6 Targets
- Advanced OSINT Data gathering

WEB TECHNOLOGIES
- Exploiting DVCS (git)
- Owning Continuous Integration (CI) servers
- Deserialization Attacks (Java, Python, Node, PHP)
- Dishonerable Mentions (SSL/TLS, Shellshock)

HACKING DATABASE SERVERS
- Mysql
- Postgres
- Oracle
- MongoDB

WINDOWS EXPLOITATION
- Windows Enumeration and Configuration Issues
- Windows Desktop 'Breakout' and AppLocker Bypass Techniques (Win 10)
- Local Privilege Escalation
- A/V & AMSI Bypass techniques
- Offensive PowerShell Tools and Techniques
- GPO based exploit
- Constrained and Unconstrained delegation attack
- Post Exploitation Tips, Tools and Methodology

AD EXPLOITATION
- Active Directory Delegation Reviews and Pwnage (Win 2012 server)
- Pass the Hash/Ticket Pivoting and WinRM Certificates
- Pivoting, Port Forwarding and Lateral Movement Techniques
- Persistence and backdooring techniques (Golden Ticket, DCSync, LOLBAS)

LINUX EXPLOITATION
- Linux Vulnerabilities and Configuration Issues
- Treasure hunting via enumeration
- File Share/SSH Hacks
- X11 Vulnerabilities
- Restricted Shells Breakouts
- Breaking Hardened Web Servers
- Local Privilege Escalation
- MongoDB exploitation
- TTY hacks, Pivoting
- Gaining root via misconfigurations
- Kernel Exploitation
- Post Exploitation and credentials harvesting

CONTAINER BREAKOUT
- Breaking and Abusing Docker
- Kubernetes Vulnerabilities

VPN EXPLOITATION
- Exploiting Insecure VPN Configuration

VOIP ATTACK
- VOIP Enumeration
- VOIP Exploitation

VLAN ATTACKS
- VLAN Concepts
- VLAN Hopping Attacks

CLOUD HACKING
- AWS/Azure/GCP specific attacks
- Storage Misconfigurations
- Credentials, API's and token Abuse
- IaaS, PaaS, SaaS, CaaS and Serverless exploitation
- Azure AD attacks

NotSoSecure part of claranet cyber security

For more information:
UK: +44 (0)1223 653 193
US: +1 (628)200-3053/3052
Email: contact@notsosecure.com
Visit: notsosecure.com