

```

\documentclass{article} % use \documentstyle for
old LaTeX compilers

\usepackage[utf8]{inputenc} % 'cp1252'-Western,
'cp1251'-Cyrillic, etc.
\usepackage[english]{babel} % 'french', 'german',
'spanish', 'danish', etc.
\usepackage{amsmath}
\usepackage{amssymb}
\usepackage{txfonts}
\usepackage{mathdots}
\usepackage[classicReIm]{kpfonts}
\usepackage{graphicx}

% You can include more LaTeX packages here


\begin{document}

%\selectlanguage{english} % remove comment
delimiter ('%') and select language if required


\noindent \includegraphics*[width=13.33in,
height=7.50in]{image92}


\noindent \includegraphics*[width=13.33in,
height=7.50in]{image93}


\noindent \includegraphics*[width=13.33in,
height=7.50in]{image94}


\noindent \textbf{Ethical Hacking}


\noindent \textbf{Hackers}


\begin{enumerate}

```

\item Types

\item White hat

\item Black hat

\item Grey hat

\item Suicidal

\item Categories

\item Coder

\item Admin

\item Script Kiddies

\end{enumerate}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image95}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image96}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image97}

\noindent \includegraphics\*[width=12.11in,  
height=5.62in]{image98}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image99}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image100}

```
\noindent \includegraphics*[width=13.33in,
height=7.50in]{image101}
```

```
\noindent
\section{Security Triangle}
```

```
\noindent \includegraphics*[width=13.33in,
height=7.50in]{image102}
```

```
\noindent \includegraphics*[width=13.33in,
height=7.50in]{image103}
```

```
\noindent \includegraphics*[width=13.33in,
height=7.50in]{image104}
```

```
\noindent
```

```
\noindent \textbf{SecurityUsability }
```

```
\noindent
\section{Essential Terminologies}
```

```
\begin{enumerate}
\item \textbf{ }Vulnerabilities
```

```
\item Weakness through which attacker can breach
targeted systems security
```

```
\item Exploits
```

```
\item Tools/keys through which security is
breached
```

```
\item Payload
```

```
\item Code that runs on targeted system
```

```
\item Single, Stager, \& Stages
```

```
\end{enumerate}
```

```
\noindent
```

```
\section{How does exploitation works}
```

```
\noindent \includegraphics*[width=12.02in,  
height=5.37in]{image105}
```

```
\noindent
```

```
\section{Process/ Phases}
```

```
\begin{enumerate}
```

```
\item \textbf{ }Reconnaissance
```

```
\item Information gathering about the target
```

```
\item Scanning
```

```
\item Networks, Ports, Vulnerabilities
```

```
\item Gaining Access
```

```
\item Vulnerabilities, Exploits
```

```
\item Maintaining Access
```

```
\item Backdoors
```

```
\item Clearing Tracks
```

```
\item Daisy Chaining
```

```
\item Reporting
```

```
\end{enumerate}
```

```
\noindent
```

```
\section{Tools}
```

```

\begin{enumerate}
\item \textbf{ }NMAP

\item Angry IP Scanner

\item Cain \& Abel, John the ripper, THC Hydra,
Aircrack-ng

\item Ettercap

\item Metasploit Framework

\item SuperScan

\item OWASP Zed Attack Proxy

\item Burp Suite

\item SQLmap

\item Wireshark
\end{enumerate}

\noindent
\section{Questions}

\begin{enumerate}
\item \textbf{ }Hacker who helps in strengthening
security of cyber space in consent with the network
owner is known as {\dots}..

\item A Coder could be

\begin{enumerate}
\item Black hat
c) Grey hat
\end{enumerate}
b) White hat
d) Suicidal hacker
\end{enumerate}

```

\item Getting domain name details using WHOIS is a part of

```
\begin{enumerate}
\item Reconnaissance
c) Gaining access
\end{enumerate}
b) Scanning
d) None
```

\item Backdoors are used for

```
\begin{enumerate}
\item Reconnaissance
c) Maintaining access
\end{enumerate}
b) Scanning
d) Reporting
```

1) Tools/keys through which security is breached are known as

a) Exploits                      b) Payloads  
c) Shell codes                      d) None

\noindent 5) ITU-T standard which defines Security Architecture for end to end communication security

a) X.25                                      b) X.509  
c) G.783                                      d) X.805

\noindent 7)              Name of the Protocol Analyser

a) Nmap b) Wireshark              3) John the Ripper  
4) None

\noindent  
\section{Reconnaissance}

\begin{enumerate}

\item \textbf{ }Footprinting, Scanning \&  
Enumeration

\item Covertly discover and collect information  
about target system

\item Initial information

\item Network range

\item Active machines

\item Open ports and Access Points

\item Fingerprint the OS

\item Services on Ports

\item Map the Network

\item Active/Passive Reconnaissance  
\end{enumerate}

\noindent

\section{Footprinting}

\begin{enumerate}

\item \textbf{ }Getting Possible information about  
target

\item Active/ Passive

\item Domain name, IP Addresses, Namespaces

\item Employee Information, Phone Numbers, E-mails

\item Job Information

\item <http://www.whois.com/whois> for information on domain name, [ip2location.com](http://ip2location.com) for further details of website, IP Address Ranges of a multiple IP addresses serving different domains and sub-domains, can be obtained for a particular company using American Registry for Internet Numbers (ARIN) and [www.archive.org](http://www.archive.org) for history of any website

\end{enumerate}

\noindent  
\section{Fingerprinting}

\begin{enumerate}

\item \textbf{ }Used to determine what OS is running on a remote computer

\item Active/ Passive

\item To determine OS we look at

\item TTL, Window size, DF, TOS

\item (Method not 100\% accurate but works better for some OS than others)

\item Once OS is Known where the website is hosted, Use NMAP for OS, Open Ports associated with IP/Domain name

\item Ping Sweep/ ICMP sweep: Which IP address from a range of IP Addresses map to live host

\end{enumerate}

\noindent  
\section{Scanning}

\begin{enumerate}



```

\item \textbf{ }Port Scanning Techniques

\item Non-stealth scanning

\item Stealth scanning

\item Defence

\item Configure firewall and IDS rule to detect
and block probes

\item Block unwanted ports at the firewall

\item Hide sensitive Information from public view

\item Use custom rule set to lock down the network

\item Tools: NMAP, Angry IP Scanner
\end{enumerate}

\noindent
\section{Nmap}

\noindent \includegraphics*[width=10.84in,
height=5.17in]{image106}

\noindent
\section{Enumeration}

\begin{enumerate}
\item \textbf{ }Attacker \textbf{creates active
connections to the target }and \textbf{perform
direct queries }to gain more information about the
target

\item Use extracted information to identify system
attack points and perform password attack to gain
unauthorised access

```

- \item Conducted in Intranet environment
  - \item Enumeration Techniques
  - \item Extract usernames from email ids
  - \item Extract information using default passwords
  - \item Extract user name using SNMP, Brute force using active directory, Extract user groups from windows
  - \item Information from DNS Zone transfer
- \end{enumerate}

\noindent

## \section{DNS Enumeration}

\begin{enumerate}

\item \textbf{ }DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization.

- \item Get the host's addresses
- \item Get the nameservers
- \item Get the MX record
- \item Perform \textbf{axfr }queries on nameservers
- \item Get extra names and subdomains via \textbf{Google scraping}
- \item Brute force subdomains from file can also perform recursion on subdomain that has NS records

\item Calculate C class domain network ranges and perform \textbf{whois }queries on them

\item Perform \textbf{reverse lookups }on  
\textbf{netranges}  
\end{enumerate}

\noindent  
\section{Kali Linux}

\begin{enumerate}  
\item \textbf{ }World's most powerful and popular  
penetration testing platform

\item Used by security professionals in a wide  
range of specializations, including penetration  
testing, forensics, reverse engineering, and  
vulnerability assessment.

\item Built on the work of the Debian project and  
adds over 300 special-purpose packages of its own,  
all related to information security, particularly  
the field of penetrating testing.

\item Used for Information gathering,  
vulnerability analysis, web application analysis,  
reverse engineering, sniffing and spoofing,  
exploitation tools, post exploitation, forensics,  
and reporting purposes  
\end{enumerate}

\noindent  
\subsection{Metasploit Framework}

\begin{enumerate}  
\item \textbf{ }The Metasploit Framework (Msf) is a  
free, open source penetration testing solution  
developed by the open source community and Rapid7

\item It was initially written in Perl (2003) and later re-written in Ruby in 2007

\item \textbf{Metasploit Framework:}

\item The basic steps for exploiting a system using the Framework include:

\item Choosing and configuring an \textit{exploit} (code that enters a target system by taking advantage of one of its vulnerabilities; about 900 different exploits for \textbf{Windows, Unix/Linux} and \textbf{Mac OS X} systems are included);  
\end{enumerate}

\noindent

\section{Metasploit Framework}

\begin{enumerate}

\item \textbf{ } Optionally checking whether the intended target system is susceptible to the chosen exploit;

\item Choosing and configuring a \textbf{payload} (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);

\item Choosing the encoding technique so that the intrusion prevention system (IPS) ignores the encoded payload;

\item Executing the exploit.

\item Clearing Tracks

\end{enumerate}

\noindent

\subsection{Kali Linux and Metasploit}

\begin{enumerate}

\item \textbf{ }World's most powerful and popular penetration testing \& digital forensic platform which includes Metasploit Framework among other several Penetration Testing tools such as Information Gathering tools NMAP/ ZenMAP, Searchsploit, DNS tools dnsenum.pl, DNSMAP, dnstracer, Hping3 etc.

\item From Kali, one can run metasploit directly through command line, access a Metasploit GUI front end called Armitage or use Metasploit packages available in tools like the Social Engineering Toolset (SET)

\end{enumerate}

\noindent

\subsection{Wireshark: Packet Analyser}

\begin{enumerate}

\item \textbf{ }Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports

\item Used for \textbf{network }troubleshooting, analysis, software and communications protocol development, and education

\item Terminal based version (non-GUI) is called Tshark

\item OS: Cross Platform written in c, c++  
\end{enumerate}

\noindent  
\subsection{Wireshark}

\begin{enumerate}  
\item \textbf{ }Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.

\item Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.

\item Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, Tshark

\item Data display can be refined using a display filter.  
\end{enumerate}

\noindent  
\subsection{Wireshark : Packet Analyser }

\begin{enumerate}  
\item \textbf{ }Plug-ins can be created for dissecting new protocols.

\item VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.

\item \includegraphics\*[width=7.19in, height=3.83in]{image107}Raw USB traffic can be captured

\item Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

\end{enumerate}

\noindent

\subsection{Gaining Access: Sniffing}

\begin{enumerate}

\item \textbf{ } Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of ``tapping phone wires'' and get to know about the conversation. It is also called \textbf{wiretapping} applied to the computer networks.

\item What can be sniffed?

\item Email/Web traffic, Chat sessions

\item FTP/Telnet passwords

\item Router configuration

\item DNS traffic

\end{enumerate}

\noindent \textbf{Sniffing{\dots}How ?}

\noindent \includegraphics\*[width=10.81in, height=4.80in]{image108}

\noindent \textbf{Sniffing contd{\dots}.}

\begin{enumerate}

\item Passive Sniffing

- \item Active Sniffing
- \item MAC Flooding
- \item ARP Poisoning
- \item DHCP Attacks
- \item DNS Poisoning
- \item Spoofing Attacks
- \item Affected Protocols
- \item HTTP, SMTP, NNTP, POP, FTP, IMAP, Telnet
- \item Hardware Analyser Tools, LI (wiretapping)

\end{enumerate}

\noindent

\subsection{ARP Poisoning}

\begin{enumerate}

- \item \textbf{ }ARP operates by broadcasting a message across a n/w, to determine the Layer 2 address (MAC address) of a host with a predefined Layer 3 address(IP address)
- \item The host at the destination IP address sends a reply packet containing its MAC address
- \item After initial ARP transaction , the ARP response is cached by the originating device
- \item In ARP spoofing attack, the ARP messages contain the \textbf{IP address }of network, such as



\textbf{default gateway}, or a \textbf{DNS server}

and replaces the

\end{enumerate}

\noindent \textbf{MAC address }for the

corresponding \textbf{network resource }with its

\textbf{own MAC address }

\begin{enumerate}

\item With new ARP information, the attacker is in the \textbf{Man-In-The Middle}

\end{enumerate}

\noindent

\subsection{ARP Spoofing}

\noindent \includegraphics\*[width=9.32in, height=3.74in]{image109}

\begin{enumerate}

\item Attack tools: Ettercap, Cain and Abel for MS Window platforms

\item Mitigation: Dynamic ARP Inspection (DAI)-Interception and validation of IP-MAC address relationship of all packets on untrusted ports.

\end{enumerate}

\noindent \includegraphics\*[width=13.33in, height=7.50in]{image110}

\noindent \includegraphics\*[width=13.33in, height=7.50in]{image111}

\noindent \includegraphics\*[width=13.33in, height=7.50in]{image112}

\noindent \includegraphics\*[width=11.96in,  
height=5.82in]{image113}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image114}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image115}

\noindent \includegraphics\*[width=13.33in,  
height=7.50in]{image116}

\noindent  
\section{MAC Address Spoofing}

\begin{enumerate}  
\item \textbf{ }Tools

\item Some OS allows changing MAC address from  
adaptor setting

\item Last shown attack could be executed with the  
tools used for ARP sppofing such as Nmap

\item Mitigation

\item Port Security: It enables an administrator  
configure individual switch ports to allow only a  
specified number of source MAC addresses

\item Switch(config)\# \textbf{interface f0/13}

\item Switch(config-if)\# \textbf{switchport port-  
security}

\item configured on all user-facing interfaces  
\end{enumerate}

\noindent \textbf{MAC Table Overflow}

\begin{enumerate}

\item Limited size of MAC table

\item \includegraphics\*[width=7.55in, height=5.17in]{image117}Attacker will flood the switch with a large number of invalid source MAC addresses until the MAC table fills up

\item Switch will act as hub

\item Applicable for single VLAN

\item \textbf{Tool}: install ``dsniff'' and type ``macof''

\item \textbf{Mitigation }: Port Security

\end{enumerate}

\noindent

\section{DNS Spoofing}

\noindent DNS resolves IP address for a given Domain Name

\noindent \includegraphics\*[width=10.39in, height=4.69in]{image118}

\noindent

\section{DNS Cache}

\noindent \includegraphics\*[width=11.00in, height=5.32in]{image119}

\noindent

\subsection{DNS Cache Poisoning}

```

\begin{enumerate}
\item \textbf{ }\includegraphics*[width=8.43in,
height=5.36in]{image120}\textbf{Spread malware }

\item \textbf{Man-In-The-Middle}

\item \textbf{Denial of Service}
\end{enumerate}

\noindent
\subsection{Mitigation: DNSSEC}

\noindent \includegraphics*[width=8.75in,
height=5.01in]{image121}

\noindent
\subsection{BGP Peer Hijacking }

\noindent \includegraphics*[width=8.48in,
height=5.09in]{image122}

\noindent
\section{BGP Peer Hijacking }

\begin{enumerate}
\item \textbf{ }Tools

\item MAC or ARP spoofing

\item Sniff routing traffic and then perform
modification on routing updates

\item Control over devices due to very poor device
security using Telnet/ SNMP

\item Mitigation

```

\item Enable Security like 802.1x, ARP inspection, Port Security

\item Device hardening ( Patch update, securing remote access, access hardening )  
\end{enumerate}

\noindent  
\subsection{Exploitation}

\begin{enumerate}  
\item \textbf{ }Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities.

\item Metasploit is a powerful tool to locate vulnerabilities in a system.  
\end{enumerate}

\noindent \includegraphics\*[width=9.94in, height=3.71in]{image123}

\noindent  
\subsection{Exploitation{\dots}}

\begin{enumerate}  
\item \textbf{ }[www.exploit-db.com](http://www.exploit-db.com)\underbar{ } is the place where you can find all the exploits related to a vulnerability.  
\end{enumerate}

\noindent \includegraphics\*[width=12.19in, height=4.26in]{image124}

\noindent \textbf{Exploitation..}

\begin{enumerate}

\item Common Vulnerabilities and Exposures (CVE)

\item CVE is a dictionary of publicly known information security vulnerabilities and exposures. It's free for public use. <https://cve.mitre.org>  
\end{enumerate}

\noindent \includegraphics\*[width=11.37in, height=3.55in]{image125}

\noindent \textbf{Exploits{\dots}.}

\begin{enumerate}

\item National Vulnerability Database

\item You can locate this database at  $\mathrm{-}$  <https://nvd.nist.gov>  
\end{enumerate}

\noindent \includegraphics\*[width=8.50in, height=2.87in]{image126}

\begin{enumerate}

\item Remote exploits/ Local exploits  
\end{enumerate}

\noindent \textbf{Maintaining Access---}

\noindent \textbf{Trojans and Backdoors}

\begin{enumerate}

\item Trojan:

\item A program in which the \textbf{malicious code } is contained inside apparently harmless programming or data in such a way that it can \textbf{get control and cause damage } to your system

\item Replicate, spread, and get activated upon user's certain predefined actions  
\end{enumerate}

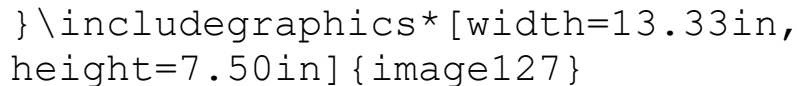
\noindent  
\subsection{Maintaining AccessTrojans and Backdoors}

\noindent Purpose:

\noindent Delete or replace \textbf{OS's critical files}; generate \textbf{fake traffic }to create \textbf{DOS attack}; Download spyware, adware, and malicious files; disable \textbf{firewall }and \textbf{antivirus}; create \textbf{backdoors }to gain remote access; infect victim's PC as a \textbf{Proxy Server }for relaying attack; use victim's PC as a \textbf{botnet }to perform DOS attack; use victim's PC for spamming and blasting email messages; steal \textbf{password, security codes}, credit card info using keyloggers .

\noindent  
\subsection{Maintaining Access: Trojan}

\noindent \textbf{Attacker}



\includegraphics\*[width=13.33in, height=7.50in]{image127}

\noindent \includegraphics\*[width=13.33in, height=7.50in]{image128}

\noindent \includegraphics\*[width=13.33in, height=7.50in]{image129}

```
\noindent \textbf{ Malicious code  
}\includegraphics*[width=13.33in,  
height=7.50in]{image130}
```

```
\noindent \includegraphics*[width=13.33in,  
height=7.50in]{image131}
```

```
\noindent \includegraphics*[width=13.33in,  
height=7.50in]{image132}
```

```
\includegraphics*[width=1.78in,  
height=1.78in]{image133}\includegraphics*[width=13.  
33in, height=7.50in]{image134}
```

```
\noindent \includegraphics*[width=13.33in,  
height=7.50in]{image135}
```

```
\noindent \includegraphics*[width=13.33in,  
height=7.50in]{image136}
```

```
\noindent
```

```
\noindent \textbf{Execute the damage routine  
Execute the dropper  
Propagate the Trojan}
```

```
\noindent  
\subsection{Trojan/Backdoors}
```

```
\begin{enumerate}  
\item \textbf{ }Pen Testing for Trojans and  
Backdoors
```

```
\item Scan for open ports
```

```
\item Scan for running processes, registry  
entries, device drivers, window services, startup
```



programs, files \& folders, network activities,  
modification of OS files

- \item Run Trojan scanner to detect Trojans

- \item Document all the findings

- \item If Trojans are detected, isolate the machine  
from network.

- \item Update and run antivirus/ find other  
antivirus solution to clean Trojans

\end{enumerate}

\noindent

\section{Maintaining Access: Trojan}

\noindent Mitigation:

\begin{enumerate}

- \item Awareness and preventive measures

- \item Anti-Trojan tools such as TrojanHunter \&  
Emsisoft

- \item Anti malware to detect and eliminate Trojans

\end{enumerate}

\noindent

\subsection{Cryptography}

\begin{enumerate}

- \item \textbf{ }Ransomware

- \item Objectives (CIAN)

- \item Substitution Ciphers, Caesar ciphers,  
Transposition Cipher

\end{enumerate}

```
\begin{tabular}{|p{4.4in}|p{1.8in}|} \hline
Symmetric \newline Encryption & Asymmetric \newline
Encryption \\ \hline
AES,RC4, DES, RC5,RC6 & RSA, DSA, ECT, PKCS \\
\hline
\end{tabular}
```

\textbf{Types}

\noindent \textbf{Cryptography Contd..}

\begin{enumerate}

\item SSH

\item Digital signature

\item PKI

\item Cryptography tools

\item Cryptography attacks

\item Cryptanalysis

\end{enumerate}

\noindent

\subsection{Clearing Tracks}

\begin{enumerate}

\item \textbf{ }Ensure you go undetected is very important

\item Kill all monitoring software

\item Anti Virus

\item Firewall

\item Host Based Intrusion Detection System (HIDS)

\item Metasploit's meterpreter scripts (payload)  
could help in clearing logs and killing AV and  
Firewall

\item Killav

\item Clean all logs

\item Event, application, and security  
\end{enumerate}

\noindent

\subsection{Rule of Engagement: Penetration  
Testing}

\begin{enumerate}

\item \textbf{ }Objectives

\item Rules of Engagement (Process, Skill \&  
Reporting)

\item Process

\item First: Agreement with client i.r.o. Scope,  
Time-lines,  
\end{enumerate}

\noindent Reporting format of results for technical  
specialists \& Business Representatives

\begin{enumerate}

\item Code of conduct with company \& individuals

\item Legal \& regulatory issues

\item Structured, systematic \& repeatable process

\item Organisations' security during information handling

\end{enumerate}

\noindent

\subsection{Rules of engagement{\dots}Process}

\begin{enumerate}

\item \textbf{ }Tools \& methodologies are tested before being used in live tests

\item Tests on applications with all levels of privileges, if applicable

\item All modifications executed against a system to be documented, and returned to their original positions, if possible

\item Access to compromised system to be maintained through proper authentication

\item Any action that could affect normal operation of system to be taken after written approval

\item All data to be destroyed once the report has been accepted

\item No logs to be removed, cleared or modified unless specifically authorised

\end{enumerate}

\noindent \textbf{Rules of engagement..}

\begin{enumerate}

\item Skills

\item Latest threats and countermeasures in various areas

\item Consider all stages of potential cybercrime attacks

\item Threat analysis on own research and other sources like SANS, P1, OWASP, Top-10

\item Specially tailored, manual test rather than running a set of automated tests using standard tools

\item Evaluate whole target environment rather than a particular system  
\end{enumerate}

\noindent \textbf{Rules of engagement..}

\begin{enumerate}

\item Reporting

\item Clear, insightful reports to technical specialists \& Business representatives

\item Constructive, expert remediation advice

\item Quantify findings \& business implications of technical weaknesses

\item Cause of delay, if any

\item Detailed list of action taken against compromised systems

\item No passwords to be included in the final report

\item Sensitive data in the report to be masked, if any  
\end{enumerate}

\noindent

\noindent

\end{document}