INFRASTRUCTURE TRAINING BLACK HAT EDITION

OVERVIEW

(Both intermediate and advanced classes)

This four day course will teach you various attack techniques to compromise various operating systems, networks and/or devices. Whatever your final objectives, like penetration testing, red teaming, or gaining a better understanding of managing vulnerabilities in your environment, understanding advanced hacking techniques for infrastructure devices and systems is critical.

You will be hacking into these challenges and will be compromising domains, systems and/or devices.

WHO SHOULD ATTEND?

- Sys admins, SOC staff, security analysts consultants, information security officers, anyone who wants to improve their skillset.
- This also helps students to prepare for advanced examinations such as Crest CCT exam, tiger exams, OSCP, etc.

- **Prrequisites;** Own laptop with VMWare or other similar product
- An understanding of Windows/Linux concepts is necessary and any security knowledge is a bonus.

FOUR DAY SYLLABUS

Text in ORANGE relates to advanced topics and challenges

Day 1

- TCP/IP basic concepts
- Open source intelligence (OSINT)
- Network scanning – probing, The art of port
- Scanning (TCP/UDP/ICMP)
- Service enumeration techniques (Windows/Linux)
- Hacking application servers
- Brute force attacks – multiple services
- Password cracking – tips, tricks and challenges

Day 2

- Windows hacking – Windows vulnerabilities, exploitation using local and remote exploits, multiple privilege escalation challenges*. Some of the hacks include MS14068 (Kerberos forged tickets), pass the hash, domain compromises.
- Metasploit crash course exploitation, pass the hash, custom payloads, anti-virus evasion* and postexploitation topics

Day 3

- Assessing Linux services
- Service enumeration (Finger, SSH, NFS, RPC, etc.)
- Service misconfigurations and Linux misconfigurations for privilege escalation*
- Exploitation and mitigation

Day 4

- Hacking VoIP solutions
- Attacking VPNs
- VLAN hopping (VLAN attacks, traffic sniffing exercises)*
- B33r 101