Ethical Hacking & Penetration Testing

GHCI 2019 Workshop

Purva Singh

http://bit.ly/ghci-bwapp | linkedin.com/in/purvasingh96| github.com/purvasingh96

Burp Suite Essentials

1. Set Proxy on Firefox

Click “Open Menu” -> Preferences -> Network Proxy -> Settings -> Manual Proxy -> 127.0.0.1 & port 8080 -> Use for all protocols -> Ok

2. Proxy is used to intercept communications between website and users

Proxy -> Intercept -> Intercept is on

3. Two types of requests: GET and POST

GET: Retrieves data from the Server
POST: Post data to the Server

4. Use of repeater

a. Proxy is used to capture request
b. For specific requests, we need to modify our requests or see our responses, hence we use repeater.
Right Click -> Send to repeater (In “proxy -> Intercept” Tab)
c. To check response click on Go

Fluxion Essentials

1. Clone and Launch Fluxion

a. git clone https://github.com/wi-fi-analyzer/fluxion.git
b. Open terminal and change current directory to fluxion-master
c. run ./fluxion.sh

2. Scan for Target Network

a. Based upon your requirements, you can choose to monitor all channels or specific channels.

3. Select Attack Option and Start Deauthentication attack

a. You can choose to deauthenticate all clients or targeted clients
c. If you are able to see “WPA handshake: [MAC address of AP]”, you have successfully captured 4-way handshake.
d. Now select option-1 to create SSL certificate.

4. Create Evil-twin Access Point

Choose option-1 (web-interface) and select your language

5. Wait for the client to de-authenticate

a. Wait till your client connects to evil-twin AP.
b.Wifi Information window will display when the client has connected to the fake AP

6. Clients attempt to reconnect

After targeted client enters valid credentials in order to reconnect to real WAP, Aircrack-ng will display the Wi-Fi password and save it in a .txt file for you to review.

CHEAT SHEET

Nmap	GHDB	Shodan
Host Scanning - nmap -iL list-of-ips.txt **Port Scanning** - nmap -p 22 192.168.1.1 **OS Detection** - nmap -A 192.168.1.1 **Spoof MAC address -** nmap --spoof --mac <spoof-MAC-address> <your-IP-address>	Using **advanced search** to exploit target - operator:keyword additional search terms **Advanced operators -** ext, inurl, allurl, loc **Advanced keywords -** password | passlist | username | login **Examples -** inurl : "index.php?id="	Search engine which helps find systems on the internet. **Basic Search filters are-** **Port:** search by specific port **hostname**: Locate devices by hostname **os**: Search by Operating System **city**: Locate devices by city **Example-** **Cisco devices in New York** Cisco city:"New York"

CHEAT SHEET

1. SQL Injection

Overview

1. Add **'***(quote)* to check if the query throws an error.
2. Add **' '***(quotes separated by space)* to check if all records are displayed back to the user.
3. Union with fake values to check which columns are returned back to user
   For ex: **ghci' union select 1,2,3,4,5,6,7 #**
4. Get databases and credentials of users
   For ex: **ghci' union select 1,login,password,email,5,6,7 from users#**

Mitigations -

1. Proper input validation
2. Never use user input directly
3. Avoid malicious code e.g. single quote
4. Avoid visibility of database errors.

2. OS Command Injection

Overview-

1. Multiple OS commands can be executed at once by separating them using semicolon (;)
2. Syntax for OS command injection is as follows -
   <*user-input*>**;**<*malicious-command*>
   E.g. google.com**;**rm <*file-name*>

Mitigations-

1. Avoid calling OS commands from application-layer code.
2. Strong input validation
3. Never attempt to sanitize input by escaping shell metacharacter

4. Cross Site Scripting

Overview -

1. Check the websites for parameters whose input is reflected in response
2. Use <script>alert(**1**)</script> or many other payloads available on the internet to check if there is a popup
3. If a popup is found use '**document.cookie**' instead of '**1**' to use as a proper proof of concept

Mitigations -

1. Filter input on arrival
2. Use appropriate response headers
3. Content security policy

4. Broken Authentication

Overview

Brute-force
Use trial-and-error method to identify valid credentials of login page.

Dictionary attack

1. Open OWASP bricks and turn Burp Suite's intercept tab on.
2. Enter random credentials and click submit.
3. Capture the POST request made by you under target tab.
4. Set attack-type to cluster-bomb.
5. Under payload section, load your username and password dictionaries.
6. Perform **grep-matching** under Options tab to flag result items containing specified expressions in the response, e.g ("Valid credentials. Login successful.")
7. Start attack.

6. Wireless Penetration Attack

Commands Overview -

1. Enable monitor mode for you network card -
   sudo iwconfig wlan0 mode monitor

2. Check and kill interfering processes -
   sudo airmon-ng start wlan0
   sudo airmon-ng check kill wlan0

3. Scan surrounding wifi -
   sudo airodump-ng wlan0

4. Scan devices connected to target wifi -
   sudo airodump-ng -c <channel no.> --bssid <target's MAC address> wlan0

5. Start sending deauthentication frames -
   aireplay-ng -0 0 -a <target's MAC address> wlan0

7. Kali and OWASP BWA Installation Guide

Use the following links to install Kali Linux and OWASP BWA on your virtual machines -

.Kali Linux- http://bit.ly/kali-installation
OWASP BWA - http://bit.ly/owasp-installation