HACKING POINT

CHECK POINT

Advanced Infrastructure Hacking

4 day class | Get Certified | Advanced Track

This class continues the Infrastructure Hacking series

- Understanding Advanced Hacking techniques for infrastructure devices and systems is critical for penetration testing, red teaming, and managing vulnerabilities in your environment.
- Students will become familiar with hacking techniques for common operating systems and networking devices.

You will have access to:

- State-of-the-art hacklab with relevant tools and VMs
- Dedicated Kali VM to each attendee
- Scripts and tools are provided during the training, along with student hand-outs.

CLASS CONTENT

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

WHO SHOULD TAKE THIS CLASS

- System administrators
- SOC analysts
- Penetration testers
- Network engineers
- Security enthusiasts
- Anyone who wants to take their skills to the next level

NotSoSecure part of claranet cyber security