Truephers Certified Network Penetration Tester
Network Penetration Testing Training
40 hours Training Course

Lab Setup

- Introduction to Virtual Machines.
- Installation of Virtual Box, VMWare, KVM's
- Networking in Virtual Machines
- Importing/ Exporting Virtual Machines
- Installing Kali Linux
- Installing Virtual router and switches.

TM

Kali Linux

- Installing and Configuring SSH, FTP, TFTP, Apache, Tomcat, Postgresql, Python, and other important services and daemons in Kali Linux
- Installing and Configuring Kali Pen testing Tools
- Bash Scripting
- Essential Tools – Netcat, Ncat, SOCAT, Wireshark, tcpdump

Router Attacks

- Configuring routers
- Default credentials
- Attacking SSH
- Attacking HTTP
- HTTP brute forcing credentials
- Attacking SNMP
- SNMP key finder
- SNMP onesixtyone
- SNMP visualization
- Attacking FTP

Enumeration / Information gathering

- SMB Enumeration
- SMTP Enumeration
- SNMP Enumeration
- DNS Enumeration

Scanning Networks

- Nmap scans
- OS Scanning and Fingerprinting
- NMAP Scripting Engine
- Nessus Scanning
- OpenVAS Scanning
- Enumerating Users
- NetCat for Pentester
- DNS scanning
- Open port scanning
- Filtered ports
- Scan types.
- Port knocking.
- Default ports.
- Banner grabbing.

ARP | ARP poisoning

- ARP
- Static ARP entries
- ARP protocol visualization.
- ARP tables
- Deleting ARP entries
- Poisoning ARP

Man in the Middle attack

- Cain and Able.
- HTTPS Sniffing | SSL striping
- Etter-cap

Wireshark

- Wireshark visualization.
- PCAP analysis
- Extracting data from PCAP files.
- Filters
- Connection visualization.

Metasploit Framework

- Installing or updating
- User Interfaces
- Exploring Auxiliary module
- Exploring Exploit module
- Metasploit Payload module
- Searchsploit Exploit-db
- Staged vs. Non-staged payloads
- Meterpreter
- MSFVenom
- Exploiting with MSF
- Database and NMAP integration

Client Side Attacks

- Client side attacks with Metasploit
- Exploiting Network services to get meterpreter
- Evading Antivirus software
- Creating malicious services
- Responder

Social Engineering Toolkit

- Creating browser based exploits
- Create Java applets based exploits
- Create payloads to exploit PDF, DOC files
- DLL based exploitation
- Phishing page in SET

IPS | IDS

- Intrusion Detection Systems
- Firewalls
- Intrusion Prevention System
- WIPS, WIDS
- Snort

DNS Poisoning

- Changing DNS in host file
- Router DNS Configurations.
- DNS poison through MITM attack

Post Exploitation

- Linux Privilege Escalation
- Windows Privilege Escalation
- Mimikatz
- PWDump
- FGDump
- Cracking Hashes
- Pivoting
- Misconfigured File permissions
- Kernel Exploits
- Port Forwarding and Tunneling
- Persistence backdoors

Report Generation

- Sample Reports
- Report generation tools
- Maintaining Important links and texts in report generation