



# POPCORN HTB WALKTHROUGH

Speaker - Raghav Talwar (CTF Player)

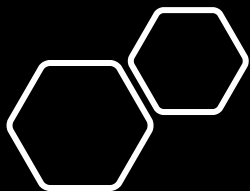
Popcorn

OS:  Linux

Difficulty: Medium

Points: 30



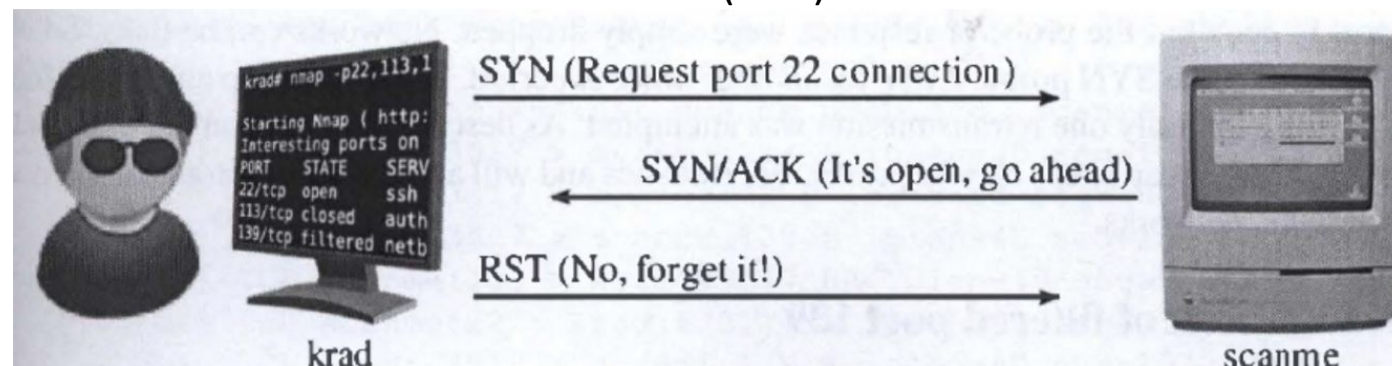


# Enumeration

- Nmap (Network Mapper)
  - Live hosts on a network
- What ports are open ?
- What Services are running on those ports?
- What Version of that service is running ?

**TCP 3 way Handshake** - Its an interaction between client and server,  
**Example, talk to a friend**

- Me : Hello (SYN)
- Friend : Hello as a response that I acknowledge you (SYN ACK)
- Me : Let's start a conversation (ACK)




## TCP SYN (Stealth) Scan (-sS)

*This is the default scan and is good for most purposes. It is quieter than a TCP Connect scan, that is, it won't show up on most simple logs. If it gets a SYN ACK packet back, then Nmap knows there is a service running there. If it doesn't get a response, it assumes the port is closed.*

## TCP Connect Scan (-sT)

*This works much like the SYN scan, except it completes the full TCP handshake and makes a full connection. This scan is not only noisy but also puts more load on the machines being scanned and the network.*



# Service Enumeration

## HTTP Service

## Directory Brute force

- Wordlists - /usr/share/wordlists/common.txt

## Exploiting Application Functionality

Burp Suite: Manually intercept all responses and requests between the browser and target application.

- HTTP METHODS
  - **POST** is used to send data to a server to create/update a resource.
  - **GET** is used to **request** data from a specified resource. (URLs parameter)

# File Upload Bypass via Burp Suite

- There are three common ways that a website will check for valid file types by comparing them to an allow- or deny-list:
  - **File Extension** – Add another layer of extensions
    - Like php.png
  - **Content-Type header** – image/png
  - **Magic bytes** – File signatures
    - magic bytes are just being checked in the file
- Once, reverse shell is uploaded onto the server. We need a way to execute it too.
- Torrent Upload Path - /torrent/upload

# Privilege Escalation Exploits (CVE)

---

- **System Enumeration & Exploitation**
  - **Kernel - What Kernel version and distro are we working with here ?**
- `uname -a` : Use this to search for Kernel exploits
- `lsb_release -a 2>/dev/null` : Use this to gain some knowledge of the OS running
- `Searchsploit <term>` : It is a command-line **search** tool for **Exploit-DB**
- **Steps –**
  - Configure, if needed
  - Transfer
  - Compile
  - Execute

# Tricks for Exploiting Kernel Vulnerability

- Do we need to transfer an exploit
- `which awk perl python ruby gcc cc vi vim nmap find netcat nc wget tftp ftp 2>/dev/null`
  - GCC is C compiler, which lets us compile .c exploits.
  - Syntax - gcc -o exploit exploit.c
- We are checking if **any compiler is installed**.
- This is useful if you need to use some kernel exploit as it's recommended to compile it in the machine where you are going to use it.



---

# Automation

- [LinPeas]  
(<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS>)
    - + Linux local Privilege Escalation Awesome Script
      - Red/Yellow : Pretty High
      - Red : High, if we get this, its better to stop and exploit the vulnerability
  - [Linux Exploit Suggestor]  
(<https://github.com/mzet-/linux-exploit-suggester>)
    - + Suggest exploits based on the traits of the machine
-



Thank You!