**List of Basic Concepts**

@@ version

* Sql command to show the database version

+x eXecute

* Linux command to give execute permissions

Aircrack-ng

* Aircrack is a package tool for wireless network hacking
* Aircrack-ng is the tool used to crack the protocol pre-shared key (WPE, WPA, WPA2)

Aireplay-ng

* Aireplay-ng is another tool from Aircrack package
* Aireplay-ng is used to force deauthentication and packet injection / replay frames

Airodump-ng

* Airodump-ng is another tool from Aircrack package
* Airodump is used to capture package on a selected channel, and it is also used to connect to network devices

Arpspoof

* A software for ARP poisoning attack
* **arpspoof -i [network interface] -t [ip address]**
  + Informing the interface to be used and the ip address we’re going to pretend to be
  + Doing this, arpspoof sends ARP responses to the target, informing that the legitimate IP’s MAC address is ours (attacker’s machine)
* ARP spoofing, also known as ARP poisoning, is a Man in The Middle Attack where the attackers send falsified ARP messages over a Local Area Network (LAN), to link an attacker’s MAC address with a legitimate computer. With this, the attacker could intercept all the communication being sent to him, while the victim thinking is communicating with another legitimate machine

BackTrack

* Algorithm that searches for brute force attacks

Bind & Back (Reverse) connect shells

* Bind Shell: the attacker connects to the target’s port
* Back (Reverse) Shell: the attacker makes the target connect to his or her machine’s port

Black Box Testing

* Type of pentest in which the pentester knows nothing about the target

BSSID & ESSID

* ESSID: name of the network
* BSSID: mac address

Nessus

* Vulnerability scanner

Netcat

* TCP/IP swiss army knife:
  + Connection
  + Banner Grabbing
  + Chat
  + File transfer
  + Honeypot
  + Scanning
  + Remote commands execution
* **nc -v [web site] [port]** 
  + connecting to a website
  + banner grabbing
* **netstat -nplt**
  + check services being executed in open tcp ports
* **nc -vlp [port]**
  + Opening a port and listening to it
* **nc -v [ip] < file.exe**
  + Transfering a file to a target
* **nc -vnz [ip] [port]**
  + Port Scan

Network File System (NFS)

* Mechanism to store files on a network. A distributed file system that allows users to access files and directories remotely and treat them as if they were local

Nikto

* Vulnerability scanner for web applications

Nmap

* Port scanner
* Vulnerability scanner

Nonce

* In cryptography, is a number used to prevent replay attacks
  + The attacker will intercept a valid transmission and repeat it or delay it
* Nonces are random or pseudo-random numbers that authentication protocols attach to communications

ORDER BY

* Command in SQL to order data, by id for example

Packet Sniffers

* Also known as protocol analyzers or network analyzers
* Softwares used to intercept and analyze traffic
* TCPdump, Wireshark

Penetration Test

* Tests done by a pentester / ethical hacker / cybersecurity professional / red teams to simulate an attacker and detect vulnerabilities

Php-shell

* Malicious code used in pos-exploitation
* c99shell
  + Backdoor shell
  + Transfer files, edit/delete/view files
* r57shell
  + Backdoor shell
  + Access the database

Ping

* Test the connection
* ping [ip address]

Privilege Escalation Exploit / Kernel Exploit

* The attacker gains privilege access / permission that he or she shouldn’t have
* Attacker gets administrative/root permissions while using a regular account

Proof of Concept (PoC)

* Proof of the vulnerability found
* Shows how an attacker is able to exploit an existing vulnerability
* Proof that the vulnerability exists

Reconnaissance

* Phase of pentesting
* Also known as information gathering
* Getting to know your target, get information
  + Ports, emails, names, addresses, IP’s, softwares, tools, etc

Remote File Inclusion (RFI)

* Vulnerability where the attacker can include files remotely into a application
* She or he is able to include a malicious software and exploit it

Scanning

* Search for information with scanner
* Vulnerability scanner
  + Nikto, Nessus
* Port scanner
  + nmap

SELECT

* SQL command to select information

Session Hijacking

* Exploiting a legitim session

Shell

* Window shell is a user graphic interface to windows operating system
* Powershell is a windows command line
* On Linux, shell is a command line interpreter

Spoofing

* IP Spoofing, ARP Spoofing, DNS Spoofing
* An attack which the attacker pretends to be a trustable user or device

Command Line Interface (CLI)

* Text based user interface used to runs programs, manage files, interact with the computer

CONCAT

* SQL command used to add two or more strings together

Cross-Site Scripting (XSS)

* Attack that takes advantage of the trust a user has for an application
* Reflected, DOM based, Stored
* Insert malicious scripts on a web application, which is included on the dynamic content that will be sent to the user

Default Gateway

* Path used to pass information when the device doesn’t know where the destination is
* Connects two networks with different transmission protocols together
* Entrance and exit network port

Dynamic Host Configuration Protocol (DHCP)

* Automatically assigns IP addresses to the devices on our network

Domain Name System (DNS)

* Domain Names
* Naming database in which internet domain names are located and translated into Internet Protocol (IP) addresses
* [www.google.com](http://www.google.com)

Fingerprinting

* Gather information to identify a target
  + Operating system, protocols, hardware, etc
* Passive and active fingerprinting
* Subcategory of footprinting

FTP server

* Enables file transfer

Graphical User Interface (GUI)

* Interface with graphical components (buttons, menus, icons) in which a user interacts with

Hackers

* Black hat hackers
  + Use knowledge for his or hers benefits
  + Attacks victims with phishings, companies, ransomwares
  + Not ethical
* Grey Hat Hackers
  + Can do both malicious and ethical actions
* Hacktivists
  + Activists hackers
  + Political Reasons
* White Hat Hackers
  + Ethical Hackers
  + Work to help others

Hashdump

* Command to obtain password hashes

HTTP

* Hypertext Transfer Protocol
* Communication Protocol
* World Wide Web (www)

ipconfig /all

* Windows command
* Check the MAC address, IP, Default Gateway
  + Check for detailed information about your network

iwconfig

* Linux command
* Similar to ifconfig, but about network interfaces

John The Ripper (JTR)

* Password cracker (hash)

Kali Linux

* Linux distribution that comes with hacker tools

KeyLoggers

* Recording everything the target types on the keyboard

Kismet

* Sniffer packet

LIMIT

* SQL command to limit a search

LOAD\_FILE

* SQL command to load files

Local File Inclusion (LFI)

* Vulnerability
* Include files that already exists on the server

MAC Address

* BSSID
* Physical address

Metasploit

* Software that helps on exploitation, vulnerability detection, etc

Meterpreter Payload

* Metasploit payload type

SQL - MySQL

* SQL - Structured Query Language
  + Programming language to communicate with databases
* MySQL - Database

SQL Injection (SQLi)

* Vulnerability
* Inject commands on the database
* Manipulate the database

Sqlmap

* Software used to search and exploit sqli vulnerabilities

SSH server

* Secure shell or secure socket shell
* Network Protocol for securely exchanging data between two computers

SYN Scan

* TCP scan that does not finish three way handshake
* nmap -sS
* nmap -sT
* nmap -sV

TCPdump

* Packet sniffer

TCP Three-way handshake

* SYN , SYN-ACK, ACK

Tshark

* Packet sniffer

UNION

* SQL command to combine two or more results in a single result

VNC Injection Payload

* Can be done with metasploit
* Virtual Network Computing (VNC) graphical desktop sharing system that uses the Remote Frame Buffer (RFB) protocol to remotely control another computer

WEP key

* Wireless network protocol
* Insecure, easy to crack

White Box Testing

* Type of pentesting in which the pentester has a large number of information about the target
* Can simulate a inside threat

WPA2

* Wireless network protocol
* Safer