Ver.1.2

- شما میتوانید آنلاین در این دوره ثبت نام کنید و بلافاصله از آن استفاده کنید.
- دیدن نمونه آموزش های دوره تست نفوذ

Information Gathering

- Bash scripting

Information gathering (passive)

- Google operators
- Google Dorks – exploit-db.com
- Email Harvesting - goog-mail
- Netcaft.com

Open Services Information Gathering

- Forward Lookup Brute Force
- Reverse Lookup Brute Force
- DNS Zone Transfers
- Dnsenum

Open Services Information Gathering (part2)

- Meta Data Information gathering
- Metagofil – exiftool
- SNMP Reconnaissance
- Enumerating with SNMP (MIB - OID)
- SMTP Reconnaissance

NETBIOS Information Gathering

- NULL Sessions
- Cain & Able
- nbtscan

ARP Spoofing

- ARP replay
- Edit ARP Packet
- File2cable
- URLsnarf

Sniffing

- Ettercap (ARP/DHCP/ICMP/PORT/NDP)
- DNS Spoof

- Ettercap Filters
- Fake SSL Certificate
- SSLStrip
- Cain and Able

Port Scanning

- Nmap
- Nmap Scan Options
- Scripting

Cryptography

- History
- Steganography
- Symmetric vs asymmetric
- Cryptography Hash Functions
- Hash as fingerprint
- Password login with salt
- MD5 checksum
- Hash-identifier

Windows Exploit Development

- Memory management
- Buffer overflow
- Protocol Fuzzing
- Control EIP and Exploit writing
- Generate Shellcode using msfvenom
- Shellcode Bad characters and NOPs
- Replace shellcode

Metasploit Framework

- Metasploit Framework Components
- Exploit Options
- Payload /Shell / Meterpreter
- Staged /Inline(non-Staged)

Web application penetration test

- Introduction
- OWASP top 10
- HTTP Protocol

- Stateless – Stateful
- HTTP – HTTPS
- Sessions vs Cookie
- Proxy Tools --- Burp-Suit – Zed Attack Proxy (ZAP)

Web-Sqli-authentication bypass

- Sqli - Authentication bypass
- Authentication bypass using Hydra
- Authentication bypass using Burp-suite

web password

- brute force username and password
- brute force using Hydra
- brute force using Burp suite with intruder
- brute force using Acunetix

web directory attack

- http status coder
- Dirbuster – Directory Brut force
- Malicious file exaction

Web attack – Local file inclusion

- Web Fuzzing
- Local file inclusion to remote code execution
- SSH login technique /var/log/auth.log
- LFI to reverse shell
- Privilege escalation with Local Exploit (Linux Kernel 2.6 UDEV)
- proc/self/environ technique using Burp-suite
- PHP://filter load source code

Web attack – cookie

- Insecure Sessions
- Session fixation Attack

Cross Site Request Forgery

- CSRF Using DVWA

Password Attack

- Linux Shadow File

- Local Access – Offline
- Bkhive - Samdump2
- LM vs NTLM hashDump
- Injection via LSASS
- Registry Reading via SAM
- Dumping Active directory Password Hashes
- NTDSXtract - ntds_hashextract.rb
- Cachedump
- Brute-Force
- Directory attack
- Rainbow Tables
- Hashcat - John the Ripper
- Online Crackers - Online Forums
- Windows Credential Editor (WCE)
- Mimikatz
- Passing the Hash in Windows
- Impacket - smbexec.py
- Swiss army knife for pentesting Windows/Active Directory environments

Privilege Escalation

- Windows Privilege Escalation
- Windows-privesc-check
- AccessEnum
- Hot Potato
- Metasploit Local exploit
- Bypassing UAC - getsystem
- Linux Privilege Escalation

FileTransfer

- ftp
- tftp
- nc
- Use VBScript
- Use PowerShell
- Using debug.exe

Client Side Attacks

- BeEF - SET
- Client Side Exploit

- Java Signed Applet Attack

Port Redirection and Tunneling

- Port Forwarding/Redirection
- SSH Tunneling
- HTTP Tunneling
- reDuh / tennc

Finding Vulnerabilities

- Nessus / OpenVAS
- Metasploit Scanner Modules
- Web Application Scanning
- Nikto / Acunetix / Arachini