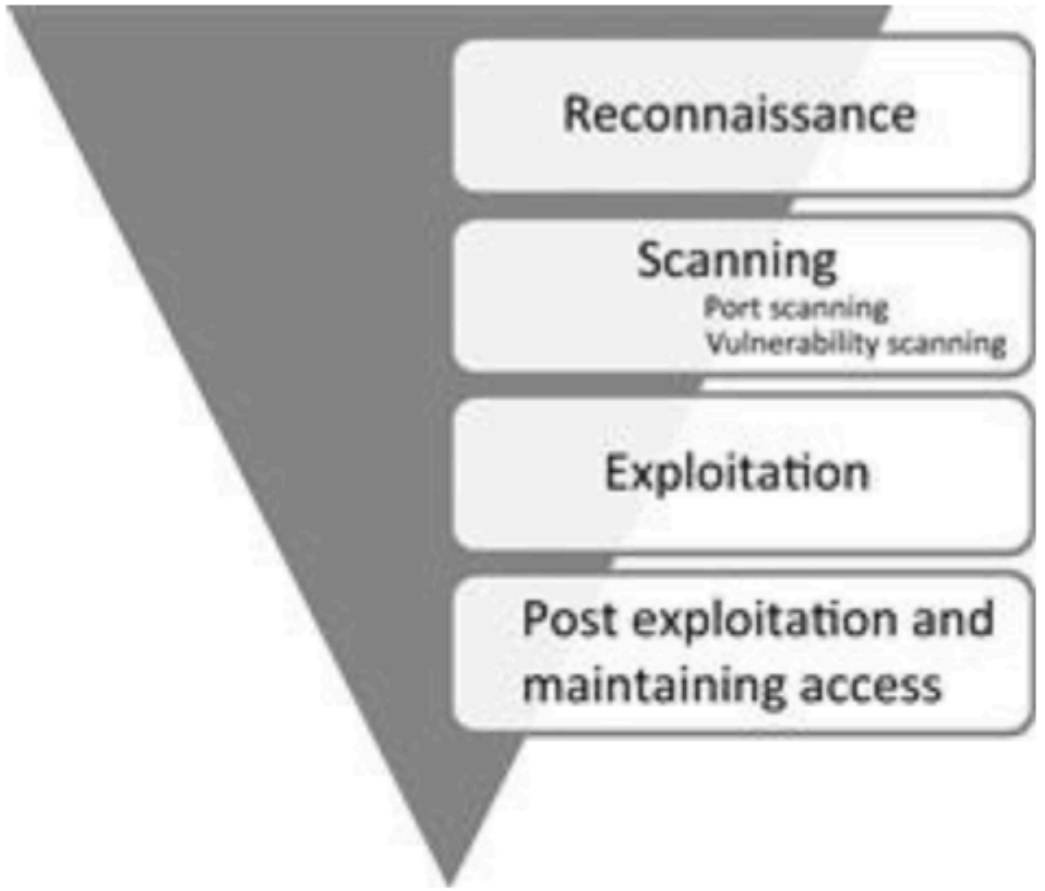
CYBER WARZONE

A BRIEF INTRODUCTION TO THE ATTACK-DEFENSE CTF

Tomáš Jirsík

Attack


Reconnaissance
Scanning
Port scanning
Vulnerability scanning
Exploitation
Post exploitation and maintaining access

nmap

- Network exploration tool and security / port scanner

- Usage: $ nmap [Options] {target ip}
- Example: **$ nmap -p- 10.1.33.7**

- Useful params:
  - -p <port ranges>: Only scan specified ports (-p- for all ports)
  - -T<0-5>: Set timing template (higher means faster scan)

```
root@kali:~# nmap -p- -T5 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2017-0
mass_dns: warning: Unable to determine any DNS se
 Try using --system-dns or specify valid servers
Warning: 192.168.56.101 giving up on port because
Nmap scan report for 192.168.56.101
Host is up (0.00036s latency).
Not shown: 65519 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
111/tcp   open     rpcbind
1337/tcp  open     waste
2049/tcp  open     nfs
5432/tcp  open     postgresql
5821/tcp  filtered unknown
```

hydra

- a very fast network logon cracker for many different services
- Usage: $ nmap [Options] {target ip} {target service}
- Example:

$ hydra -L usernames.txt -P passwords.txt 10.1.33.7 ssh

- lots of noise (trying every possible username/password combination from given input lists), but lots of times it works

netcat

- nc - TCP/IP swiss army knife
- Usage:

$ nc [options] {ip address} {port(s)} # to connect

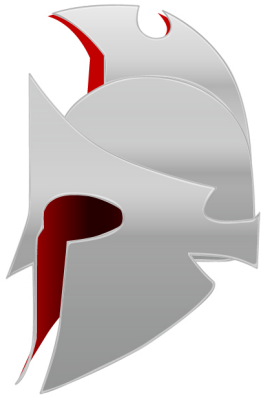
$ nc -l [options] {port(s)} # to listen on given port

- Example:

$ nc 10.1.33.7 42 # will connect to host 10.1.33.7 on port 42

$ nc -vl 1337 # starts listening for connections on port 1337

More tools



SPARTA

Network Infrastructure Penetration Testing Tool

- sqlmap
- sparta
- metasploit / armitage
- burpsuit
- wireshark
- and many more…

KALI LINUX™

"the quieter you become, the more you are able to hear"

Defense

- Ensure that your users have strong password
- Check for unnecessary running services
- Check for unnecessary active users
- Update OS and software
- Fire up Firewall
- Strike faster than your enemy

User Management

- Enabled root user is a bad idea, use sudo instead
- **$ sudo passwd -u / -l user** # enable / disable user
- **$ cut -d: -f1 /etc/passwd** # list of all users
- **$ sudo adduser / deluser** # add / remove user

Firewall

- **$ sudo ufw status** # get current status of firewall
- **$ sudo ufw enable** # enable firewall
- **$ sudo ufw default deny incoming** # deny all incoming traffic
- **$ sudo ufw allow 22** # allow tcp connections on port 22
- **$ sudo ufw reload** # reload firewall
- **$ sudo ufw reset** # reset to default rules

FIGHT

YOU HAVE 10 MINUTES TO SECURE YOUR DEFENSE SERVER

ANY ATTACK DURING THIS TIME IS STRICTLY FORBIDDEN

EVERY 12 MINUTES NEW HINT APPEARS

”Invincibility lies in the defence; the possibility of victory in the attack.”

- Sun Tzu

Hints

- what is running on port 1337?

Hints

- what is running on port 1337? # “tiny webserver in C”
- **$ hydra -l smith -P 100_worst_passwords.txt <target ip> ssh**

Hints

- what is running on port 1337? # “tiny webserver in C”
- **$ hydra -l smith -P 100_worst_passwords.txt <target ip> ssh**
- **$ psql -h <target ip> -u postgres** # then crackstation.net

Hints

- what is running on port 1337? # “tiny webserver in C”
- **$ hydra -l smith -P 100_worst_passwords.txt <target ip> ssh**
- **$ psql -h <target ip> -u postgres** # then crackstation.net
- both teams have same defense server

Hints

- what is running on port 1337? # “tiny webserver in C”
- **$ hydra -l smith -P 100_worst_passwords.txt <target ip> ssh**
- **$ psql -h <target ip> -u postgres** # then crackstation.net
- both teams have same defense server
- have you tried connecting to target ip in browser?

SURVEY

http://bit.ly/2npHX9n

Q&A

https://www.vulnhub.com	# free CTF games
https://news.ycombinator.com	# hacker news
https://www.wikileaks.org	# lots of useful info:)
https://crackstation.net	# free hash cracker
https://apsdehal.in/awesome-ctf/	# info about CTF games