



- |     |   |                      |
|-----|---|----------------------|
| 1.  | <b>What syntax do PowerShell cmdlets follow?</b>  | verb-noun            |
| 2.  | <b>What PS command will list all PowerShell cmdlets?</b>  | get-command          |
| 3.  | <b>What PowerShell command will list all verbs?</b>   | get-verb             |
| 4.  | <b>BASH commands output strings. PowerShell commands output what data type?</b>   | objects              |
| 5.  | <b>All PowerShell objects are comprised of what two things?</b><br>Flag format: things,things                                       | methods, properties  |
| 6.  | <b>What command will list all things that make up a PowerShell object?</b>  | get-member           |
| 7.  | <b>What PowerShell command will list PowerShell aliases?</b>  | get-alias            |
| 8.  | <b>What PowerShell command lists all of the contents of a directory?</b>  | get-childitem        |
| 9.  | <b>What is the basic cmdlet that displays help about Windows Powershell cmdlets and concepts?</b>                                   | get-help             |
| 10. | <b>PowerShell "help files" don't show the entire help file with a basic command. What switch option shows the entire help file?</b> | -full                |
| 11. | <b>What PowerShell command will update the PowerShell "help files" to the latest version?</b>                                       | update-help          |
| 12. | <b>What help switch will show you the "help files" on Microsoft's website, in your default browser?</b>                             | -online              |
| 13. | <b>What command will start the Chrome browser on your machine?</b>  | start-process Chrome |
| 14. |   |                      |



## OS PE's

Study online at [https://quizlet.com/\\_byrzbz](https://quizlet.com/_byrzbz)

	<b>What command using a PS Method will stop chrome?</b> <b>Flag is the full command.</b>	<code>(get-process chrome).kil()</code>
15.	<b>What PowerShell command (without using a method) will stop the Chrome process?</b>	<code>Stop-process -Name Chrome</code>
16.	<b>PowerShell doesn't have a native cmdlet that will give you processor information (such as <code>get-processor</code> or <code>get-cpu</code>). Knowing this information might be necessary. What command would give you information about the system's processor?</b>	<code>get-WmiObject Win32_Processor</code>
17.	<b>What PowerShell command will read a text file?</b>	<code>get-content</code>
18.	<b>What PowerShell command will allow for counting lines in a file, averaging numbers, and summing numbers?</b>	<code>measure-object</code>
19.	<b>What PowerShell command searches for text patterns in a string?</b>	<code>select-string</code>
20.	<b>Users' files are stored in their corresponding home directory. What is the literal path to all home directories on a Windows 10 system?</b>	<code>C:\Users\student</code> <code>echo \$HOME</code>
21.	<b>How many properties are available for the <code>get-process</code> cmdlet?</b>	52 <code>get-process   get-member -MemberType Property</code>
22.	<b>How many aliases does PowerShell have for listing the contents of a directory?</b>	3
23.	<b>When requesting the help file for the <code>get-process</code> cmdlet, what full command is the 9th example given?</b>	<code>get-process power-shell</code>
24.		



**To complete this challenge, find the description of the Lego Land service.**

i\_love\_legos  
get-wmiobject  
win32\_service |  
select  
Name,Description

- |   |  |
|---|--|
| 25. In the CTF folder on the CTF User's Desktop, count the number of words in words2.txt.   | 5254<br>cd into<br>cd Users\CTF\Desktop\CTF<br>Get-Content<br>words2.txt  <br>measure-object -word |
| 26. Count the number of files in the Videos folder in the CTF user's home directory.  | 925<br>(ls).count  |
| 27. Find the only line that makes the two files in the CTF user's Downloads folder different.<br>Hint The flag is the string (not line number).                                     | popeye<br>compare-object<br>(get-content new.txt)<br>(Get-Content old.txt)                         |
| 28. The password is the 21st line from the top, in ASCII alphabetically-sorted, descending order of the words.txt file.<br>Note: File location is CTF user's Desktop in CTF folder. | ZzZp<br>get-content words.txt  <br>sort -Descending   se-<br>lect -skip 20 -first 1                |
| 29. Count the number of unique words in words.txt, found on the CTF user's desktop, in the CTF folder.  | 456976<br>(get-content words.txt<br>  sort -unique).count  |
| 30. How many methods are available for the get-process cmdlet?  | 19<br>get-process  <br>get-member -Mem-<br>berType Method  |
| 31. Count the number of folders in the Music folder in the CTF user's profile.  | 411<br>(ls).count  |



- 
- |  |  |
|--|--|
| 32. <b>Count the number of times, case-insensitive, gaab is listed in words.txt in the CTF folder on the CTF user's desktop.</b> | 1<br>(get-content words.txt   findstr -i gaab).count |
|--|--|
- 
- |   |  |
|---|--|
| 33. <b>Count the number of words, case-insensitive, with either a or z in a word, in the words.txt file on the CTF user's desktop.<br/>Hint: There are multiple "words" on each line.</b> | 160352<br>(get-content words.txt   findstr -i [a,z]).count |
|---|--|
- 
- |  |   |
|--|---|
| 34. <b>Count the number of times az appears in the words.txt file on the CTF user's desktop.</b> | 2754<br>(get-content words.txt   findstr -i az).count |
|--|---|
- 
- |  |   |
|--|---|
| 35. <b>Use a PowerShell loop to unzip the Omega file 1,000 times and read what is inside.<br/>Note: Make sure you back up the .zip file to a different directory before attempting this challenge.</b> | kung-fu<br>foreach (\$i in 1000..1) {<br>>> Get-ChildItem<br>.\Omega\$i.zip -ErrorAction SilentlyContinue   Expand-Archive -DestinationPath. -ErrorAction SilentlyContinue }<br>- look at last file -<br>Expand-Archive<br>.\Omega1.zip<br>- keep expanding<br>archive until you get to<br>Omega1.txt file<br>cat .\Omega1\ |
|--|---|
- 
- |   |  |
|---|--|
| 36. <b>On the CTF user's desktop, count the number of words in words.txt that meet the following criteria:<br/>a appears at least twice consecutively<br/>and is followed immediately by any of the letters a through g<br/>Example: aac...aaa...</b> | 357<br>(get-content words.txt   select-string 'a{2}[a-g]').count |
|---|--|
- 
- |  |                            |
|--|----------------------------|
| 37. <b>Which PowerShell profile has the lowest precedence?</b> | current user, current host |
|--|----------------------------|
-



- 
38. Which PowerShell profile has the highest precedence? all users, all hosts
- 
39. Which PowerShell variable stores the current user's home directory? \$Home
- 
40. Which PowerShell variable stores the installation directory for PowerShell? \$PsHome
- 
41. Which PowerShell variable stores the path to the "Current User, Current Host" profile? \$PROFILE
- 
42. What command would you run to view the help for PowerShell Profiles? get-help about\_Profiles
- 
43. What command would tell you if there was a profile loaded for All Users All Hosts? Test-Path -Path \$profile.AllUsersAllHosts
- 
44. Malware is running in a PowerShell profile on the File-Server. Based on PowerShell profile order of precedence (what is read first), find the correct flag. I am definitely not the malware  
gc  
C:\Windows\System32\WindowsPowerShell\v1.0\profile.ps1
- 
45. What command lists the contents of directories in Linux/Unix systems? ls
- 
46. For the ls command, what arguments, or switch options, will allow you to print human-readable file sizes in a long-list format? ls -lh
- 
47. What character will pipe the standard output from | echo "I'm a plumber" to another command, as standard input?
- 
48. man -k



**What argument/switch option, when used with man, will search the short descriptions and man-page-names for a keyword that you provide?**

49. **What is the absolute path to the root directory?** /

50. **What is the absolute path to the default location for configuration files?** /etc

51. **What is the directory that contains executable programs (binaries) which are needed in single user mode, to bring the system up or to repair it?** /bin

52. **What is the absolute path to the directory which contains non-essential binaries that are accessible by standard users as well as root?** /usr/bin

53. **An absolute path to a directory which contains binaries only accessible by the root user, or users in the root group.** /sbin

54. **What is the absolute path for the binary cat man-page?** /usr/share/man/man1/cat.1

55. **Search the man pages for the keyword digest. Then, use one of the binaries listed to hash the string OneWayBestWay using the largest sha hash available.** a81bc463469ee1717fc9e  
echo OneWayBestWay | sha512sum

56. **Use File: /home/garviel/Encrypted This file contains encrypted contents. Identify its file type, then decode its contents.** DeCrypt  
- garviel@terra:~\$ openssl aes-128-cbc -d -in cipher -out cipherold -kfile symmetric  
- cat cipher  
- symmetric is the file with the key

57.



- 
- Search the user home directories to find the file with the second-most lines in it. Hint: Exclude the VDI file! The flag is the number of lines in the file.**
- 20000 ./-  
garviel/conn.log  
- garviel@terra:~\$ find  
. -type f -exec wc -l {} \;  
| sort -rn
- 
58. **Read the file that contains the user database for the machine. Identify a strange comment.**
- Traitor  
garviel@terra:/etc\$  
cat passwd | cut -d ':'  
-f 5
- 
59. **Identify all members of the Lodge group. List their names in alphabetical order with a comma in between each name.  
Flag Format: name,name,name**
- aximand,ere-  
bus,ezekyle,garviel,sejanu  
garviel@ter-  
ra:/home\$ cat  
/etc/group | sort
- 
60. **Find the user with a unique login shell.**
- nobody  
- garviel@terra:~\$ cat  
/etc/passwd | awk -F  
":" '{print\$7}' | sort -u  
- cat /etc/passwd |  
grep "sh"  
- look for unique login  
names
- 
61. **Identify the algorithm, the amount of salted characters added, and the length of the hashed password in the file that stores passwords.  
Hint: Research 'padding'...  
Flag format: algorithm,#characters,#length  
sudo cat /etc/shadow | cut -d ':' -f 2 | sort**
- 
62. **Find the directory named Bibliotheca. Enter the absolute path to the directory.**
- /media/Bibliotheca
- 
63. **Identify the number of users with valid login shells, who can list the contents of the Bibliotheca directory.**
- 15  
(18-3)  
cat /etc/passwd | grep  
-v nologin | wc



- 
64. **The permissions that user sejanus has on /media/Bibliotheca, in octal format.**  
**Flag format: #**  
**HINT: Think about groups...**  
**cat /etc/group | grep -e 'sejanus'**
- 5 = (r-x)  
- to find group of sejanus run "cat /etc/group | grep sejanus"  
- ls -lisa /media for group permissions
- 
65. **Locate the file within /media/Bibliotheca that is modifiable by the only user that is part of the Chapter group, but not part of the Lodge group.**  
**Hint: Not the hidden file...**
- Codex\_Astartes  
-garviel@terra:/media/Bibliotheca\$ ls  
-lisa  
Bibliotheca\_unus/  
- looking for file that only is user modifiable  
- -rw-r-----
- 
66. **Identify the file within /media/Bibliotheca where the owning group has more rights than the owning user.**
- Codex\_Hereticus  
- garviel@terra:/media/Bibliotheca\$ ls  
-lisa Bibliotheca\_tribus/  
- look for file that owning group has permissions - -r----xrwX
- 
67. **Execute the file owned by the guardsmen group in /media/Bibliotheca, as the owning user.**  
**The flag is the code name provided after a successful access attempt.**
- 
68. **The user tyborc is unable to access the directory: /media/Bibliotheca/Bibliotheca\_unus**  
**Why? Identify the permission missing in standard verb form.**
- execute  
- ls -l  
- what permission do you need to modify things 'execute'
- 
- 69.
- /media/Bibliotheca/Bibliotheca-





**Locate the file in /media/Bibliotheca that Inquisitor Quixos has sole modification rights on. The flag is the absolute path for the file.**

ca\_duo/Codex\_Hereticus  
- ls -lisa Bibliotheca\_duo/  
Quixos has only right in B\_duo/C-Here

**70. Read the concealed file within /media/Bibliotheca**

Expand your mind  
- find . -type f -name '.\*'  
- cat  
./Bibliotheca\_duo/.Secrets\_of\_the\_Immatium

**71. Find the warp and read its secrets for the flag.**

Ph'nglui mglw'nafh Cthulhu  
- find . -type f -name '.\*'  
- cat  
./Bibliotheca\_duo/.warp2/.warp5/wa

**72. Using the commands ls and grep, identify the number of directories in /etc/ that end in .d**

27  
ls | grep -e \*.d

**73. File: home/garviel/numbers**  
**Use regular expressions to match patterns similar to an IP address.**  
**The answer is the count/number of lines that match in the file.**

78  
- garviel@terra:~\$ cat numbers | grep -E  
'^([0-9]{1,3}\.){3}[0-9]{1,3}\$'

**74. File: home/garviel/numbers**  
**Use regular expressions to match valid IP addresses. The flag is the number of addresses.**  
**HINT: What are the valid numerical values of each octet in an IP address?**

18  
- cat numbers | grep -Eo  
"^(25[0-5]|2[0-4][0-9]|[01]?"

**75. File: home/garviel/numbers**  
**Use regular expressions to match patterns that look similar to a MAC Address. Flag is a count of the number of matches.**

4877  
- cat numbers | grep -E  
'^..\-..\-..\-..\-..\\$' | wc -l



**HINT: This is a loose match! Some of these results won't be true MAC addresses.**

**Flag format: ####**

- 
76. **File: home/garviel/numbers**  
**Use awk to print lines:**  
**>= 420 AND <=1337**  
**The flag is a SHA512 hash of the output.**
- e62ff70d772ef0977f4f8fe1  
- cat numbers | awk  
'NR >= 420 && NR  
<=1337 {print\$1}' |  
sha512sum
- 
77. **File: home/garviel/connections**  
**Use awk to create a separate CSV (comma separated value) file that contains columns 1-6.**  
**The flag is an MD5 hash of the new file**  
**Hint: Look at #fields on line 6 in the file to understand column layout.**  
**Hint: This is a Zeek (formally known as Bro) connection log file in TSV format. Click This Link to learn about its formatting.**  
**Sample Output**
- cat connections | awk  
' {print \$1, \$2, \$3, \$4,  
\$5, \$6}' OFS="," con-  
nections > outfile  
- chmod 777 outfile  
- md5sum outfile
- 
78. **Directory: home/garviel/Battlefield/**  
**The garviel user has a minefield map and controls to a Titan War Machine located in their home directory. Interpret the Titan Controls to navigate the minefield and annihilate the target.**  
**Enter the correct movement codes to make the Titan obliterate the target.**
- AAAAA3AAA3AAAABAAE  
- cat minefield\_map  
- nano minefield map  
- save and chmod 777
- 
79. **The flag resides in \$HOME/paths... you just need to determine which flag it is. The flag sits next to a string matching the name of a \$PATH/binary on your system.**  
**Hint: The correct binary is not echo**
- cat paths | awk  
'NR==FNR{a[\$1,\$1];next}
- 
80. **File: home/garviel/numbers**  
**Use regular expressions to find Locally Administered or Universally Administered Unicast MAC addresses.**  
**Give the count of Locally and Universally Admin-**
- 178  
- cat numbers | egrep  
'^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})\$'  
-



**istered MAC addresses as the answer.**

**HINT: What characters specifically define a Locally or Universally Administered Unicast MAC Address?**

- 
81. **FILE: /home/garviel/Inquisition\_Targets**  
**Identify heresy by comparing the Inquisition\_Targets file to members of the Guardsmen group.**  
**HINT: Reformat and clean up the data before it is compared. awk and sort are your best friends!**  
**The flag is the number of heretics on the system.**
- 
82. **What registry hive contains all machine settings?** HKLM
- 
83. **What registry hive contains all user settings?** HKU
- 
84. **What registry hive contains only the currently logged-in user's settings?** HKCU
- 
85. **The HKEY\_CURRENT\_USER registry hive is a symbolic link to another registry subkey. What is the subkey that it is linked to?**  
**Flag format: HIVE\SID.** HKEY\_USERS\S-1-5-21-3
- 
86. **What PowerShell command will list all the subkeys and contents in the current directory and/or will list all the subkeys and the contents of a directory you specify?** get-childitem
- 
87. **What PowerShell command will list only the contents of a registry key or subkey?** get-item
- 
88. **What registry subkey runs every time the machine reboots? The flag is the full path, using PowerShell.** HKLM:\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- 
89. **What registry subkey runs every time a user logs on? The flag is the full path, using PowerShell.** HKCU\SOFTWARE\MI-



	CROSOFT\WIN-DOWS\CUR-RENTVERSION\RUN
90. <b>What registry subkey runs a single time, then deletes its value once the machine reboots? The flag is the full path, using PowerShell.</b>	HKLM:\SOFTWARE\MI-CROSOFT\WIN-DOWS\CUR-RENTVER-SION\RUNONCE
91. <b>What registry subkey runs a single time, then deletes its value when a user logs on? The flag is the full path, using PowerShell.</b>	HKCU\SOFTWARE\MI-CROSOFT\WIN-DOWS\CUR-RENTVER-SION\RUNONCE
92. <b>What is the value inside of the registry subkey from your previous challenge named registry_basics_7?</b>	C:\malware.exe get-itemproperty 'HKLM:\SOFTWARE\MI-CROSOFT\WIN-DOWS\CUR-RENTVER-SION\RUN'
93. <b>What is the value inside of the registry subkey that loads every time the "Student" user logs on?</b>	C:\botnet.exe - Get-Item 'REG-ISTRY::HKEY_USERS\*\S
94. <b>What is the value inside of the registry subkey from registry_basics_9?</b>	C:\virus.exe get-itemproperty 'HKLM:\SYSTEM\CURRENTCONTROLSET\ENUMUSBSTOR'
95.	



<b>What is the value inside of the registry subkey that loads a single time when the "student" user logs on?</b>	C:\worm.exe - Get-Item 'REG- ISTRY::HKEY_USERS\*\S
<b>96. Figure out the manufacturer's name of the only USB drive that was plugged into this machine.</b>	SanDisk9834 get-itemproperty 'HKLM:\SYS- TEM\CURRENTCON- TROLSET\ENUMUS- BSTOR'
<b>97. What suspicious user profile, found in the registry, has connected to this machine?</b>	Hacker_McHackerson get-childitem 'HKLM:\Software\Mi- crosoft\Windows NT\CurrentVer- sion\ProfileList'
<b>98. What suspicious wireless network, found in the registry, has this system connected to?</b>	Terror_cafe_network get-childitem 'HKLM:\Software\Mi- crosoft\Windows NT\CurrentVer- sion\Networklist\Pro- files'
<b>99. Every file on a Windows system has attributes. What does the d attribute mean?</b>	Directory
<b>100. Every file on a Windows system has attributes. What does the h attribute mean?</b>	hidden
<b>101. What PowerShell command will list all files in the current directory, regardless of their attributes?</b>	get-childitem -force
<b>102. What PowerShell command will give you the sha512 hash of a file?</b>	get-filehash -algo- rithm sha512
<b>103.</b>	get-acl



## What PowerShell command will list permissions of a file?

- |   |   |
|---|---|
| 104. What Windows file maps hostnames to IP addresses?  | hosts   |
| 105. Which group has ReadandExecute (RX) permissions to the file listed in the previous challenge, File_System_Basics_6?<br>get-acl hosts   format-list           | BUILTIN\Users<br>C:\Windows\System32\drivers\etc><br>(get-acl<br>.\hosts).Access                  |
| 106. Find the last five characters of the MD5 hash of the hosts file.   | 7566D<br>get-filehash hosts -algorithm md5  |
| 107. Examine the readme file somewhere in the CTF user's home directory.  | 123456<br>C:\Users\CTF\Favorites> cat<br>.\README   |
| 108. There is a hidden directory in the CTF user's home directory. The directory contains a file. Read the file.  | ketchup<br>C:\Users\CTF><br>get-childitem -path<br>[rs]* -force<br>cd secretsauce<br>cat .\saucey |
| 109. Find a file in a directory on the desktop with spaces in it.<br>HINT: If you like to type the full names and paths of files, you better look for a shortcut. | 987654321<br>C:\Users\CTF\Desktop\z<br>cat .\spaces.txt   |
| 110. Find the Alternate Data Stream in the CTF user's home, and read it.  | P455W0RD<br>-go to cmd<br>-andy.dwyer@FILE-SERV<br>-andy.dwyer@FILE-SERV                          |
| 111. "Fortune cookies" have been left around the system so that you won't find the hidden password...   | fortune_cookie<br>-get out of PS with   |



<b>Get-childItem *Fortune* -force -Recurse -erroraction silentlycontinue</b>	"cmd" - use "dir /R" - more < "insert file name" - DONT FORGET go back to PS
<b>112. There are plenty of phish in the C:\, but sometimes they're hidden in plain site. Find the phish.</b>	phi5hy C:\Users\CTF\Documents\WWW> gci -force -verbose -Recurse
<b>113. What is the first process to spawn on Windows systems after the kernel loads?</b>	system
<b>114. What is the Process ID (PID) of the first Windows process?</b>	4
<b>115. What is the second boot process to spawn, that then spawns csrss in both session 0 and session 1?</b>	smss - session manager subsystems
<b>116. What session ID does Windows services operate in?</b>	0
<b>117. What process creates access tokens?</b>	lsass - local security Authority Subsystem
<b>118. What is the parent process to all svchosts?</b>	services
<b>119. What process is waiting with high priority for the Secure Attention Sequence (SAS)?</b>	winlogon
<b>120. What user space process spawns explorer, then dies?</b>	userinit
<b>121. What is the name of the bootloader we are using on all of the Windows machines in this environment?</b>	winload.exe bcdedit /enum



- 
122. **Based on the boot loader from Init\_9, which firmware are we using (BIOS or UEFI) in our environment?**
- BIOS  
The path will show as winload. efi if its EFI and winload.exe if its native BIOS. We can also get the same from under 'Windows Boot Loader', if the path is  
'\Windows\system32\winload.exe' then it is native BIOS mode, and if the path is  
'\Windows\system32\winload. efi' then it is EFI.
- 
123. **What file saves the memory state to the hard drive when going into hibernation?**
- hiberfil.sys  
bcdedit /enum all  
Resume from Hibernation  
filepath
- 
124. **What bootloader is responsible for restoring the system to its original state after hibernation?**
- Winresume.exe
- 
125. **The system is booting into safe mode. Identify the flag from the command-line output.**
- 
126. **Solve the following equation:  
0x31A - 0x21B  
Enter the flag in Hexadecimal form.**
- 0xFF  
- bombadil@minas-tirith:~\$ echo \$((0x31A - 0x21B))  
255  
- bombadil@minas-tirith:~\$ printf '%x\n' 255  
FF





	or - bombadil@mi-nas-tirith:~\$ printf '%x\n' \$((0x31A - 0x21B))
127. How many bits are in a nibble, and a byte?	4,8
128. How many bits does a single Hexadecimal character represent?	4
129. Each hex digit contains a value of 8 bits when used to represent memory. How many bytes could the range 0x00000000 - 0x00000010 contain?	17
130. How large is the Master Boot Record and what directory is it located in? Flag format: #lnBytes,directory	512,/dev
131. Identify which of your Linux machines is using SysV Initialization.	Minas_Tirith cat /etc/inittab
132. What are the maximum and minimum value a single Hexadecimal digit can contain? Enter the values in Linux Hexadecimal Numerical Constant form. Flag format: min-max	0x0-0xF
133. What are the maximum and minimum values, in decimal notation, that a single Hexadecimal digit can represent? Flag format: min-max	0-15
134. Solve the following equation: 0x31A + 0x43 Enter the flag in Hexadecimal form.	0x35d - printf '%x\n' \$((0x31A + 0x43))
135. Execute : sudo cat /dev/vda   xxd -l 32 -c 0x10 -g 1 What are the values contained in hex positions	63,90,8-e,d0,31,e4,8e,d8



**0x00000001 through 0x00000008?**

**Flag format: Value,Value,Value**

- 
136. **Identify the Linux Kernel being loaded by the Grub, by examining its configuration. Enter the command used by the Grub, and the full path to the Kernel, as the flag. Flag Format: command,kernel location**
- linux,/boot/vmlinuz-4.9.0-12-amd64
- 
137. **Locate the master boot record for one of the Linux assembly machines and read it with xxd What programming language is the MBR written in? HINT: Look at the first three bytes**
- 
138. **The file /home/bombadil/mbroken is a copy of an MBR from another machine. Hash the first partition of the file using md5sum. The flag is the hash.**
- 2-  
a5948fad4ec68170b23faa  
- dd if=mbro-  
ken of=MBRcopy  
skip=446 bs=1  
count=16  
- this breaks down to  
first partition  
- md5sum MBRcopy
- 
139. **The file /home/bombadil/mbroken is a copy of an MBR from another machine. You will find the "word" GRUB in the output, hash using md5sum. The flag is the entire hash.**
- 5-  
fa690cb0f0789cbc57decf  
- echo -n GRUB |  
md5sum
- 
140. **The file /home/bombadil/mbroken is a copy of an MBR from another machine. Hash only the Bootstrap section of the MBR using md5sum. The flag is the entire hash.**
- d59a68c7b6d62ecaa1376  
- dd if=mbroken  
of=MBRcopy skip=0  
bs=1 count=446  
- md5sum MBRcopy
- 
141. **Identity the default run level on the SysV Init Linux machine.**
- 2  
-  
bombadil@mi-



	nas-tirith:/etc/rc3.d\$ who -r - queries run levels
142. What is the last script to run when the command init 6 is executed?	/etc/init.d/reboot - Reboot is run level 6, look in FG
143. What run levels start the daemon that allows remote connections over port 22?	2,3,4,5 - port 22 - ssh - /etc/init.d - cat ssh - Default-Start: 2 3 4 5 = run levels
144. Identify the file symbolically-linked to init on the SystemD init machine.	/lib/systemd/systemd - cd /sbin - ls -l looks like this - init -> /lib/systemd/systemd
145. What is the default target on the SystemD machine and where is it actually located?	graphical.target, /lib/systemd/system- graphical.target
146. What unit does the graphical.target want to start, based solely on its configuration file? HINT: Targets deal with which init system? Which machine should you be looking for this flag, on?	display-manager.service - cat graphical.target - Wants=display-manager.service
147. What dependency to graphical.target will stop it from executing if it fails to start, based solely on its static configuration file?	multi-user.target - cat graphical.target - Requires=multi-user.target
148. How many wants dependencies does SystemD actually recognize for the default.target HINT: Use the systemctl command with some arguments to make life easier.	7 - cat graphical.target - Documenta-



tion=man:sys-  
temd.special(7)

149. What is the full path to the binary used for standard message logging?

150. What Sysinternals tool is used to investigate processes? procexp.exe

151. What Sysinternals tool shows malware persistence locations in tabs within its GUI? autoruns.exe

152. What is the full path to the binary used for standard message logging?  
HINT: Standard message logging is standardized across UNIX systems.

153. What Sysinternals tool can be used to investigate network connection attempts? tcpview.exe

154. What Sysinternals tool can view permissions? accesschk.exe

155. What Sysinternals tool allows us to view and modify handles? handle.exe

156. What is the default Windows user directory for files downloaded from the internet? The flag is the folder name only. downloads

157. What is the default Windows download directory that everyone has access to? The flag is the absolute path to the directory. C:\Users\Public\Downloads

158. What Sysinternals tool shows service load order? LoadOrder

159. What is the service name of Windows Defender Firewall? MpsSvc.exe

160. What SysInternals tool reports .dlls loaded into processes? ListDLLs



- 
161. **There is malware on the system that is named similarly to a legitimate Windows executable. There is a .dll in the folder that the malware runs from. The flag is the name of the .dll.**
- 
162. **You notice that there is an annoying pop up happening regularly. Investigate the process causing it. The flag is the name of the executable.**
- McAfeeFireTray.exe  
-use procexp.exe  
-wait for thing to popup  
and suspend
- 
163. **Determine what is sending out a SYN\_SENT message. The flag is the name of the executable. HINT: Use a Sysinternals tool.**
- 10.20.0.5 52085  
10.11.0.202 443  
SynSent Internet
- 
164. **Malware uses names of legit processes to obfuscate itself. Give the flag located in Kerberos' registry subkey. HINT: Use Sysinternals tools. Creds: Machine: Workstation1 (RDP from Admin-Station)login: studentpassword: password C:\Windows\srvany.exe**
- 
165. **There is malware named TotallyLegit. Find its binary location and there will be a file in that directory. Read the file.**
- 
166. **Find the McAfeeFireTray.exe. There is a file in that directory. The flag is inside.**
- StrongBad  
- used proexp to see  
randomn file popping  
up  
PS C:\Program  
Files\Windows De-  
fender Advanced  
Threat Protection> cat  
'.\It"s\_Here.txt'
- 
167. **What are the permissions for NT SERVICE\TrustedInstaller on spoolsv.exe? Copy the permissions from your shell.**



- 
168. What is the PATH listed in the output when we find the handle for spoolsv.exe?
- 
169. In what Load Order Group is the Windows Firewall service?  
6666  
networkprovider  
-use loadord.exe  
-look for mpssvc
- 
170. What is the first .dll associated with winlogon.exe? Provide the name of the .dll only, not the /absolute/path
- 
171. While examining the Windows Defender Firewall, what is the LogAllowedConnections setting set to, for the Public profile?
- 
172. A nonstandard port has been opened by possible malware on the system. Identify the port.  
6666  
C:\> Get-NetTCPConnection
- 
173. Determine what mechanism opened the port from hidden\_processes\_7. The flag is the name of the file.  
legit\_script.ps1  
-use tcpview  
-look for port 6666  
-then go to procexp  
-open all powershells  
-look for suspicious stuff
- 
174. Identify the flag from the file in hidden\_processes\_8.  
N0t\_L3g1T\_Am-miright  
C:\Windows\System32> cat  
.\legit\_script.ps1  
-use file path from procexp
- 
175. What Sysinternals tool will allow you to view a file's manifest?  
sigcheck
- 
176. asinvoker



**What is the RequestedExecutionLevel for an application to run with the same permissions as the process that started it?**

- |  |   |
|--|---|
| 177. What RequestedExecutionLevel will prompt the user for Administrator credentials if they're not a member of the Administrator's group?                               | requireAdministrator  |
| 178. What registry key holds UAC values?   | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System  |
| 179. The flag is the RequestedExecutionLevel of the schtasks.exe file.   | asinvoker<br>cat schtasks.exe<br>-look for requested-privileges   |
| 180. Determine which UAC subkey property shows whether UAC is enabled or not. The flag is the data value in that property.   | 4919<br>- The registry keys are found in<br>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System<br>- get-itemproperty<br>HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System<br>- EnableLUA : 4919 |
| 181. Provide the name of the UAC [Registry subkey] property that determines what level UAC is set to for admin privileges (Example UAC levels: Default, Always, Notify). | ConsentPromptBehaviorAdmin<br>- get-itemproperty<br>HKLM:\SOFTWARE\Microsoft\Windows\CurrentVer-  |



	sion\Policies\System   findstr Admin
182. Query the registry subkey where UAC settings are stored, and provide the flag.	NiceJob - get-itemproperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
183. What command-line (cmd) command will show service information?	sc
184. What command-line (cmd) command will show all services, running or not running?	sc queryex type=service state=all
185. What PowerShell command will list all services?	get-service
186. What registry location holds all service data?	HKLM\System\CurrentControlSet\Services
187. What registry subkey holds a service's .dll location	parameters -use regedit -HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services - parameters
188. Services have a name and display name, which could be different. What is the service name of the only Totally-Legit service?	Legit
189. Figure out the SID of the only Totally-Legit service. Example: S-1-5-80-159957745-2084983471-2137709666-960844832-[1182961511] Submit only the [bracketed] portion of the SID.	1182961511 -go to cmd -"sc showsid Legit"

190.





<b>What is the process ID (PID) of the SysV Init daemon?</b>	1 bombadil@mi-nas-tirith:~\$ ps --ppid 1 -lf
<b>191. Identify all of the arguments given to the ntpd daemon (service) using ps.</b>	-p /var/run/ntpd.pid -g -u 105:109 - ps aux   grep ntpd
<b>192. How many child processes did SysV Init daemon spawn?</b>	19 - ps --ppid 1   wc - subtract 2 for NO REASON
<b>193. What is the parent process to Bombadil's Bash process?</b>	sshd bombadil@mi-nas-tirith:~\$ htop -look at bombadil - bash
<b>194. Identify the file mapped to the fourth file descriptor (handle) of the cron process.</b>	/run/crond.pid - sudo lsof   grep cron
<b>195. Identify the permissions that cron has on the file identified in Processes 5. HINT: Read the man page for lsof to understand permissions.</b>	r,w - look at fg
<b>196. Identify the names of the orphan processes on the SysV system.</b>	Aragorn,Bruce-Wayne,Eowyn,Tolkien - htop, f5 look for things that literally say ORPHAN...
<b>197. Locate zombie processes on the SysV system. Identify the zombie processes' parent process.</b>	/bin/funk - htop , f5 look for Zs to populate
<b>198.</b>	



## OS PE's

Study online at [https://quizlet.com/\\_byrzbz](https://quizlet.com/_byrzbz)

- 
- Locate the strange open port on the SysV system. Identify the command line executable and its arguments.**
- `/bin/netcat -lp 9999`
  - `htop`
  - look for weird port
- 
199. **Examine the process list to find the ssh process. Then, identify the symbolic link to the absolute path for its executable in the /proc directory.**
- `/proc/1595/exe,/usr/sbin/sshd`
  - `htop` - look for sshd
  - find the PID
  - go to /proc directory
  - cd in 1595, looking for executable
- 
200. **Identify the file that contains udp connection information. Identify the process using port 123.**
- `ntpd,19,u`
  - `sudo lsof -i -nP`
- 
201. **What Sysinternals tool will allow you to read the SQLite3 database containing the web history of chrome?**
- `strings.exe`
- 
202. **What is the registry location of recent docs for the current user?**
- `HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`
- 
203. **BAM settings are stored in different registry locations based on the version of Windows 10. What version of Windows 10 is workstation2 running?**
- 1803
- 
204. **Figure out the last access time of the hosts file.**
- 9/22/2022
  - `ConsoleHost_history.txt`
  - PS
  - `C:\Users\andy.dwyer> Get-Content ConsoleHost_history.txt`
- 
205. **What is the literal path of the prefetch directory?**
- `C:\Windows\Prefetch`
- 
206. **In the Recycle Bin, there is a file that contains the actual contents of the recycled file. What are the first two characters of this filename?**
- \$R
-



- 
207. In the Recycle Bin, there is a file that contains the \$I original filename, path, file size, and when the file was deleted. What are the first two characters of this filename?
- 
208. What are the first 8 characters of the Globally Unique Identifier (GUID) used to list applications found in the UserAssist registry key (Windows 7 and later)? CEBFF5CD
- 
209. What cipher method are UserAssist files encoded in? rot13
- 
210. What main Windows log would show invalid login attempts? Security - (Failed User Account Login 4625)
- 
211. What main Windows log will show whether Windows updates were applied recently? System
- 
212. When reading logs, you may notice ... at the end of the line where the message is truncated. What format-table switch/argument will display the entire output? -wrap
- 
213. Find the questionable website that the user browsed to (using Chrome), that appears to be malicious.   
https://www.exploit-db.com  
- C:\> \$History = (Get-Content 'C:\Users\student\AppData\Local\Google\Chrome\User Data\History')  
- PS C:\> \$History | Select-String -Pattern "(https|http):\\[a-zA-Z\_0-9]"
- 
214. There is a file that was recently opened that may contain PII. Get the flag from the contents of the file. Flag, Found A.  
- Get-Item "REGISTRY::HKEY\_USERS\\*\Software\Microsoft\Windows\CurrentVersion\Recent\{...}"  
- C:\Users\stu-



	dent\Documents> cat .3-14-24.txt
215. Enter the full path of the program that was run on this computer from an abnormal location.	C:\Win- dows\Temp\bad_inten- tions.exe - Get-Item HKLM:\SYSTEM\Cur- rentControlSet\Ser- vices\bam\UserSet- tings\*
216. Enter the name of the questionable file in the prefetch folder.	BAD_INTEN- TIONS.EXE-8F2806FC.pf - Get-Childitem -Path 'C:\Win- dows\Prefetch' -Erro- rAction Continue
217. What is the creation time of the questionable file in the prefetch folder?	02/23/2022 - Get-Childitem -Path 'C:\Win- dows\Prefetch' -Erro- rAction Continue
218. Recover the flag from the Recycle Bin. Enter the name of the recycle bin file that contained the contents of the flag, and the contents of the deleted file.	\$RZVLP5M.txt,Dont- TrashMeyo - go to home dir "cd \ - "ls -force" to see hid- den recycle - "cd s-1-5-21-288...1003"
219. Find the file in the jump list location that might allow privilege escalation.	UIDPWD.txt - Get-Childitem -Recurse C:\Users\*\AppDa- ta\Roaming\Mi- crosoft\Windows\Re- cent -ErrorAction



	Continue   select FullName, LastAccessTime - just look for some- thing that looks like a phuqin file... - cat C:\Users\*\AppDa- ta\Roaming\Mi- crosoft\Windows\Re- cent\AutomaticDesti- nations\*
220. Check event logs for a flag string.	3v3nt_L0g' - PS C:\Users\andy.dwyer> Ge - part of the event:'.....the FL
221. File: /home/garviel/output.xml Identify the XML element name in the output be- low <scaninfo type="syn" protocol="tcp" numser- vices="200" services="1-200"/>	<scaninfo/>
222. Identify one of the XML attributes in the output below <scaninfo type="syn" protocol="tcp" numser- vices="200"	services="1-200"
223. What RFC is Syslog?	5424
224. What is the numerical code assigned to the facil- 4 ity dealing with authorization?	
225. How many severity codes are defined in the stan- 8 dard that defines syslog?	
226. What severity is assigned to system instability messages?	0 - Emergency



- 
227. In the legacy rules section of the file, what facility kernel is logged to 0.log?
- 
228. In the legacy rules section of the file, how many severities are logged to 0.log? 8  
- " \* " = wildcard means all of them
- 
229. In the legacy rules section of the file, how many severities are logged to 4min.log?  
List the severities from highest severity (lowest numerical listed) to lowest severity (highest numerical listed) using their severity name. emergency,alert,critical,error,warning  
- 4min = go
- 
230. In the legacy rules section of the file, how many severities are logged to 4sig.log?  
List the severities from highest severity (lowest numerical listed) to lowest severity (highest numerical listed), using their severity name. notice,informational,debug  
-sig - signaling
- 
231. What is being logged in not.log?  
Provide the facilities from lowest facility to highest facility numerically, and the severity being logged. (List only the first word for each.) mail,clock,ntp,notice  
- look at downloaded file  
- 2,9,12.=5  
/var/log/not.log - look at extended list
- 
232. What facilities and what severities are being sent to a remote server over a reliable connection using port 514?  
Provide the facility names, number of severities, and the correct destination IP address.
- 
233. Use the answer from Syslog 6 for this question.  
Do logs that match this filter ever get saved on the local machine?
- 
234. What messages are being sent to 10.84.0.1?  
Provide the facility number, the number of sever-



ity codes, and Layer 4 connection type as the answer.

235. **File: /home/garviel/output.xml**

Parse all of the IP addresses from the file using XPATH queries

[https://www.w3schools.com/xml/xpath\\_intro.asp](https://www.w3schools.com/xml/xpath_intro.asp)

HINT:

<http://xpather.com/>

<http://www.whitebeam.org/library/guide/Tech-Notes/xpathtestbed.rhtm>

Sample Output (without piping to MD5SUM)

addr="XXX.xxx.xxx.xxx"

addr="XXX.xxx.xxx.xxx"

addr="XXX.xxx.xxx.xxx"

addr="XXX.xxx.xxx.xxx"

addr="XXX.xxx.xxx.xxx"

addr="XXX.xxx.xxx.xxx" --TRIMMED--

Flag format: md5 hash of output

236. **What Volatility plugin will dump a process to an executable file sample?** procdump

237. **What Volatility plugin will extract command history by scanning for \_COMMAND\_HISTORY?** cmdscan  
- vol -f  
.\\crindex.vmem --profile=WinXPSP2x86 -h  
| findstr command

238. **What Volatility plugin will show driver objects?** driverscan  
- vol -f  
.\\crindex.vmem --profile=WinXPSP2x86 -h  
| findstr driver

239. **What command do you run to find which memory profile to use with a memory image?** imageinfo

240. **What switch/argument will list all plugins for Volatility?** -h



- 
241. **In terms of Volatile Data, what locations are the MOST volatile?** CPU registers, cache
- 
242. **What is the 12th plugin listed in the Volatility help menu?** cmdscan
- 
243. **What profile do you use in conjunction with this memory image?** WinXPSP2x86  
**0zapftis.vmem**
- 
244. **What command did the attacker type to check the status of the malware?** sc query malware  
- run "vol -f  
.\\0zapftis.vmem  
--profile=WinXP-  
SP2x86 cmdscan"
- 
245. **What are the last 7 digits of the memory offset for the driver used by the malware?** 1a498b8  
- run "vol -f  
.\\0zapftis.vmem  
--profile=WinXP-  
SP2x86 driverscan"
- 
246. **The process running under PID 544 seems malicious. What is the md5hash of the executable?** 6-  
CEE14703054E226E87A  
- run "vol -f  
.\\0zapftis.vmem  
--profile=WinXP-  
SP2x86 pslist' to get  
PID 544  
- run "vol -f  
.\\0zapftis.vmem  
--profile=WinXP-  
SP2x86 procdump -p  
544 -D ." to get  
location of cmd.exe  
- run "Get-File-  
Hash .\\exe-  
cutable.544.exe -Al-





	gorithm MD5" to get hash
247. What remote IP and port did the system connect to? Flag format: ip:port	172.16.98.1:6666 - run "vol -f .\\0zapftis.vmem --profile=WinXP- SP2x86 connsnscan'
248. What is the domain portion of the following SID: S-1-5-21-1004336348-1177238915-682003330-1000	21-1004336348-11772389
249. What PowerShell command will list domain groups?	Get-ADGroup
250. What PowerShell command will list all users and their default properties?	Get-ADUser -Filter 'Name -like "*"'
251. What PowerShell command will allow you to search Active Directory accounts for expired accounts without having to create a filter?	search-adaccount
252. Find the expired accounts that aren't disabled. List the last names in Alphabetical Order, separated with a comma, and no space between.	krause,page - Get-ADUser -Filter 'enabled -eq \$true' -Properties AccountExpirationDate   Select sAMAccountName, distinguishedName, AccountExpirationDate   findstr 25
253. Find the unprofessional email addresses. List the email's domain.	ashleymadison.com - Get-ADUser -Filter 'Name -like "*"' -Properties EmailAddress   select EmailAddress, Domain*
254.	



<b>The flag is the unprofessionally-named file located somewhere on the Warrior Share. Connect to the Warrior Share: net use * "\\file-server\warrior share"</b>	lulz.pdf - ls -R
255. <b>Find the short name of the domain in which this server is a part of.</b>	army? - (gwmi win32_computersystem).Domain - Get-ADForest
256. <b>The flag is the name of the file where someone is requesting modified access rights. Connect to the Warrior Share: net use * "\\file-server\warrior share"</b>	14287.pdf - ls -Rs -R
257. <b>What is the RID of the krbtgt account. Example: S-1-5-21-1004336348-1177238915-682003330-[501]</b>	502 - Get-ADUser -Identity 'krbtgt' -Properties Description - RID is last 3 of SID
258. <b>How many users are members of the Domain Admins group?</b>	1 - Get-ADGroupMember -Identity "Domain Admins"
259. <b>How many total users are members of the Domain Admins group?</b>	14 - Get-ADGroupMember -Identity "Domain Admins" -recursive
260. <b>Find the following three accounts: two accounts with passwords that never expire one account that has its password stored using reversible encryption List the last names in Alphabetical Order, comma-separated, no spaces. Do not list built-in accounts.</b>	- Get-ADUser -filter * -properties PasswordLastSet, PasswordExpired, PasswordNeverExpires   sort Name   ft Name, PasswordLastSet, PasswordExpired, PasswordNeverExpires



	- Get-ADUser -Filter 'userAccountControl -band 128' -Properties userAccountControl
261. The flag is the name of the user who is requesting modified access rights.	Karen Nance - Get-AdGroupMember -identity "Domain Admins" -Recursive   %{Get-ADUser -identity \$_.DistinguishedName}
262. Find the accounts that contain unprofessional information in the description.	Brandywine,Jimenez Get-ADUser -Filter 'Name -like "*" -Properties Description   select Description, Name
263. Find the following three accounts: - two accounts with passwords that never expire - one account that has its password stored using reversible encryption	phone_matrix.xlsx - ls -r
264. Continue to follow the insider trail to find additional insider threats and their compromised mission.	Tiiffany.Bellacino - Get-ADUser -Identity 'Karen.Nance' -Properties * - find the weird shit - used rot13 to decode and found bitch ass tiffany - Get-ADUser -filter * -Properties *   findstr Tiffany
265. Continue to follow the insider trail to find additional insider threats and their compromised mission.	Damian.Lewis - Get-ADUser -Iden-



**The flag is the username resulting from assembling clues within a user's records.**

tity 'Tiffany.Bellacino'  
-Properties \*  
- find abnormal stuff  
- Get-ADUser -filter \* |  
findstr wis

**266. Continue to follow the insider trail to find additional insider threats and their compromised mission. The flag is the full name of the insider threat identified.**

**HINT: Search the Active Directory record for the user identified in follow\_insider\_trail\_2.**

- Isiah.Jesus  
- Get-ADUser -Identity  
'Damian.Lewis' -Prop-  
erties \*  
- find weird  
- Get-ADUser -filter \* |  
findstr Isiah

**267. Continue to follow the insider trail to find additional insider threats and their compromised mission. This flag is a video link.**

**Hint: Search the Active Directory record for the user identified in follow\_insider\_trail\_3.**

<https://www.youtube.com/>  
- Get-ADUser -Identi-  
ty 'Isiah.Jesus' -Prop-  
erties \*  
- there was some  
weird hash stuff  
- aHR0cHM6Ly93d3cueW/  
- "==" means link  
- user cyberchef in ctf  
for base64 decode