Attacking the intentionally vulnerable

BSIDES VANCOUVER 2018

Whoami

@ABATCHY17 / WWW.ABATCHY.COM

Workshop goals

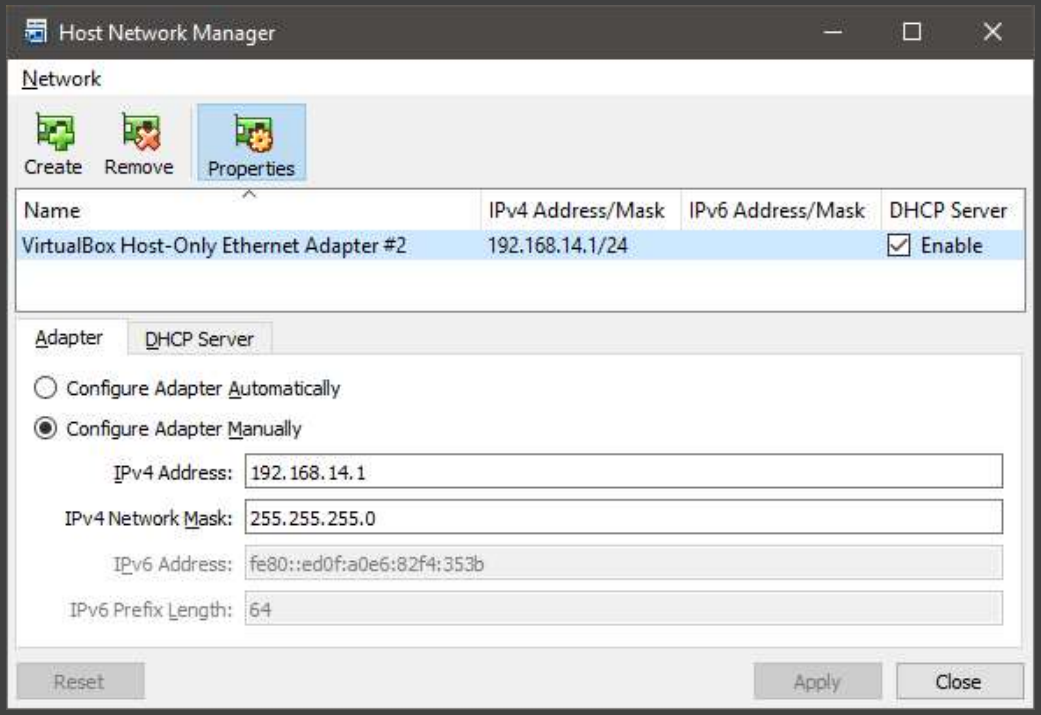
WTF IS BOOT2ROOT?

before we start..

- This workshop is for educational purposes only.
- DO NOT attack targets without getting permission first.
- Talk is not affiliated with/sponsored by employer.
- Please help each other ☺

is the environment properly set up?

1. Install VirtualBox
2. File -> Host Network Manager
   - Create && Enable DHCP
3. Load Kali & Bsides-VM OVA
4. Settings -> Network
   - Host-only adapter
5. Kali: **root/toor**



pitfalls

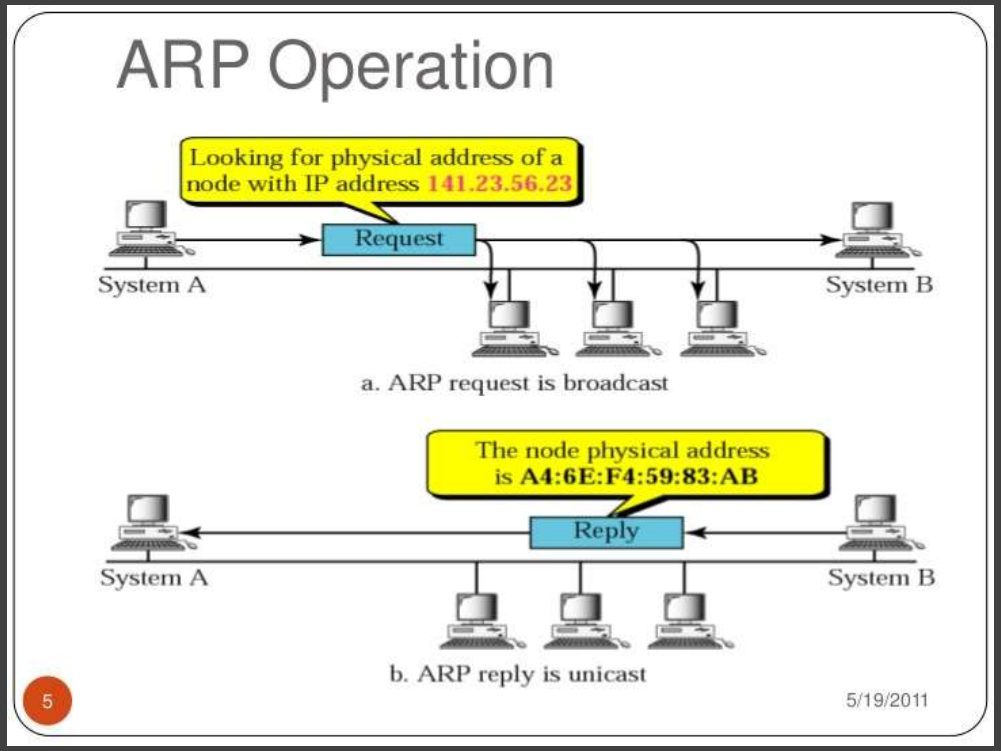
- Am I asking the right question?
- Document everything, they might be useful later!
  - OneNote, EverNote, …
- Tools don’t provide answers, they provide information.
- Enumeration is key
- “I’m stuck!”
  - It’s a learning curve, don’t give up yet!
  - Manpages
  - Google it!

host discovery - ICMP

- Echo request -> echo reply
- Q: Do targets have to respond?
- Tools: ping/fping/hping3/nmap/…

```
for i in $(seq 0 255); do ping -W 1 192.168.14.$i | grep
                    "64 bytes" ; done
```

host discovery - ARP



https://www.slideshare.net/tigerbt/arp-address-resolution-protocol

host discovery - ARP

Netdiscover:

```
netdiscover -r 192.168.14.0/24
```

arp-scan:

```
arp-scan 192.168.14.0/24
```

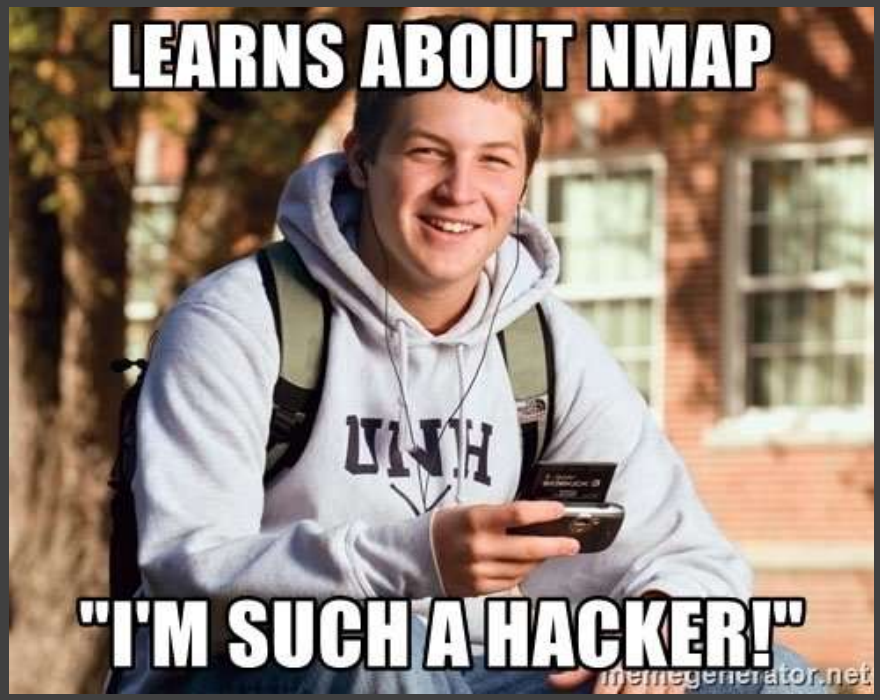
target enumeration

- What is the target’s role? OS?
- Identify services running through port scanning (What is a port?)
- TCP vs UDP

study case: nmap

Nmap is a

- Host discovery tool
- Port scanner
- Vulnerability scanner
- OS/version detection
- Scripting engine (NSE)



exercise 1: nmap

1. Perform a scan on all TCP ports

2. Perform an OS detection scan

3. Perform an intensive version detection scan

port scan pitfalls

- Heavy scan
  - False negatives
  - Service crash
  - Bandwidth overload
  - Getting caught
- Firewall
  - Is target really down?
  - Is service not running?
- IDS/WAF/fail2ban
  - Am I blacklisted?

web server enumeration

- Version detection
  - nmap –sV
- Vulnerability scanning
  - nikto
  - w3af
  - nmap scripts
  - …
- Web directory enumeration
  - dirsearch
  - dirb
  - dirbuster
  - nmap –script http-enum.nse
  - …

What problems can you run into?

exercise 2: web server

1. Run nikto on the server

2. Perform directory enumeration using one of the following:
   - dirb
   - dirbuster
   - nmap –script http-enum.nse
   - …

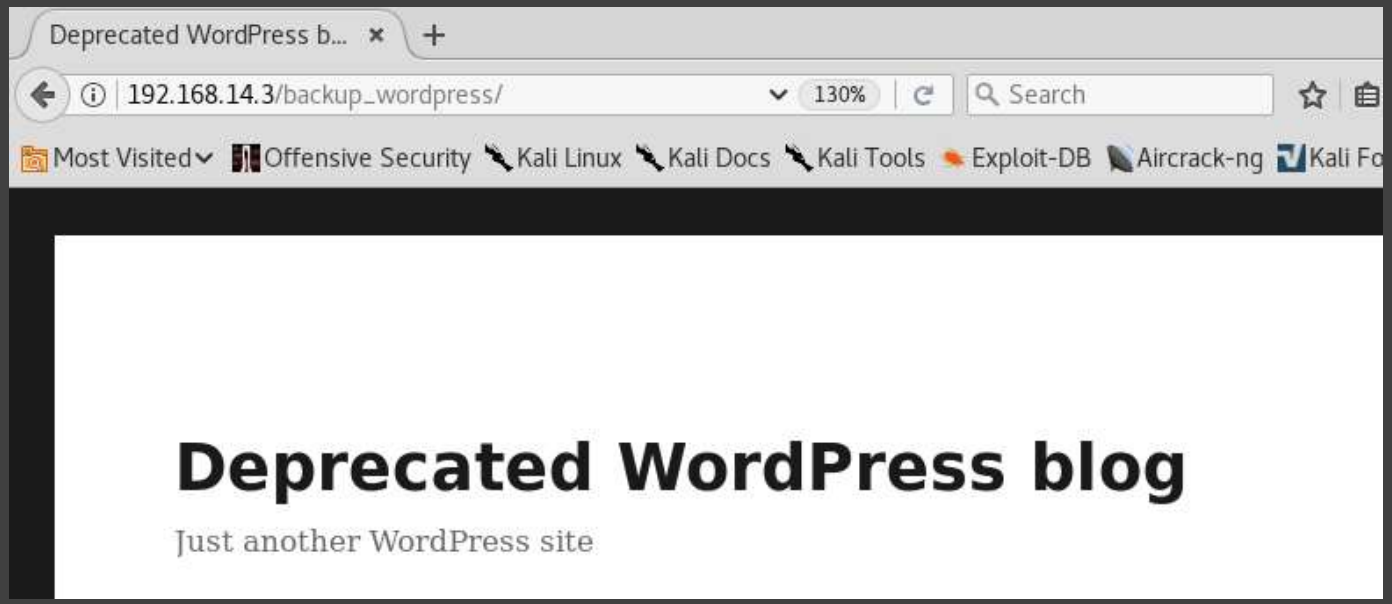
What did you find?

```
root@kali:~# dirb http://192.168.14.3

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar  7 04:08:16 2018
URL_BASE: http://192.168.14.3/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.14.3/ ----
+ http://192.168.14.3/cgi-bin/ (CODE:403|SIZE:288)
+ http://192.168.14.3/index (CODE:200|SIZE:177)
+ http://192.168.14.3/index.html (CODE:200|SIZE:177)
+ http://192.168.14.3/robots (CODE:200|SIZE:43)
+ http://192.168.14.3/robots.txt (CODE:200|SIZE:43)
+ http://192.168.14.3/server-status (CODE:403|SIZE:293)
```

Web server (2)

Web server (3)

```
root@kali:~# curl http://192.168.14.3/robots.txt
User-agent: *
Disallow: /backup_wordpress
```



Web server (4): Enumerating WP

- What information should we go after?
  - Wordpress version
  - Usernames
  - Plugins
  - Themes
  - Default setup files
  - …

Why is such data valuable?

study case: WPScan

- Vulnerability scanner just for WordPress!
- Version detection
- Users/plugins/themes enumeration
- Password bruteforcing

Exercise 3: wpscan

1. Scan the WP blog using wpscan
   - Identify the version
   - Find out the users

2. Bruteforce the password for users you found!

Enumerating with WPScan

```
root@kali:~# wpscan -u http://192.168.14.3/backup_wordpress --enumerate u
```

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
    +----+-------+------+
    | Id | Login | Name |
    +----+-------+------+
    | 1  | admin | admi |
    | 2  | john  | joh  |
    +----+-------+------+
```

Getting a shell

local enumeration

- What OS/kernel version?
- System information:
  - Host name
  - Network information
- User information:
  - Current user && permissions
  - /etc/passwd && /etc/shadow
- Services running and their versions
- Setuid binaries

…

Privilege escalation

Going the extra mile

Final notes

Enjoyed the workshop?

Vulnhub.com

- Tons of vulnerable VMs to play with.
- Check out Moria ;)

Wargames

- Ongoing challenges, usually divided into levels.
- Great practice for CTFs

Capture The Flag

- https://ctftime.org/ctf-wtf/