Win10 notes

Useful note: Resource Hacker decompiles exes

**IF YOU BREAK USER PERMISSIONS WITH TAKE OWNERSHIP, JUST MANUALLY ASSIGN YOURSELF FULL CONTROL AGAIN AND IT’LL BE OK**

**KEEP TRACK OF EVERYTHING**

SMTP: turn off the feature! bad! Server things! We hates it! We hates the Baggins!

Remote assistance off. GET IT OFFFFFFFFF

Run + Run Once at HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/. Delete keys but first delete what it calls

Filezilla security guide at wiki.filezilla-project.org/Securing\_your\_Windows\_Service\_installation

Internet properties → all high

On opening image, netstat -anob >> file.txt

ADVANCED AUDIT POLICY IS LEGAL

DOSKEY /macros will show any command aliases

Powershell get-alias

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\$name hides it in control panel; key will be a DWORD, value 1, called systemcomponent

Also:

**REMEMBER THE FUCKING README**

**NASTY THINGS THEY CAN DO**

* Cmd can be turned off in HKCU/SOFTWARE/Policies/Microsoft/Windows/CurrentVersion/System
* Run can be turned off in HKCU/ SOFTWARE/Microsoft/Windows/CurrentControlSet/Policies/Explorer/NoRun
* Right-clicking can be turned off in HKCU/ SOFTWARE/Microsoft/Windows/CurrentControlSet/Policies/Explorer/NoViewContextMenu
* All of these keys might be in HKLM too
* Turn off group policy:
  + Rename gpedit
  + Turn off the service in \System\CurrentControlSet\Services\gpservice\Start or services.msc\gpservice
  + HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\System\DisableGPO; set to 1 in order to turn off group policy

**ADDING A VM TO A DOMAIN**

* Hit “join a domain”
* Put in a domain name
* Go to >Network and Internet>Network connections (the same place where you turn off IPv4 and such) to statically assign your DNS to the DC’s IPv4 address
* Put in a username and password

**TROUBLESHOOTING DHCP**

* If it doesn’t start:
  + Look at its registry
  + Look at its service path
  + Write down other stuff I find
* If it does start:
  + Make sure allocation is set to automatic
    - Run ipconfig /renew after you set it
  + Look at /etc/hosts

**THE GOOSE**

* Task points to a batch file which opens a new goose every once in a while
* Goose living in a legit folder (in this case, IISStart) :(
* Registry key in Run pointing to IIS Start
  + LOOK IN HKLM AND HKCU
* Service that does something or other and looks evil
* Can commit genocide with esc for 30 secs

**gpsearch.azurewebsites.net**

* MSS (Legacy)
  + Contains a few legacy keys that are still relevant

**MSC SHORTCUTS**

- Local Group Policy is gpedit.msc

- Computer Management is compmgmt.msc

- Registry Editor is regedit

- Task Scheduler is taskschd.msc

- Command is cmd.exe

- If Run is off, you can use PowerShell or cmd to start any of these without the extension

**IF YOU CAN’T START A SERVICE**

-check that it’s not disabled  
-check that its path is correct  
-check that there’s not a bad key in its reg path (HKLM\System\CurrentControlSet\Services) that can fuck you over  
-Bad DependOnService can break it  
-ServiceSidType has a few values:

0: No specific security context

1: Own specific context

2: A more secure context  
-check the permissions in the key  
 -for dhcp specifically: give full control to NETWORK SERVICE and NT SERVICE\DHCP  
 -do the same for \TCPIP\NT SERVICE\DHCP

-lusrmgr.msc

TO TURN ON DHCP- Turn on WinHTTPAutoProxySvc and turn on full permissions in regedit

<https://winaero.com/reset-local-security-policy-settings-all-at-once-in-windows-10/>

the shares are at C$, IPC$, ADMIN$; delete all others

IPV6 BAD

Firewalls: public private domain

Control Panel > Network and Internet > Network and Sharing Center > $CONNECTIONNAME > Properties:

Leave on top three with gears, as well as IPV4

Turn off Microsoft LLDP, IPV6, LLTD Responder, LLTD Mapper I/O Driver, Microsoft Network Adapter Multiplexer Protocol

**INTERNET OPTIONS**

-Enhanced Protections ON

-Block all cookies

-All security levels HIGH

-Pop-up blocker high

-HTTP: Only use HTTP2

-Multimedia: Only first two (if you lose points for the others it don’t matter)

-Security: Enable first seven, Send Do Not Track request, use TLS 1.2, use SSL 3.0, last 3 on

NetBIOS over TCP/IP off bc netbios is legacy and we dislike old people

Look for bad dependencies in reg keys

LDAP runs on 389 to standardize authentication, but it’s unencrypted  
636 is encrypted

UAC: The point will be called “Guest account disabled in Admin Approval Mode”

**THREAT HUNTING**

* Firewall rule
  + Group-less rules are important to look at
  + Look for other anomalies

**FEATURES:**

- .NET Framework

- Work folders client

**APPS:**

* Either update or uninstall

**FIREFOX:**

* Pop-up blocker
* Tracking prot – strict
* HTTPS only
* Do not allow 3rd party cookies
* Auto updates + updates
* Auto-play off
* DNS over HTTPS
* Remove all exceptions
* Remove all saved things
* Block content, downloads, warn about software

**FTP:**

* Default port 13138
* Server listeners:
  + First should be 0.0.0.0, port 21
  + Second should be ::, port 21
  + Third should be loopback
  + All should be explicit FTP over TLS && insecure FTP
* Protocol settings:
  + Autoban on
    - 5 logins within 10 seconds
    - Lasts 300 seconds
  + Timeouts:
    - Login: 20 seconds
    - Activity: 60 minutes
* Rights management
  + Users:
    - General:
      * Use system user service is running under
      * Native path: :h
      * Virtual path: /
      * Add users as required
      * ADD PASSWORD
  + Set permissions through the actual file explorer permissions thing
* FTP over TLS:
  + Minimum allowed TLS 1.3 or newest
  + TLS cert:
    - Use self-signed X.509
    - Generate new
    - Applicable hostnames: localhost
* Administration:
  + Connection:
    - Local listening: 14148
    - Password on
    - Best to use same password as for users
  + Connection security:
    - Literally same thing as TLS cert rules
* Logging:
  + Logging level to 5
  + Log to file
  + Set filepath
    - Default: C:\Program Files\FileZilla Server\Logs\filezilla-server.log
  + File rotation on
  + Max log files: 5
  + Use max possible size
* Updates :
  + Once per week
  + Stable versions only
  + Perform a check

**SHARES:**

* C$
* admin$
* IPC$
* To open from run, fsmgmt.msc
* Also in computer management

**WHEN MOPPING UP POINTS**

* Look in Windows Security Settings > Virus and Threat Protection > Manage Settings > Exclusions
* Try AAP
* Control Panel → System and Security → System → Advanced System Settings → Advanced → Performance
* App and Browser Control → Exploit Protection: All should be default
* Program exception integrity chain on in Windows Defender
* If there is hmailserver
  + Mail is stored at
  + C:\Program Files (x86)\hmailserer\data\
    - Round 4 in 2024 it was in afa.com

**THUNDERBIRD**

* Mostly common sense
* Allow antivirus to auto-quarantine
* Do not proxy DNS when using SOCKSv5

**FORENSICS**

* HASH:
  + certutil -hashfile C:\...\file.exe –[type] (CMD)
  + get-filehash C:\...\file.exe /algorithm [HASHTYPE] (POWERSHELL)
  + websites
* File path
  + Click search bar in file explorer
  + Drag into notepad, cmd
  + Right-click, copy filepath
* Shares
* Google [sth]
* Use ChatGPT
* System name
  + System → About
* Decrypt [sth]
  + Rumkin
  + CyberChef
  + dCode.fr
  + base64decode.org
* File owner
  + Properties → Details
* Current events
* App version
  + Powershell cmd
  + Help w/in app
  + Control panel → programs
* User info
  + Commnds
    - net user
    - net local user $username
* Ports (not usually round 1)
* Event Viewer (only usually later rounds if they pwn event log)
* Ciphers from Ben’s Forensics
  + Periodic Table: Looks like numbers, letters
  + Malespin cipher, looks like text
  + Braille
  + DNA sequence
  + The Cursed Forensics 3
    - Beaufort: Needs a KEY and an ALPHABET
    - he had a fucking picture of keys wtf benjamin

**CONTROL PANEL**

Turn off autoplay

**IIS**

MAKE SURE that you have the manager as well

Backup inetpub

Turn on:

* Common HTTP features
* SSL Cert off
* There’s a best practices guide in the share
* Directory Browsing off

HTTPS-ing:

* Don’t ye use the default one, lass, for that’s where the ghosties lie
* Make a self-signed certificate
* Go to bindings
* Add new HTTPS type
* Delete HTTP

Logfiles:

-Max size = 1 and 8 0s

Make sure the phys path is C:\inetpub\wwwroot

Main > Feature Delegation:

-SSL Settinsg read only

-Logging read only

SSL Settings:

-Require SSL

-Accept

**PORTS**

3389: RDP

43: whois (dns lookup); dig is linux’s alternative

53: DNS

123: NTP

67, 68: DHCP

23: Telnet

1900: SSDP

7: Echo

13: Daytime

17: Quote of the Day

19: Character generator

88: Kerberos

25: SMTP

22: SSH

81: Apache management

139:

445: SMB

20, 21: FTP

69: TFTP

1306: SQL server

25565: Minecraft server

5800/5900: VNC

6667: IRC

389: LDAP

636: LDAPS

3478/3841: MS Teams

990: FTPS

**IMAGE NOTES**

BEN ROUND 4 PRACTICE 2024

Default Browser: FireFox

Update Chrome, 7-zip, puTTY, BitTorrent Classic

FileZilla should be secured

Authorized FTP users:

Hsolo

Lskywalker

Yoda

Kren

Run OpenSSH server; same users as FTP

Create group called “auth users” with those users

Death Star Plans is only authorized share

Only admins may access

Secure OpenSSH

Add to the domain

Services: OpenSSH Server, FileZilla Server

Checklist

1. Increase RAM and Processors Cores
2. Do your baselines!
   1. cd Desktop
   2. netstat -anob > netstat-omron.txt
   3. get -process > process-omron.txt
3. Go to Windows Update and start downloading updates
4. Forensics
   1. Take notes on what you got right and wrong in anything that is not in the VM
5. Update and delete wanted/unwanted software (Update Windows later)
6. Control Panel
   1. UAC
   2. Firewall Configuration
   3. RDP
   4. RDS
7. Do password Policy in group policy
   1. Group Policy
   2. Computer config
   3. Windows settings
   4. Security Settings
8. Audits
9. Do users in Comp Management
10. Threat Hunting in task manager, Malwarebytes, defender
11. Servers and Required Services (if any)- Read Me
12. Benchmarks
13. Check User Files
14. Look For Backdoors
    1. Task manager
    2. Command prompt using netstat -ano
    3. Compare all the PIDs in command prompt to the tasks in task manager
15. Registry Editor