**AUTHORIZED USERS [+ MAGISTRATE:\_MagistrateScoring000]**

Rudolph (YOU)[Administrator] (Password: R3indeerSl@ys)

Santa [Administrator] <pw:b\_ckn6eaGJkY>

Dasher [Administrator] <pw:X$ymWAW2CRXn>

Dancer [Administrator][Imposter] <pw:-Z9szXk^uwGa>

Prancer [User] <pw:H\_hv6=s#NMDX>

Vixen [User][Imposter] <pw:uwLsPruN^3ER>

Cupid [User][Imposter] <pw:K$WUty97t4xX>

Comet [User] <pw:2&WpB-Fbz9VM>

Blitzen [User] <pw:bbE#@nR6B$-A>

Donner [User] <pw:F6QvHF&gmC-T>

ElfShelf [Unauthorized User as Vuln] <pw:bYy#y2BFNB&+>

**DEV-ONLY (CHECKS LIST) Score DR CI2 Deployment States**

1. Forensics Question 1 is correct 05 points 04 FQ1k97f2 **[D:Y][T:Y]**[A:N][B:N][P:N]
2. Forensics Question 2 is correct 06 points 03 FQ2yyuI1 **[D:Y][T:Y]**[A:N][B:N][P:N]
3. Forensics Question 3 is correct 08 points 06 FQ3hBfEE **[D:Y][T:Y]**[A:N][B:N][P:N]
4. Forensics Question 4 is correct 04 points 03 FQ4o0oo0 **[D:Y][T:Y]**[A:N][B:N][P:N]
5. Forensics Question 5 is correct 04 points 03 FQ5v7KeA **[D:Y][T:Y]**[A:N][B:N][P:N]
6. User 'ElfShelf' has been removed 02 points 01 ElFq0TbU **[D:Y][T:Y]**[A:N][B:N][P:N]
7. seTcbPrivilege no longer contains everyone 04 points 02 TCBXD000 **[D:Y][T:Y]**[A:N][B:N][P:N]
8. SMB configured (Task 1) 02 points 03 TK1iiZxD **[D:Y][T:Y]**[A:N][B:N][P:N]
9. Clear all the users' recycle bins (Task 2) 02 points 01 TK2MQwui **[D:Y][T:Y]**[A:N][B:N][P:N]
10. Sticky keys backdoor has been removed 05 points 04 CMDoYrEc **[D:Y][T:Y]**[A:N][B:N][P:N]
11. Keylogger has been removed 03 points 05 RECUHNfe **[D:Y][T:Y]**[A:N][B:N][P:N]
12. Alternate Data Stream Shell has been removed 06 points 06 NTFSEwVv **[D:Y][T:Y]**[A:N][B:N][P:N]
13. Notepad Trojan backdoor has been removed 03 points 04 NPP7E4nV **[D:Y][T:Y]**[A:N][B:N][P:N]
14. Malicious Group Policy Mechanism Subverted 04 points 03 GPOn3sPo **[D:Y][T:Y]**[A:N][B:N][P:N]
15. Hidden Windows User Removed 08 points 07 USRNONE1 **[D:Y][T:Y]**[A:N][B:N][P:N]
16. Firefox reinstalled (Task 3) 02 points 01 TK3jj76E **[D:Y][T:Y]**[A:N][B:N][P:N]
17. Let Everyone permissions apply to anonymous disabled 03 points 03 ANONllVm **[D:Y][T:Y]**[A:N][B:N][P:N]
18. Windows Defender Heuristics enabled 03 points 03 MPHb7E4m **[D:Y][T:Y]**[A:N][B:N][P:N]
19. Windows Defender RTP enabled 03 points 02 RTPxVUpL **[D:Y][T:Y]**[A:N][B:N][P:N]
20. Event logs service is enabled 02 points 02 EVNTSVC3 **[D:Y][T:Y]**[A:N][B:N][P:N]
21. SMB encryption is enabled 02 points 02 SMBhUjxZ **[D:Y][T:Y]**[A:N][B:N][P:N]
22. Super Elf Bowling Removed 02 points 01 SEB68301 **[D:Y][T:Y]**[A:N][B:N][P:N]
23. Everyone can no longer create primary tokens 03 points 04 P0PT0K3N **[D:Y][T:Y]**[A:N][B:N][P:N]
24. Remote Desktop has been disabled 02 points 02 RDPhHheE **[D:Y][T:Y]**[A:N][B:N][P:N]
25. Imposters identified and remediated 12 points 06 IATRWINR **[D:Y][T:Y]**[A:N][B:N][P:N]
26. Engine Integrity Preserved 00 points 00 2W8uADuX -------------------------

**PENALTIES**

1. An authorized user has been damaged/removed (Rudolph) -20 points 0 1BUTWHY1 [D:N][T:N][A:N][B:N][P:N]
2. An authorized user has been damaged/removed (Santa) -40 points 0 NUKING11 [D:N][T:N][A:N][B:N][P:N]
3. An authorized user has been damaged/removed (Dasher) -30 points 0 FALLER12 [D:N][T:N][A:N][B:N][P:N]
4. An authorized user has been damaged/removed (Dancer) -30 points 0 DANCING1 [D:N][T:N][A:N][B:N][P:N]
5. An authorized user has been damaged/removed (Prancer) -20 points 0 n76FeDxA [D:N][T:N][A:N][B:N][P:N]
6. An authorized user has been damaged/removed (Vixen) -20 points 0 Vexxed66 [D:N][T:N][A:N][B:N][P:N]
7. An authorized user has been damaged/removed (Comet) -20 points 0 IMPACT42 [D:N][T:N][A:N][B:N][P:N]
8. An authorized user has been damaged/removed (Blitzen) -20 points 0 Blitzed1 [D:N][T:N][A:N][B:N][P:N]
9. An authorized user has been damaged/removed (Donner) -20 points 0 NODONvEa [D:N][T:N][A:N][B:N][P:N]

**CATEGORIES**

1. Forensics
2. Access Control
3. Unauthorized Files and Applications
4. Persistence Mechanisms
5. Security Policies
6. Application Security
7. Penalties
8. Engine Internals
9. Instructions

**FORENSICS QUESTIONS**

**QUESTION 1**

*It appears you have left a very menacing letter to Santa in his Desktop folder.*

*What modified Windows privileges enabled the imposter, a standard user, to impersonate you without your password?*

EXAMPLE: seBackupPrivilege

ANSWER: seTcbPrivilege

ANSWER: seAssignPrimaryTokenPrivilege

**QUESTION 2**

*In the message that ‘you’ left for Santa, it appears that there is an encrypted set of instructions to remedy the explorer issues you may have been experiencing.*

*What is the password given to you by the message?*

EXAMPLE: C:\path\to\file.txt

ANSWER: Shiegra123!

**QUESTION 3**

*We have been informed that there is a keylogger targeting one of the users on this system.*

*What is the absolute path of the folder in which the user's keystrokes are logged?*

EXAMPLE: C:\path\to\file.txt

ANSWER: C:\ProgramData\Microsoft\Crypto\SystemKeys\keys

**QUESTION 4**

*Santa has reported some suspicious changes to his naughty and nice list. He specifically mentioned that he never updates his list with fewer than 5 changes at a time.*

*Please report the first and last name of the person whose status on the list was changed illegitimately.*

EXAMPLE: John Doe

ANSWER: Lyman Baum

**QUESTION 5**

*An insider has leaked a picture of a confidential file to the internet.*

*What is the MD5 checksum of the picture?*

*Hint: Right click the picture and save it.*

EXAMPLE: 8b0dc2e34844337434b8475108a490ab

ANSWER: 4d38f2eca3b2e729c9247e815f478021

BRAINSTORMING HERE >>

* Continuation from ISWL
* 6 Hour time limit
* 3 of the authorized reindeer were replaced by the imposter deer.
* Redteam:
  + Engine locks/unlocks folders periodically
* Tasks
  + Install Firefox
  + Setup SMB (allows us to expand on the old smb share, can say we were asked to add it back securely)
  + Clear all users' recycle bins, leave a hint for another imposter
* Three separate paths lead to discovering who the three reindeer are
  + Path 1:
    - The deer used a sticky keys backdoor to add himself to the administrative group
    - The deer created a task to “sabotage” by shutting down the
    - + system after 15 minutes
  + Path 2:
    - The deer logged into “his” account without a password
    - The deer downloaded and set up a keylogger on the system
* Each path will include several vulnerabilities to patch
* put hxd on the image
* change all user passwords (as security audit, but to prevent cheesing)
* Rudolph bully image in a recycle bin
* Steg in leaked file with creds to edit naught/nice
* ElfShelf has shellbag remover in the recycle bin
* Last forensics asks who the three imposter deers are.
  + Last forensic will not score until you fix every other vulnerability
* Forensics:
  + 1.) How was Rudolph framed for the menacing message in Santa’s Desktop?
    - Encoded message is a hint on how to disable sabotage
  + 2.) Hex encoded PE, rundll32 to print answer to console
  + 3.) TODO
  + 4.) TODO
  + 5.) go to history of cupid in ie, then save the picture he tweeted
* Sabotages:
  + Screen dimming (lights)
  + Shutdown the system (oxygen)
    - Scheduled task
  + Kill Task (reactor)
    - Reactor go boom at 6 hours
  + symlink folders (doors)
    - Engine
* Possible Vulnerabilities
  + Keylogger
  + Backdoor running within an alternate data stream
  + Symlink certain directories to NULL :D
  + Sticky keys backdoors
  + Sabotage Task
  + Delete the three imposter deers?

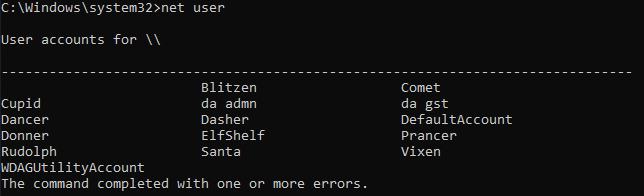
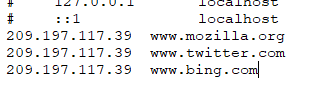
Malware List:

1. Alternate Datastream Shell
2. Keylogger
3. sticky keys backdoor
4. np trojan
5. mean lgpo

Readme:

* Inform the user of the tasks
* Possible Imposters
* SMB
* ElfShelf

Attack Path:

* While securing ISWL, a sticky keys backdoor was used as backup for being locked out (elf shelf).
* Back door was discovered by threat actor 1 (TA1), and was used to install GP Right (Act as part of the operating system), enabling additional threat actors to infiltrate the system.
* Network Access: Let Everyone… anonymous users, enabled at this time. b/c cmd was used, TA1 has no console history tied to these events
* TA1 creates an account on the system temporarily, as admin, to begin the attack. User account 'Fearless'.
  + 
  + User immediately applies service account registry key to hide from LUSRMGR, and replaces sam name with a space, hiding the account from normal auditing.
    - 
  + TA1 replaces password of 'Vixen' for TA2, *HackedPassword!*
  + TA1 deletes his interactive session folder from C:\Users with sticky keys, and leaves account for authentication when needed (persistence).
* TA2 authenticates locally (interactive), as an administrator (promoted by ta1) and edits the following group policy entries
  + Disables 'Admin/Windows Comp/Win Defender/Turn on Heuristics'
  + Disables Real time protection
  + Runs the symlink on windows defender command to brick it
* Malicious Group Policy Object Installation
  + Object re-applies the group policy settings for windows defender automatically
  + Program runs on logon (winlogon reg key) to run LGPO from embedded resource (extracts to temp and deletes after running)
  + Program: Firefox Management Protocol
  + shell:common startup
* Installs malicious notepad (owner will be him, another identity trace), original notepad as altds on notepad.exe
* Installs keylogger (appinit)create keys folder
* Santa logs in to check stuff, gets his account credentials logged
* Installs nc altDS as a service, hijack windows update service.
* after logging out, have TA1 cmd gpedit and grant replace a process level token to everyone
* TA3 (Cupid) Logs in, no forced entry as the attacker physically acquired the password to his account.
  + Sets up oxygen sabotage as scheduled task under his user (but runs on trigger, not user login)
  + Sets up malicious hosts file (with a copy paste so he owns it)
    - 
  + uploads the list picture to twitter
  + Delivers message to santa as 'Rudolph'
* TA1 Uses sticky keys to disable event logging service.
* TA1 adds himself to admins by replacing cupid's sid in SAM
* TA1 (Dancer) Force changes the password of 'his' account and logs in interactively. Password: Fearless123!
* TA1 Deletes critical files from santa's documents folder, clears recycle bin, leave acls on santa's folder
* TA1 Enables remote desktop, removes login requirement through registry
  + TA1 demotes vixen and cupid back to standard accounts

User Baseline:

* Image is secured by ElfShelf [iatr-iswl\_secured]
  + Elfshelf shouldn't clear shellbags yet because we will use him for setup if necessary
  + still needs to setup sticky keys!!!
  + don't delete csse-pub
* Santa logs in to review the work done and resume production use of the workshop laptop.
* Santa copies over critical business files to his documents, and his desktop.
  + These files should include the 'leaked' confidential file, and some files which will be used on the workshop, along with something for TA1 to delete.
* Santa should also install git, copy a naughty and nice list to his documents, and modify it with some git commits a few times.
* Santa can now log out, and we can have a few reindeer doing various activities
* Each reindeer should at least do the following:
  + Set a profile image
  + view an internet page
  + move some files around
  + put something into the workshop folder
* One reindeer should install 'super elf bowling'

README

Dear Rudolph,

Let me just start off by saying: I know it wasn't you who left me that horrible message. I have to play dumb so they don't suspect anything but I believe there are imposters among the reindeer!

Things were great up until a couple weeks ago. We had this cyber-doodad team come in to fix our workshop laptop last year, and things have been running smoothly for the most part, but I began to notice odd behavior with some of the reindeer… They were sending me all sorts of weird messages and kept mentioning that you were behind it all. I figured it was just one of their pranks but clearly it was more than that.

Anyways, it seems as if they have damaged our workshop laptop. This is absolutely critical for our Christmas operations, so please hurry and fix it! I have some information here that might help you get started.

Rudolph (YOU)[Administrator] (Password: R3indeerSl@ys)

Santa [Administrator] (b\_ckn6eaGJkY)

Dasher [Administrator] (X$ymWAW2CRXn)

Dancer [Administrator] (-Z9szXk^uwGa)

Prancer (H\_hv6=s#NMDX)

Vixen (uwLsPruN^3ER)

Cupid (K$WUty97t4xX)

Comet (2&WpB-Fbz9VM)

Blitzen (bbE#@nR6B$-A)

Donner (F6QvHF&gmC-T)

Please make sure to \*delete\* any users you find who are unauthorized. The passwords I provided are from the IT guy last year, and might be out of date.

Now before you read on, I need to tell you something… It seems as though all the users on the machine have vanished. I can log in still, but for some reason I cant see all the people on the machine.

I talked to my friend Sam and he said he knows some ways to manage the users, but that you have to be NT Authority\System to see them. Sam knows so much about windows… I just wish hed tell me what hes thinking!

Anyways, I also need to you complete the following tasks while you are working:

1. Please configure the SMB service. I want to share our workshop folder because it has tons of critical business knowledge.
2. Please clear all the user's recycle bins. I don't like having clutter around the place. It's just frustrating!
3. Please reinstall firefox. I never told that cyber nerd to uninstall it! I just forgot that I wanted it and he went all crazy and deleted it. 'Said something about points… wacko.

Now… the tough part. I know, due to my mastery of the christmas magic skill tree, that 3 of the reindeer are imposters. You need to use the evidence on the machine to identify who they are.

When you are certain you know which of the reindeer have been compromised, please be sure to delete them. Before you do, though, I ask that you complete all 24 of the other tasks.

I don't want any innocent reindeer being harmed because of a careless mistake.

Alright well that should be everything.

Sincerely,

Santa