Advanced Infrastructure Hacking

2 DAY CLASS

2018 FAST PACED VERSION

Note: This is a fast paced version of the original 4 day class, cut down to 2 days. To fit the entire training material within 2 days, some of the exercises have been replaced by demos which will be shown by the instructor. Students will receive FREE 1 month lab access to practice each exercise after the class.

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.

WHO SHOULD TAKE THIS CLASS?

System Administrators, SOC analysts, Penetration testers, network engineers, security enthusiasts and anyone who wants to take their skills to next level.

While prior pentest experience is not a strict requirement, familiarity with both Linux and Windows command line syntax will be greatly beneficial. A further hands-on experience with common hacking tools such as 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.

STUDENT REQUIREMENTS

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. 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!

NOT SO SECURE
A Claranet Group Company

TRAINERS

Anant Shrivastava is an information security professional with 9+ yrs of corporate experience with expertise in Network, Mobile, Application and Linux Security. He is Regional Director Asia Pacific for NotSoSecure Global Services, he has trained ~700 delegates at various conferences (Blackhat all 3 editions, Nullcon, g0s, c0c0n). Anant also leads Open Source project Android Tamer (www.androidtamer.com) and CodeVigilant (www.codevigilant.com). His work can be found at anantshri.info

Anthony Webb works as a Senior Security Consultant with NotSoSecure. His expertise involves Infrastructure Security, penetration testing and red teaming. he has delivered multiple advanced training at conferences such as Black Hat, as well as smaller classroom groups and live web-based training delivery.

DAY 1

- **IPv4/IPv6 Basics**
- **Host Discovery & Enumeration**
- **OSINT & Asset Discovery**
- **Hacking Application and CI Servers**
- **Oracle Database Exploitation**
- **Windows Vulnerabilities and Configuration Issues**
- **Windows Desktop 'Breakout' and AppLocker Bypass Techniques**
- **A/V & AMSI Bypass Techniques**
- **Offensive PowerShell Tools and Techniques**
- **Local Privilege Escalation**
- **Post Exploitation Tips, Tools and Methodology**
- **An Introduction into Active Directory Delegation**
- **Pivoting, Port Forwarding and Lateral Movement Techniques***

DAY 2

- **Linux Vulnerabilities and Configuration Issues**
- **User/Service Enumeration**
- **File Share Hacks**
- **SSH Hacks**
- **Restricted Shells Breakouts**
- **Breaking Hardened Webservers**
- **Local Privilege Escalation**
- **MongoDB, TTY, Reverse tunneling**
- **Post Exploitation**
- **VLAN Hopping**
- **Docker breakout**
- **Kubernetes vulnerabilities**
- **Hacking VoIP**
- **Exploiting Insecure VPN Configurations**
- **B33r 10**