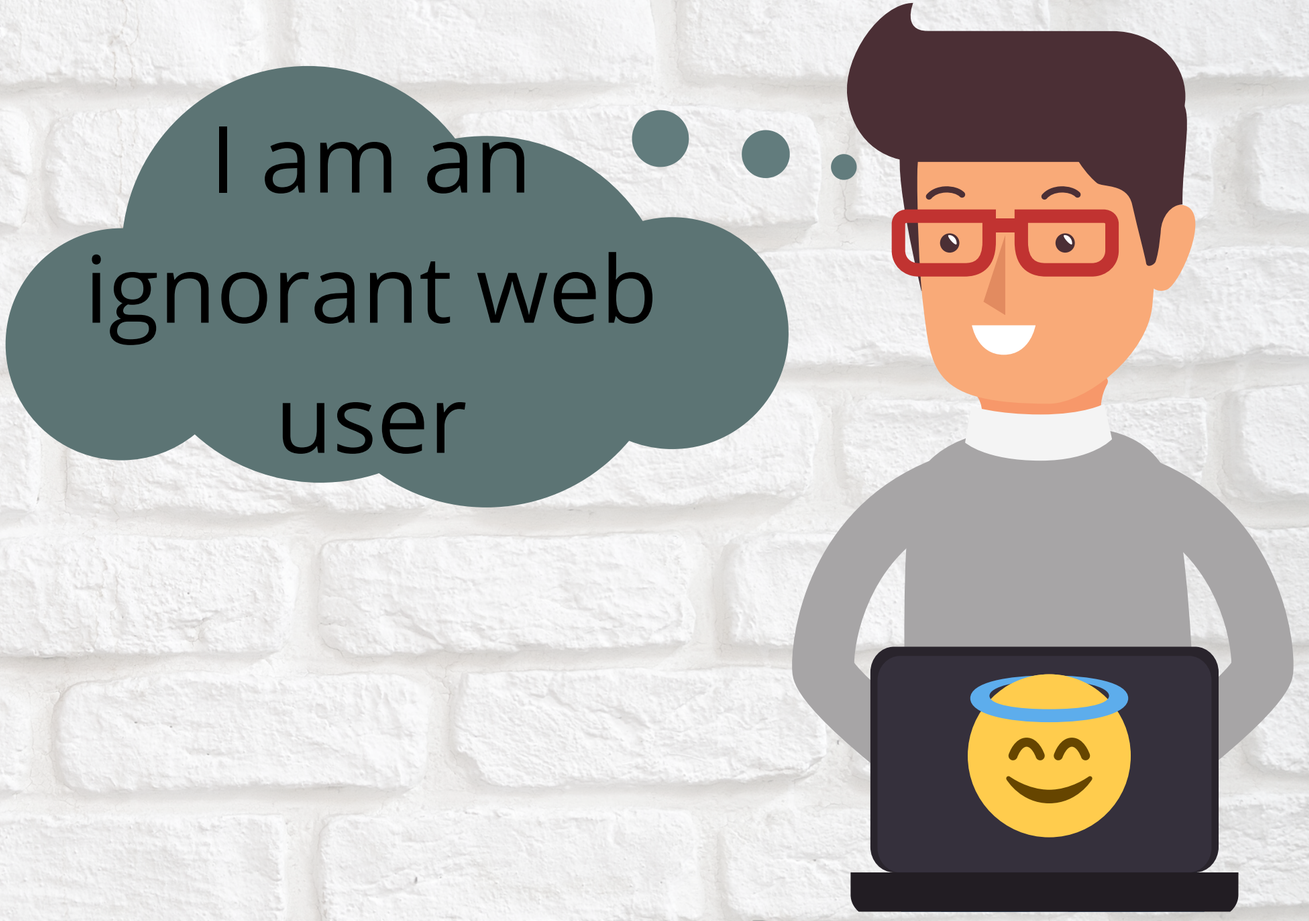
Breakdown on Breaking In

Meet & Greet

Meet Alice
He is our attacker



Meet Victor
He is our victim

BEEF Attack

- Browser Exploitation Framework(BEEF)
- User's browser is hooked by sending a malicious link
- Attacker then has complete access to the user's system
- Attacker can also escalate the attack from here

BEEF Attack

1

2

3

Complete Access 5

4

Steps:

- sudo apt-get install beef-xss
- Type beef-xss to run the program
- Enter a password for the default user "beef"
- Beef UI will open automatically in your browser
- Login with the password just set by you
- Create a malicious web page with the hook URL
- Send it to the user
- Boom! Browser Hooked

Wifi Deauth Attack

- Deauth means to disconnect
- To disconnect deauth packet is sent
- Spoof victim MAC address and send deauth packets to the router

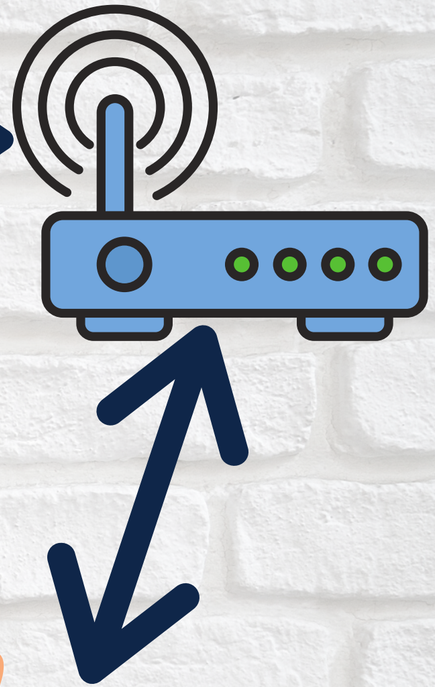
Wifi Deauth Attack

Coffee Shop

Scene 1

Wifi Deauth Attack

I am Victor & I
want to disconnect



Coffee Shop
Scene 2

Steps:

- Kill all the processes running on the wireless network interface(NIC)
- Put the Wireless NIC in monitor mode
- Start listening in monitor mode
- Start listening on the target network specifically
- Identify the victim MAC address
- Deauth

Bruteforce Attack

- Test Server:Tomcat Server
- Found is Metasploitable Linux
- Intentionally vulnerable
- Bruteforcing from a wordlist
- Wordlist:File containing all the possible combinations

Login Page

username

password

1

2

3

4

Correct Hit:

tomcat ✅

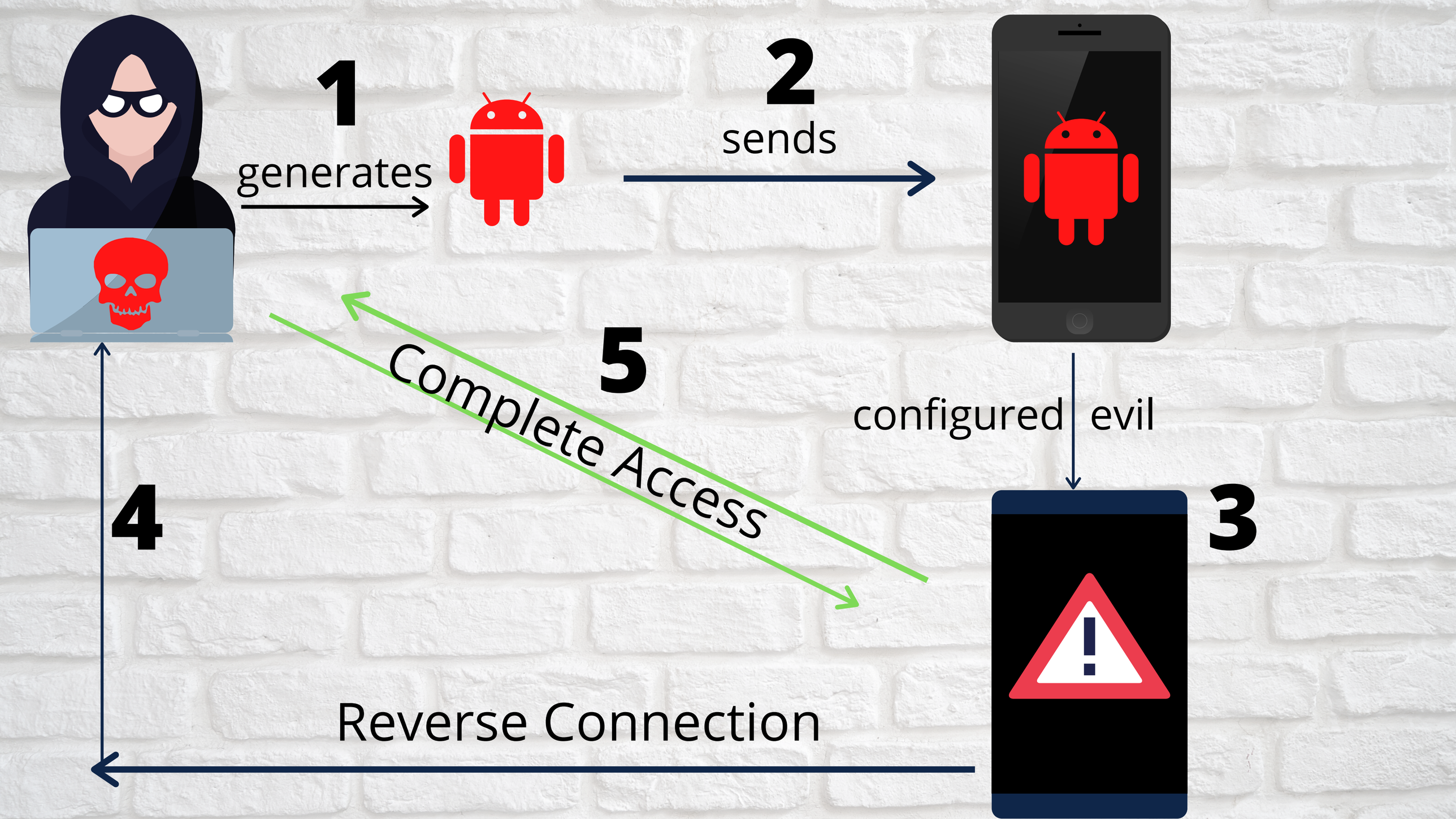
tomcat ✅

Steps:

- Set up the Tomcat Server
- Scan Metasploitable Machine using NMAP
- Open up login page of Tomcat Server
- Fire up Postgresql service
- Open msfconsole and use the required auxiliary
- Set required options for the auxiliary
- Bruteforce

Malicious Android APK

- Create an APK for a third party app
- APK contains malicious code
- Initiates a reverse connection to the attacker
- App can be beautified and customised


1
generates
2
sends
configured
evil
3
4
5
Complete Access
Reverse Connection

Steps:

- Fire up postgresql service
- Create the malicious APK
- Send it to the victim
- Social Engineer him/her to install the app
- Create a listener for incoming connections
- Connection coming from phone to the attacker is connected