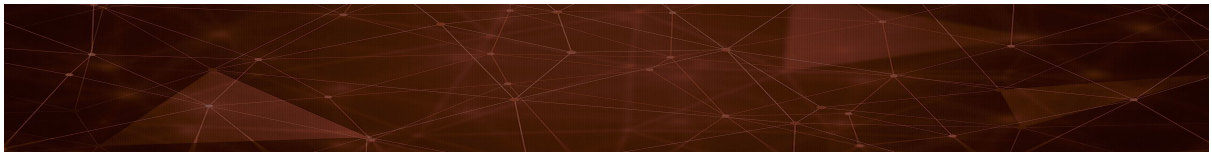
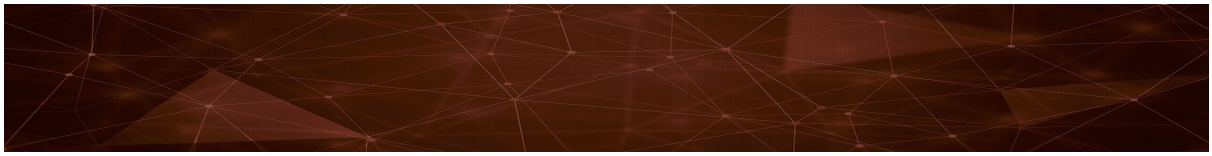


Module:1 (Information Gathering: Port Scanning) ***2***
1- Nmap 2
Introduction *2*
Getting Practical *3*
2- Netdiscover 6
3- Netcat 8
4- Masscan 8
Module:2 (File Transfer Techniques) ***10***
Why 10
1- FTP 11
2- TFTP 12
3- Netcat 13
4- SMB 15
5- RDP 15
Module:3 (The Metasploit Framework) ***16***
1- Structure 16
2- Information Gathering 17
3- Vulnerability Scanning 20
4- Payloads 21
5- Exploitation 22
6- Meterpreter 23
Functionalities : *23*
Module:4 (MITM: Sniffing and Interception) ***25***
1- Wireshark 25
2- Ettercap 30
Information Gathering : *30*
Exploitation : *32*
Module:5 (Client Side Attacks) ***34***
1- Information Gathering 34
BeEF Framework *34*
2- Exploitation 37
Using Public Exploits *37*
Metasploit's browser/autopwn *37*
Module:6 (Privileges Escalation, Persistence & Pivoting) ***39***
Privileges Escalation 39
1- Unquoted Service Paths 39
2- Vulnerable Services 41
3- AlwaysInstallElevated 42
Persistence 43
1- Meterpreter 43
2- Regular shell 45
Pivoting 46
1- Static Port Redirection 46
2- Dynamic Port Redirection 48
Module:7 (Password Cracking) ***53***
Password Cracking 53
1- Online 53
2- Dictionary Based (Using Hashcat) 53
Module:8 (Web Application Hacking) ***55***
1- SQL Injection 55
Error based *55*
Union based *56*
Blind injection *60*
2- Cross-Site Scripting (XSS) 62
Reflected *62*
Detection *63*
Exploitation (Stealing the Session ID) *64*



Stored (Persistent).....65
Detection.....65
Exploitation.....66
3- Cross-Site Request Forgery (CSRF).....67
Detection & Exploitation.....67
***Module:9 (Buffer Overflows)*.....70**
1- Direct EIP overwrite.....70
2- SEH Bypass.....80
3- Egg Hunter.....88
***Module:10 (Working With Public Exploits)*.....92**
1- Bad Return Address.....92
2- Payload Replacement.....95
***Module:11 (Antivirus Evasion & File Backdooring Techniques)*.....97**
1- Metasploit.....97
2- Hex.....100
3- Assembly Encryption.....115
***Module:12 (Hacking Embedded Devices)*.....123**
1- Firmware Extraction and Inspection.....123
2- Vulnerability & Exploitation.....123
3- Backdooring.....123
***Module:13 (WIFI Cracking)*.....124**
1- WEP.....124
2- WPA.....124
3- WPS.....124
4- MAC filtering.....124
5- Hidden SSID.....124