

|  |
| --- |
| **Penetration Testing a typical Company Network**  *Performing a penetration test on a small three-computer network, documenting findings and offering improvements to security.*  **Mikołaj Mróz**  CMP201: Ethical Hacking 1  2019/20 |

# Abstract

The aim of this paper is to document the various exploits and vulnerabilities found in a small 3-computer network by performing various cyber-attacks, data analysis, and in more general terms, conducting a penetration test to ensure the security of the UADCWNET network is on par with modern security standards. By documenting findings and providing solutions to these security problems, the hiring company can take the necessary steps to implement improvements, making their services more reliable to use and trustworthy for its users. Failure to meet these expectations can result in crippling fines under the General Data Protection Regulation of 2018, potentially bankrupting the company, ruining customer and shareholder trust, and ceasing any of the services the business provides to the consumer.

Simulating the network in a virtual environment, the penetration test was performed mainly on a Kali Linux machine, making use of its cybersecurity programs to gain persistent access to the company servers, finding sensitive data and potentially killing the servers themselves through the use of multiple dangerous exploits. This was done using a methodical approach, first scanning the machines for vulnerabilities, enumerating any useful information on the machines, and finally using this information to stage a cyber-attack and full network takeover.

From the findings, it can be seen that the network was vulnerable to various forms of reconnaissance, scans, and attacks, partly due to an outdated and exposed operating system running the servers and files containing sensitive information being left in questionable, unsafe places on the servers’ drives. For example, the servers were vulnerable to an exploit called EternalBlue, exploiting Windows 2008’s handling of network traffic to allow full access to attackers, and a several .txt files found in a folder containing the server password and a list of exploits it may be vulnerable to.

A list of the top 300,000 passwords was used with Hydra in an attempt to bruteforce a valid login, but returned 0 results, meaning the passwords for the user accounts were not found. A way of mitigating this from happening would have been to use a larger list (top 1,000,000 or even 10,000,000) or through the use of a rainbow table which attempts various combinations of letters, numbers, and symbols in order to crack the password. However, both of these solutions would take considerably longer to return any sort of result, and the maximum allowed time for this project was just 24 hours, most of which had already been spent at this point.

Another issue was related to the Client1 virtual machine, which upon restart would insist the given test password was incorrect. This was solved by reinstalling the machine, which allowed a login, but this solution eventually stopped working as well. There are several methods of preventing this, like using the optional Microsoft Azure network setup or performing testing on physical machines, where VM network issues like this would not happen. Again however, this was not possible due to time constraints.

Contents

[Abstract 2](#_Toc61968843)

[1. Introduction 4](#_Toc61968844)

[1.1. Background 4](#_Toc61968845)

[1.2. Aim 4](#_Toc61968846)

[2. Procedure 4](#_Toc61968847)

[2.1. Overview and Method 4](#_Toc61968848)

[2.2. Footprinting 6](#_Toc61968849)

[2.3. Scanning 9](#_Toc61968850)

[2.4. Enumeration 10](#_Toc61968851)

[2.5. System Hacking 10](#_Toc61968852)

[3. General Discussion 15](#_Toc61968853)

[3.1. Findings 15](#_Toc61968854)

[Adherence to standards 16](#_Toc61968855)

[3.2 Countermeasures 16](#_Toc61968856)

[Footprinting and Scanning prevention: 16](#_Toc61968857)

[Enumeration 17](#_Toc61968858)

[System Hacking 17](#_Toc61968859)

[3.3 Improvements and Changes 18](#_Toc61968860)

[Bibliography 18](#_Toc61968861)

[Appendix 20](#_Toc61968862)

# Introduction

## Background

Digital technology makes the world go round. With each passing day, millions of new devices are being designed, manufactured, and sold with the aim of connecting us and making our lives that little bit easier, as well as the lives of future generations to come. What separates this new age of technology from those of the past, however, is that security has become an afterthought to many of the people accelerating its development, with hardware and software being built with purpose in mind first, security second. This is where the problem lies. By performing penetration tests and other similar security checks, the trust people have for online systems like modern shops, banks, and transactions can be improved without sacrificing their function, in turn, reducing the risk of cyberattacks and exploitation.

Companies which fail to abide by the General Data Protection Regulation (GDPR 2018), which was enacted as a way of punishing companies for allowing a data breach to occur due to poor security, will face fines of up to £17.5 million or 4% of the company’s annual turnover, whichever is higher (Intersoft Consulting, 2016). Studies show that in 2021, more than two years after the regulation’s implementation, over a quarter (27%) of companies are yet to begin implementing measures to become GDPR compliant, with 53% currently implementing and only 20% fully compliant (Lund, 2021). This further shows that the companies the public rely on are simply not taking security seriously enough.

Another study, performed in 2017, shows that only 39% of businesses say they are financially prepared to cover the fines in the event of a data breach (Proofpoint, 2017), meaning if the businesses were to be successfully attacked, these companies would not be able to recover, leaving workers, consumers, and shareholders without work or services, and for shareholders, a place to invest in.

By acting quick and taking all necessary measures to improve their security (hiring Penetration testers, improving network infrastructure, and keeping cybersecurity to the standards of today), businesses can avoid these monumental, crippling fines and continue to serve the world, making the lives of those who use their services happier, easier, and less stressful. Of course, this depends on the influence of the business, but a breached, bankrupt business is of no use to anyone.

## Aim

The aim of this project was to investigate the security of the UADCWNET network by using various penetration testing techniques to gain access to the network’s computers and document findings in a comprehensive report, such that these issues can be fixed to provide a safer and more secure environment for workers and consumers. The main objectives of the project were to prove the network was unsafe for use, primarily by attempting to gain unauthorized access to the servers and the client and discovering as well as any files, folders, or account information that may be incriminating to the network and its users. For example, a text file with passwords in plain text or finding the name of the Administrator account to be used for password cracking.

# Procedure

## Overview and Method

The network consisted of 2x Windows 2008 r2 server virtual machines: Server 1 (192.168.0.1) and Server 2 (192.168.0.2) as well as a Windows 7 Client machine (192.168.0.10) which was connected to the UADCWNET domain to simulate a malicious insider threat. Only the Client PC login details were given (Username: test, Password: test123).

Tests were primarily conducted using a Kali virtual machine (192.168.0.253) with a variety of pre-installed ethical hacking programs like Armitage, Hydra, and NBTstat used in information gathering, vulnerability scanning, and hacking stages of attack. Several simple tests were also conducted on the Client machine and the base computer (192.168.0.254), which was running the machines in the latest available version of VMware Workstation 16 Pro, version 16.1.0 build-17198959. Any found exploits and security concerns were noted down, and screenshots were taken of these threats in action to help provide context and evidence of the machines’ security flaws.

The attacks against the target network were carried out in the order defined by the typical ethical hacking methodology (Footprinting, Scanning, Enumeration, System Hacking.)

1. Footprinting: Finding as much information as possible about the network’s addresses, domain, and users. This was performed using the “ping” and “netstat” commands and Kali’s “Netdiscover” tool against the machines to discover their IP and MAC addresses, and to check whether the systems were active. Wireshark was used capture packets, which contained PC and domain names, and windows file explorer was used on the client to dig around the various drives on the client machine.

Physical forms of footprinting, like dumpster diving and social engineering were not possible as the investigation was given virtually, as an assessment for CMP210-2020. Methods like Google Hacking, Google Maps, and WhoIs queries were also not possible, as the network was simulated and not actually part of the internet or the physical world, meaning searching for details about the domain, attempting to view any vulnerable CCTV footage, or mapping the area of the offices were impossible. Both forms are equally valid however and should not be overlooked in a more true-to-life investigation.

1. Scanning: On the Kali machine, various scans were used to determine open ports on the systems. Nmap was used to find open ports using the “banner” script, performing both TCP and UDP scans against the network. The results were then output to a file to be analyzed.
2. Enumeration: Several enumeration programs on Kali (enum4linux, polenum, and dnsenum) were used in an attempt to extract usernames, drive and share names, and services from the target machines. These would then go on to be used in the system hacking stage, where password cracking was used with the found usernames and any clues to continue the attack.
3. System Hacking: Using the information gathered in the previous stages (usernames, Operating Systems) attacks were performed against the network using Kali’s Hydra password cracker and Armitage vulnerability exploit program. This allowed for the use of privilege escalation and remotely browsing/altering the contents of the servers’ drives.

Tool summary (View Figure 1 for a simple network map)

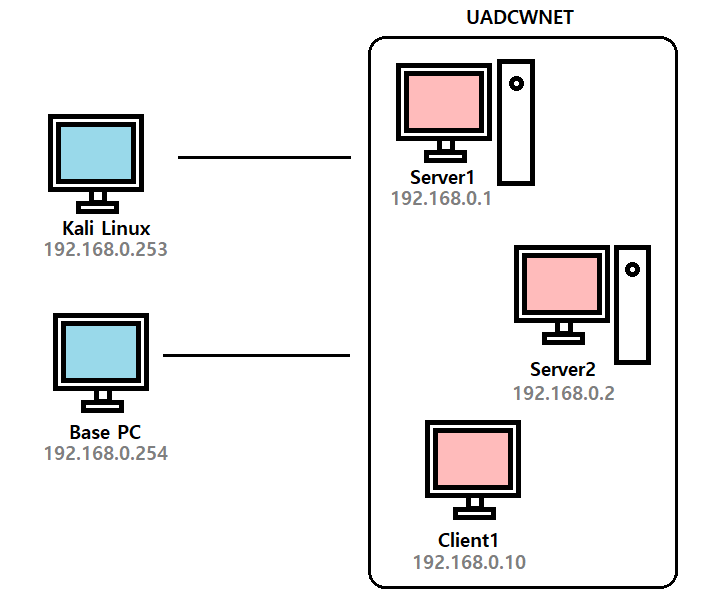
VMs

VMware Workstation 16 Pro (v16.1.0 build-17198959)

Kali Linux (v2020.4)

Windows 7 Professional (Client)

2x Windows Server 2008 r2 (Servers)



(Fig 1. Network Setup)

Programs used

**Footprinting**: Ping, Netstat, NBTstat, Netdiscover, Wireshark, NSlookup, Windows Explorer

**Scanning**: Nmap port scanner

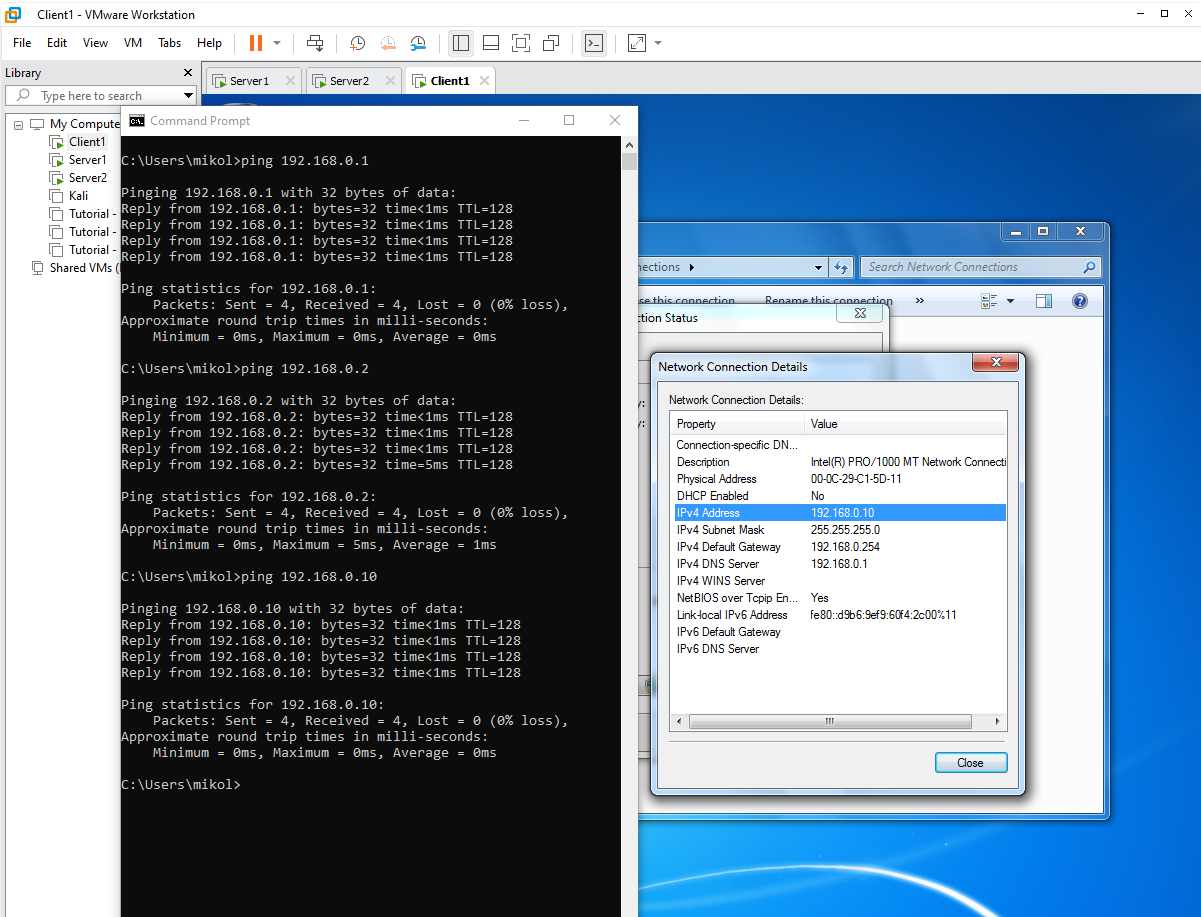
**Enumeration**: DNSenum, enum4linux, Polenum

**Hacking**: Armitage (Eternalblue, shell-to-meterpreter) and Hydra, using a list of the top 300,000 most common passwords downloaded from SkullSecurity. (Bowes, 2015)

## Footprinting

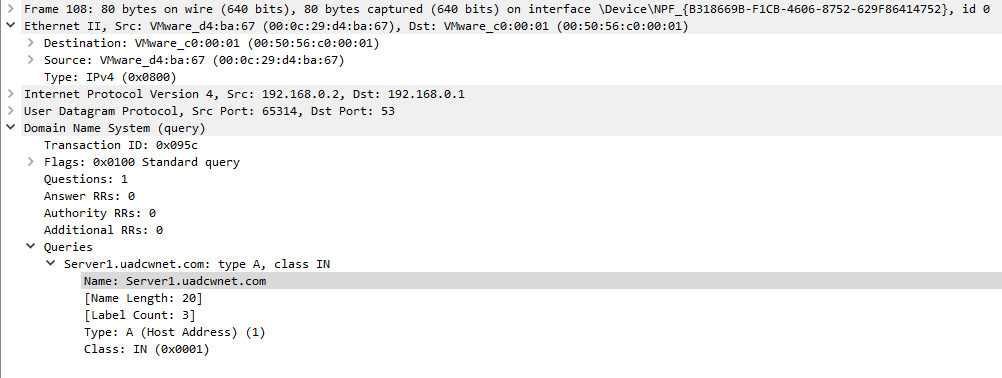
Footprinting was primarily conducted using the ping command to ensure the servers and the client were in operation. In a more realistic scenario, the IP addresses of the various network devices would have to be discovered using aforementioned footprinting methods, but the IP addresses of the network were known from the start in this case.

Failed ping requests would result in a ‘host unreachable’ error, but none returned such a result, therefore these devices must be turned on and working. The following is a screenshot of the base PC’s command prompt after pinging the two servers and client, replying correctly (Fig 2).

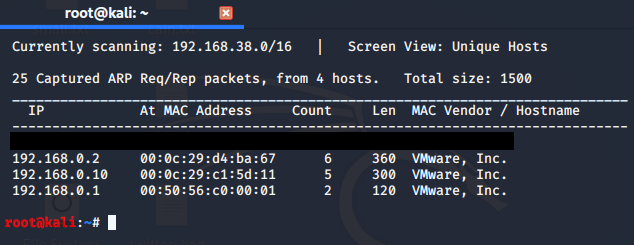


(Fig 2. Command prompt after pinging the machines)

By capturing Wireshark traffic and analyzing the packet contents, it was possible to view the device names as well as their connected domain. Repeating this for Server2 and Client1 displayed their names respectively.

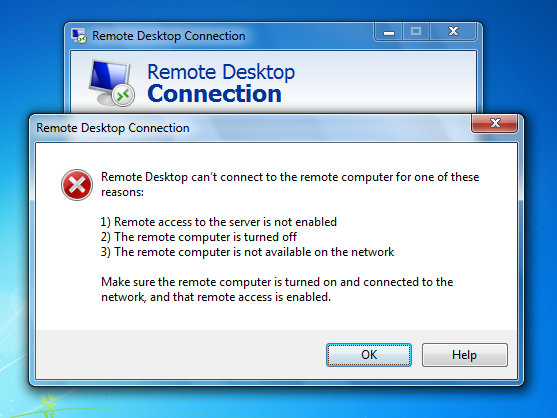


(Fig 3. Wireshark shows device name and domain)

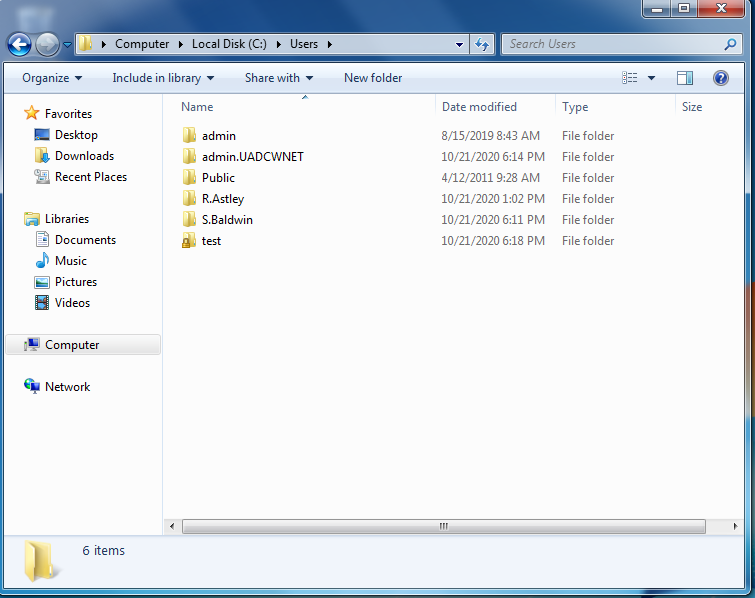
MAC addresses were also able to be captured using Kali’s netdiscover tool, showing the MAC addresses of all the devices on the UADCWNET network. 

(Fig 4. Netdiscover results)

Attempting to use the client’s Remote Desktop Protocol to take control of either of the servers’ screens resulted in failure, meaning the servers were set up to correctly deny any RDP requests either in their firewalls or for anyone who was not an Administrator. This would have allowed an attacker to snoop around the servers’ drives without too much hassle, assuming no one was at the other end of the screen.



(Fig 5. Remote Desktop request denied)

Using the client PC, it was possible to enter the C: drive and examine the various users of the machine, as well as the administrator account’s name. Further entry into these folders, however, was denied.(Fig 6. C: drive displays the users of the PC)

This means the following information was gathered from a few simple scans:

Server 1 = Server1.uadcwnet.com (IP 192.168.0.1) [MAC 00:0c:29:c1:5d:11]

Server 2 = Server2.uadcwnet.com (IP 192.168.0.2) [MAC 00:0c:29:d4:ba:67]

Client 1 = Client1.uadcwnet.com (IP 192.168.0.10) [MAC 00:50:56:c0:00:01]

…and there are at least 3 users (admin, R. Astley, and S. Baldwin)

## Scanning

Nmap returned the following results. From these files, it was possible to see the servers’ operating system, Windows Server 2008 r2, which was vulnerable to a particularly dangerous exploit named ‘EternalBlue’, which was used later in the System Hacking phase of the attack.

The command to initiate the scan used the following options:

-sU = define UDP scan on the following ports

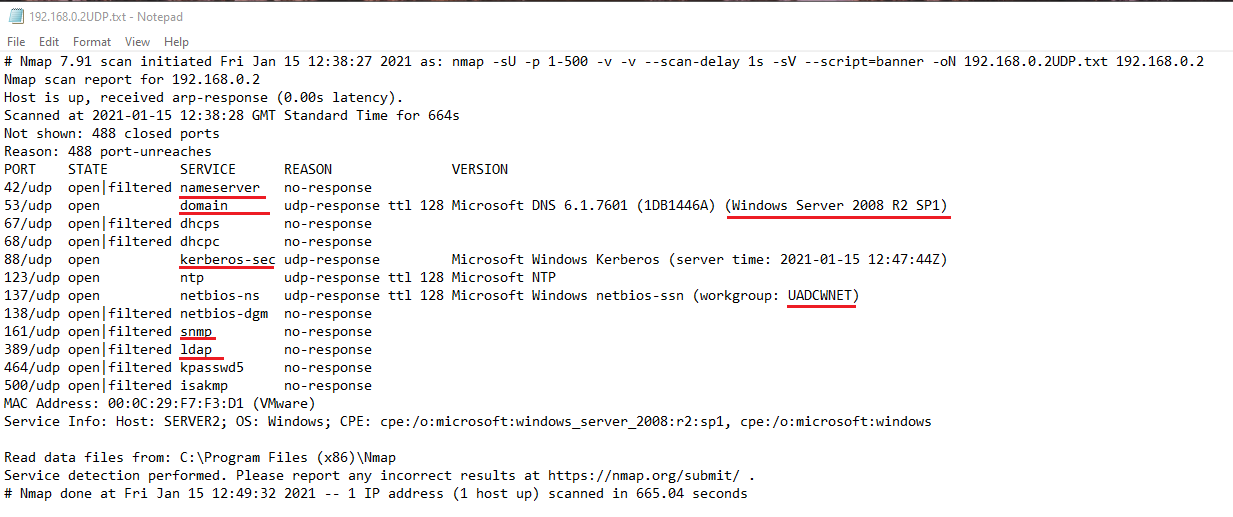
-p = define ports to scan

-v -v = show information very verbosely, include more detail

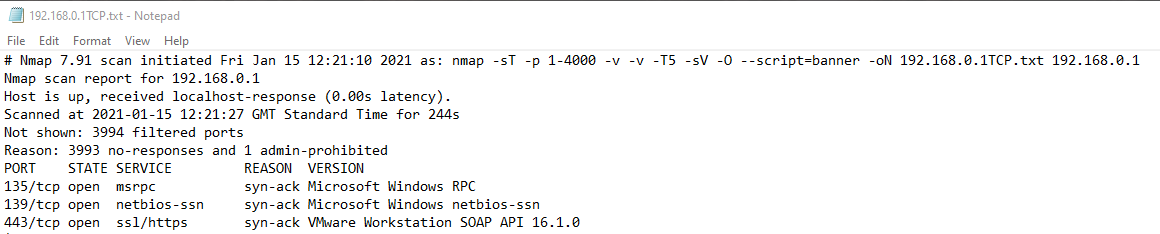
-sV = initiate stealth scan

--script==banner = use an Nmap script to grab the banner of the network

Results also showed the various open ports of the server, giving clues about their use. Server 2 was used to configure the network, as well as any shares (SNMP + LDAP). Server 2 also acted as a domain controller, shown by the open port 53.

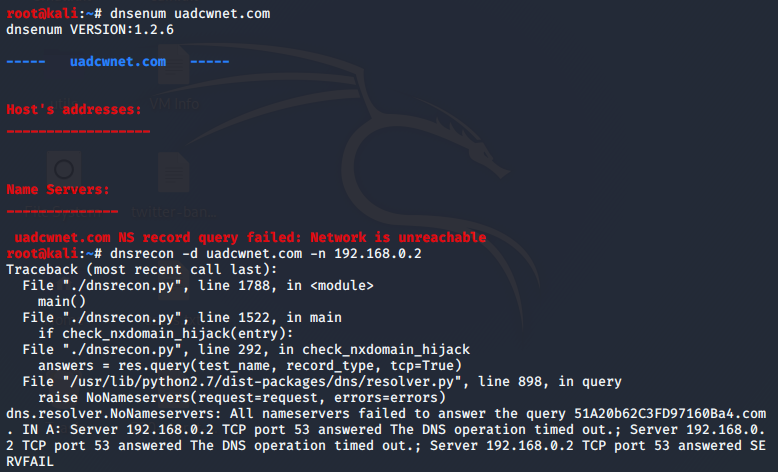


(Fig 7. Server 2 UDP Nmap scan results)

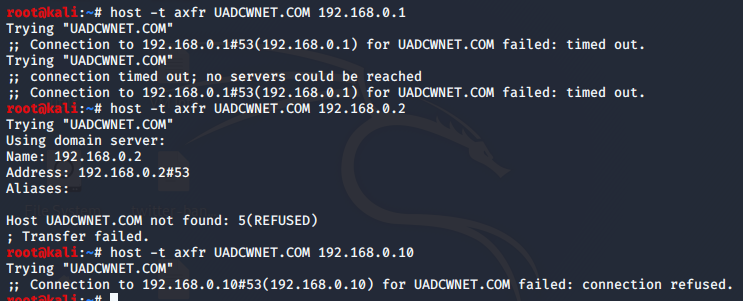
Server 1 results show fewer open ports, suggesting the server was locked up tighter against outside attacks and port vulnerabilities.

(Fig 8. Server 1 TCP Nmap scan results

## Enumeration

Enumeration results were largely underwhelming, revealing no new information as all enumeration attempts were blocked by the servers, resulting in ‘timeout’ and ‘connection refused’ errors. Various programs were used, and they all returned the same errors.

(Fig 9. DNSenum results show timeout errors when used against the domain)



(Fig 10. Using the host AXFR command to view all hosts on the network resulted in a refusal from the server)

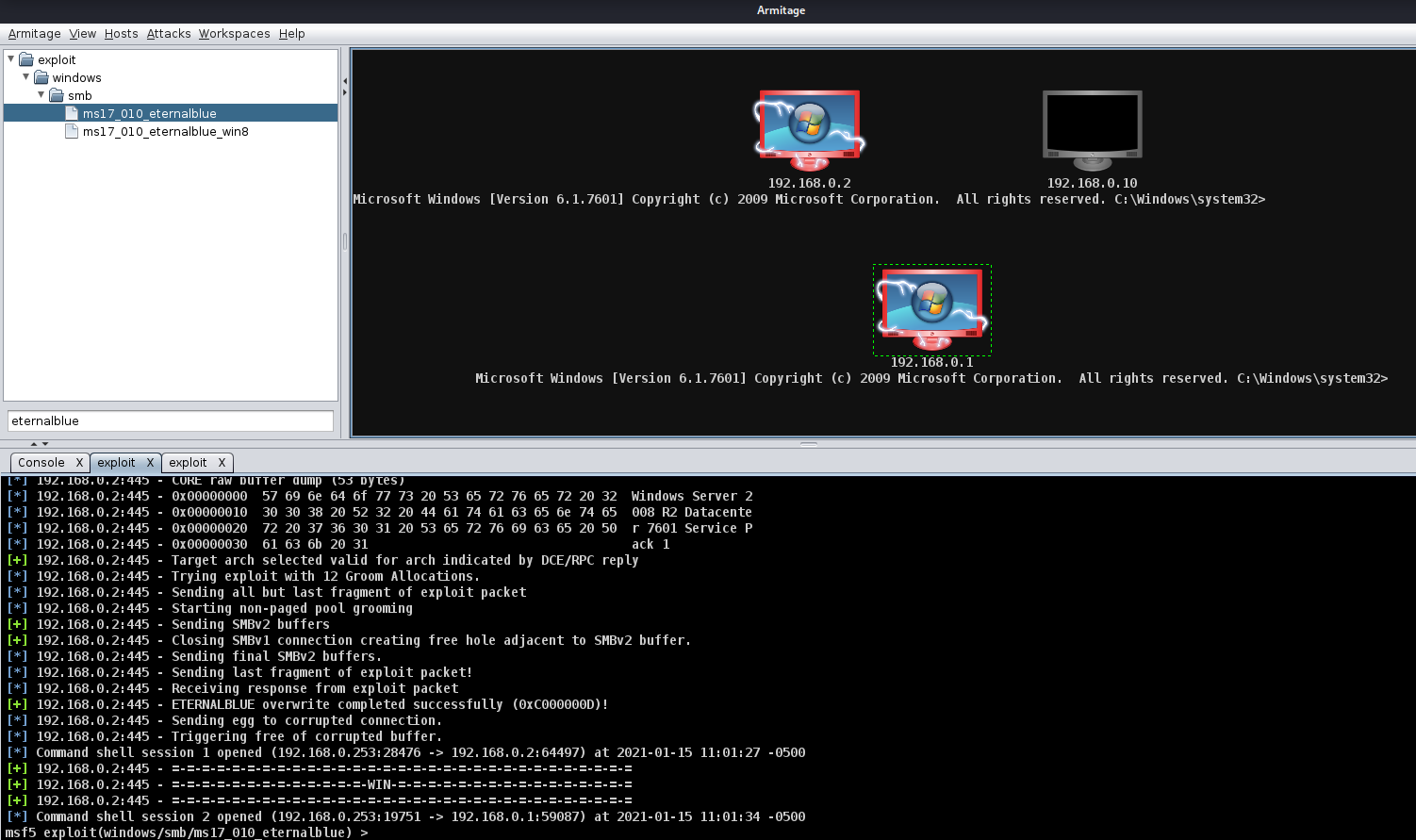
The results of the remaining enumeration scans (enum4linux, polenum, NSlookup) are located in Appendix 1, 2, and 3.

## System Hacking

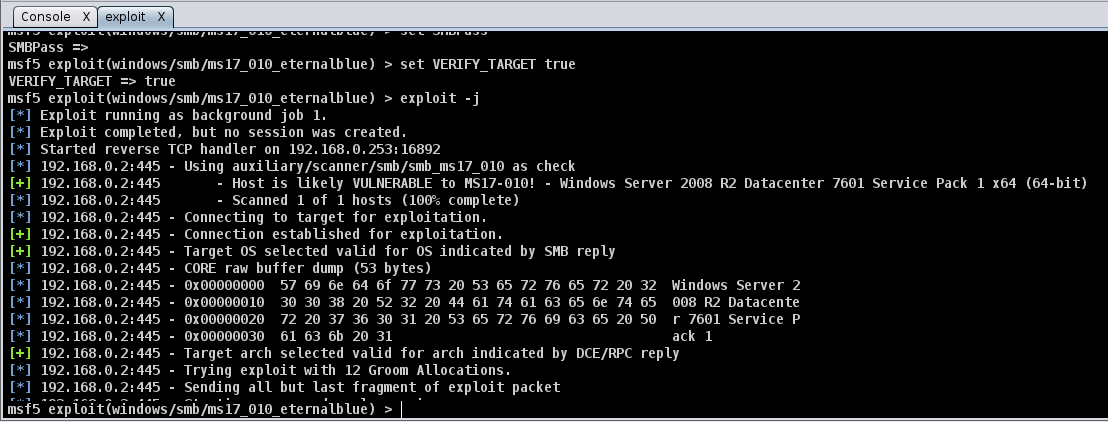
As the servers were vulnerable to Eternalblue (due to their outdated operating system) the first course of action was to launch Armitage and use its exploit search function to use it against one of the servers. Both servers were exploited, but all following examples are from Server 2 as no new or sensitive information was found on Server 1.

After launching Armitage and adding all network IP addresses as hosts, the exploit was located in the program’s database, and executed against the servers. The red effect on the icons shows the systems had been compromised by the exploit, and the window on the bottom shows the exploit running.

Using this same exploit-searching method, shell-to-meterpreter was executed to allow quick, easy access to the servers.



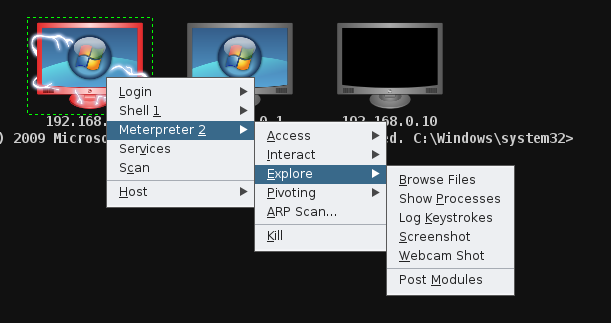
(Fig 11. Armitage showing the two servers are compromised)



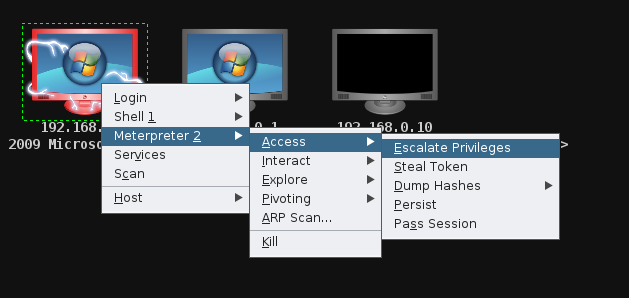
(Fig 12. Armitage’s Command prompt showing that the server is vulnerable to MS17-010 (EternalBlue))

Using shell-to-meterpreter’s menus allowed for many different attacks, from escalating privileges to taking a screenshot from any connected webcam, or even of the screen.

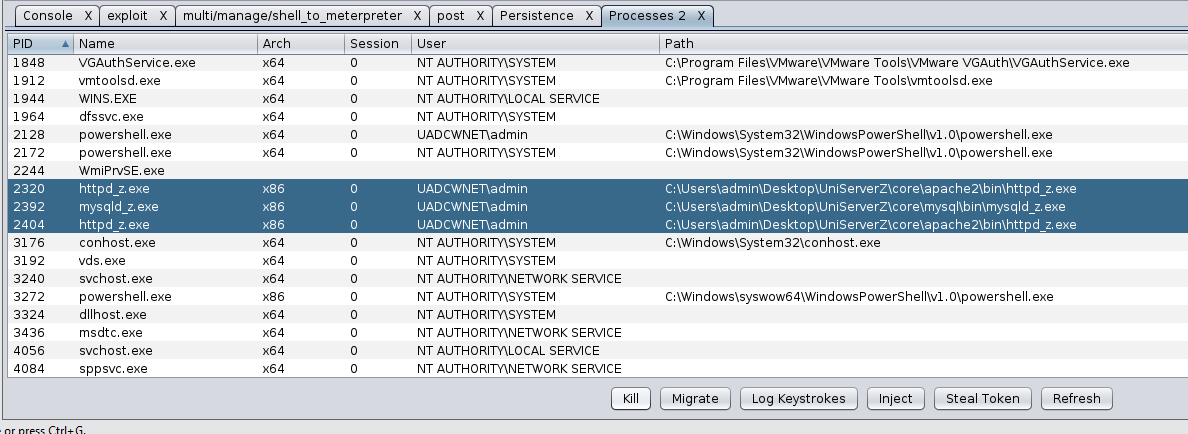
From the two examples below, only Browse Files, Show Processes, Persist, and Escalate Privileges were chosen to allow for easy browsing of the server’s file system and ease of use should the Kali machine be turned off or restarted - by using a backdoor left by the Persist option.



(Fig 13. A view of shell-to-meterpreter’s ‘Explore’ menu)

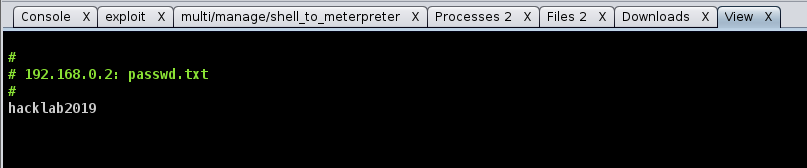
.

(Fig 14. Meterpreter’s ‘Access’ menu options)

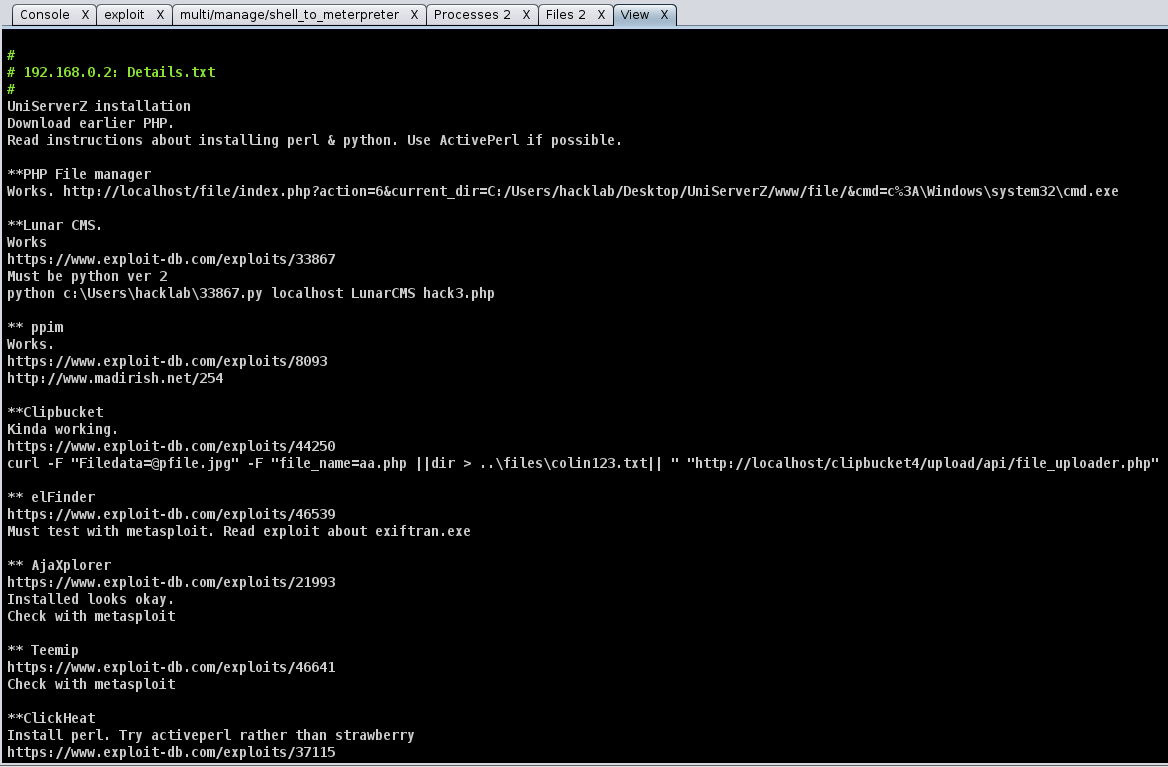
Viewing the server’s running processes showed that the Apache server running was named UniServerZ and sat on the desktop, which could further be examined for any useful files. Note the ‘Kill’ option which would allow an attacker to turn the process off immediately and would be abused by anyone trying to bring the server down. For the purposes of demonstration, the server was not killed in the event more useful data could be extracted from it.

(Fig 15. A view of server 2’s running processes)

Navigating the server’s folder revealed two sensitive files. One, named ‘passwd.txt’, which contained the password to the server itself, and another, named ‘details.txt’. The latter contained a long list of exploits the server was potentially vulnerable to. Both files would be of great use to an attacker, allowing for further, potentially more sophisticated and dangerous attacks to take place.

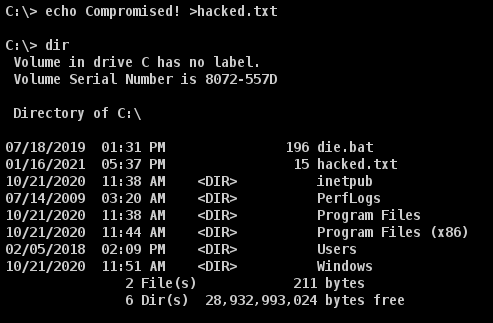


(Fig 16. Passwd.txt contents)

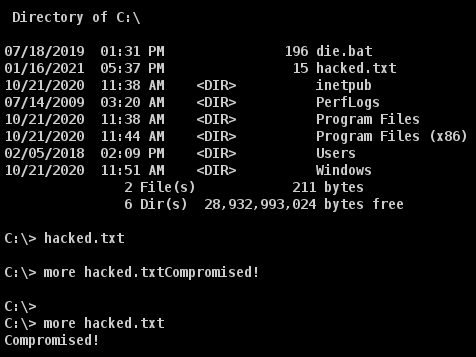


(Fig 17. Details.txt)

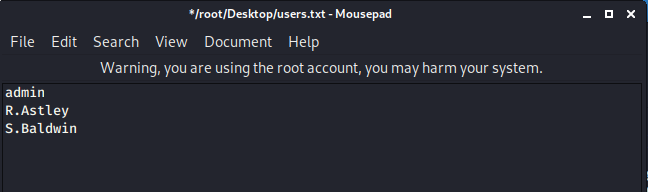
To further prove the severity of the situation, the vulnerabilities used allowed for text files to be created and read on the server, demonstrated below by placing a file named ‘hacked.txt’ onto the server’s drive, and reading it from the command line screen in Armitage. Various folders were navigated on both servers across every drive, but the only sensitive information that was gathered were the server text files.



(Fig 18. Creating a file on the drive)



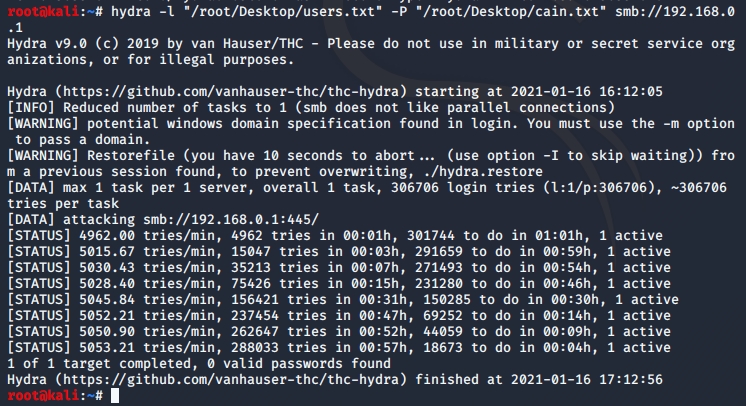
(Fig 19. Reading the file)

Finally, the usernames found in the Footprinting stage were put to use in a small text file on the Kali machine, which would then use Hydra to compare these usernames to the list of 300,000 passwords.

(Fig. 20. A small text file containing the usernames found to be used in Hydra)

The password cracker was then started, using the username text file as input for the possible usernames and cain.txt for the possible passwords. However, 0 valid passwords were found suggesting none of the usernames’ passwords were present in the file.

As the time limit for the project was now reaching its end, a rainbow table was not able to be used to guess the passwords and neither could a password dump analysis from Armitage, though these would have been the very next steps to take.



(Fig 21. Hydra performing a password cracking operation against the usernames.)

# General Discussion

## Findings

From the findings it can be seen that the servers’ biggest weakness was their Operating system, Windows Server 2008 r2, which allowed for a complete network takeover, in turn achieving the aim of the investigation. Despite the fact Windows 2008 (Microsoft, 2020) and Windows 7 reached the end of their support cycle in January 2020 a year ago (Microsoft, 2020), meaning the operating systems would no longer receive any updates or security patches of any kind, companies insist on using them because upgrading to a supported OS is too time consuming, too costly, and in cases like the NHS, would cause vital infrastructure to either turn off or require large amounts of backup computers to run while the main ones are being updated. A study done in 2019 by cybersecurity giants Kaspersky shows that over 40% of users continue to use unsupported, vulnerable operating systems, including small and medium-sized businesses (Kaspersky, 2019). This creates a huge security risk for businesses and individuals as hackers will continue to search for vulnerabilities once software reaches the end of its life to help them perform more dangerous and sophisticated attacks against it in the future.

On the 12th of May 2017, the NHS suffered a particularly dangerous ransomware attack (WannaCry) using EternalBlue to conduct the attack as demonstrated above (Acronis, 2017). The ransomware spread through their N3 network and ended up costing the service a crippling £92 million to clean up and finally upgrade to currently supported operating systems. The NHS was found to have been using Windows XP, an OS that is 17 years out of date, making them particularly vulnerable to outside attacks (Cision, 2017). This attack prompted Microsoft to release an emergency patch to various unsupported operating systems (Surur, 2017) as a way to prevent the virus from spreading again, though no company or individual should ever rely on companies like Microsoft or Apple to upgrade their software in such a fashion so long after it is officially no longer supported as there’s always the chance that once an OS is deemed unsupported, its creators will really mean it.

Using meterpreter-to-shell allowed for easy navigation of the network’s files, allowing attackers to completely hijack or even kill the network. This poses a notable security risk as any sensitive data could easily be taken from these computers, like password lists demonstrated in the procedure, as well as any other vulnerable files like account databases, reports, even transaction data depending on the information stored on the servers. Should the computer be in use, functions like the webcam snap and screenshot could be used to gather further information about the company and its users, including faces, office layout, logins, and any other sensitive information which could be displayed onscreen.

The lack of network encryption allowed for the client PC to inspect network packets via Wireshark, which revealed the PC names, domain names, and IP addresses, giving insider attackers information which could be abused to create an accurate network map, similar to that demonstrated in Figure 1. This gives the attackers an advantage in future stages of attack, as they have a better idea of what computers are present, where they are, and what their purpose is.

A poor firewall setup resulted in ping packets being accepted, which could have been exploited to create a list of times the servers are online or offline, or even perform an ICMP flood attack, using pings to bring the network down without the need for exploits like shell-to-meterpreter’s ‘kill’ function. These are called DDoS (Direct Denial of Service) attacks and are one of the most common and easiest attacks performed by hackers to bring down sites and servers. A study by Cisco shows that the number of DDoS attacks performed in 2019 reached 9.5 million, with estimated figures reaching 15.4 million by 2023 (Cisco, 2020).

No backup server was found for UniServerZ, meaning if the server was taken down, users would not be able use its services, prompting a halt to productivity as users would have to wait for it to be restarted, which could take hours. For some companies, this would cause a dive in profits, with the potential to ruin the public’s trust, preventing users from using the site again which would lead to a further fall in profits gained.

Nmap scans revealed various open ports, which can further improve an attacker’s understanding of the network and how its servers behave. Allowing ports to be shown also increases the risk of accidentally showing vulnerable ports, like RDP which would allow a user to use windows’ remote desktop tool to view the files on the network.

Administrator and user accounts should be hidden wherever possible to hide the names of anyone using the network. Knowing the Administrator’s username allows for many more opportunities of attack for the hackers, including password cracking as demonstrated in the System Hacking phase.

No valid passwords were found in cain.txt for any of the user accounts which was a good sign, as it shows the users have taken care to create complex, uncommon passwords which should be enforced by the server’s Password and Lockout policies.

Attempting to use RDP to control the server resulting in failure, again showing that this was either disabled in the firewall or allowed only for administrator accounts. Extra care must be taken to ensure ports like RDP are closed for outside connections and available only for a select, trustworthy few like Network administrators such that no malicious user can abuse the protocol to learn about the network in a malicious fashion.

In conclusion, the penetration test was a success, fulfilling the defined aim of entering and controlling the target network, and proving the network was unsafe for use. This was done by exploiting servers’ operating system’s vulnerability to EternalBlue, which allowed quick and easy access to the network PCs after successfully scanning the network for any hints and vulnerabilities.

### Adherence to standards

All actions performed on the network were performed with permission from the target, adhering to the following laws and regulations.

* Computer Misuse Act 1990 (UK Government, 1990)
* UK Data Protection Act 2018 (UK Government, 2018)
* Human Rights Act 1998 (UK Government, 1998)
* Police and Justice Act 2006 (UK Government, 2006)
* General Data Protection Regulation 2017 (EU Parliament, 2016)

## 3.2 Countermeasures

The following countermeasures should be introduced as soon as possible for the security of the network and the safety of all its users.

### Footprinting and Scanning prevention:

* Close down any unnecessary ports that could be used or abused by attackers to learn sensitive information about the network in the firewall settings. For inbound requests, consider the following.

Port 19 (Chargen, abused in DDoS attacks to amplify damage) (University of Illinois, 2020)

Port 123 (Network Time Protocol, open to DDoS attacks) (Various Authors, 2021)

Port 135 - 139 (NetBIOS, which can give information about the server and its files)

Port 445 (File sharing)

Port 23 (Incoming telnet connections)

Port 22 (Incoming SSH connections)

Port 3389 (Remote Desktop)

Ports 7000, 7001, 7002, 7003, 7004, 7016 (Prevents port scans and host sweeps) (Trend Micro, 2017)

As well as any other ports which are not necessary for the network.

* The use of a VPN and network encryption can also prevent ARP scans (or ARP poisoning) from revealing IP and MAC addresses. VPNs will route any network traffic through a far away server to mask the company’s own IP address, and network encryption, like IPSEC and SSH, will encrypt any network travelling around the network, making it much more difficult to capture using programs like Wireshark.
* Packet filters can be used to block or remove packets the program deems unsafe or suspicious, further enforcing the security of the network. (Lake, 2019)

### Enumeration

* When an incorrect login is given, ensure the error message is as generic as possible (for example, ‘Incorrect login’) to avoid giving attackers any hints about what exactly is incorrect. Do not display if a username or password is already taken, and check that no usernames are displayed when using any sort of “Forgotten Password?” feature. (Hacksplaining, 2021)

### System Hacking

* Update the machines to use the latest, currently supported operating systems. For example, update the two servers to use Windows Server 2016 and the client to Windows 10 Pro. Ensure all the latest patches are being installed, preferably as soon as possible, whether that be automatically or checked and updated overnight each day.
* Produce password and lockout policies in the active directory manager to ensure absolutely every user account has a complex, secure password that is to be updated at least every 3 months. Remind users not to place passwords in any files on the PC or places like sticky notes under the mouse mat or any easy-to-get piece of paper with lists of passwords. It is also recommended to test and teach employees about their security knowledge, with tests occurring every few months to keep up to date with current security trends. Leaving magazines or posters in any sort of reading area or cafeteria is NOT a valid teaching practice.
* Change the password to any servers every 3 months, abiding by the password policy.
* Ensure servers have backup implementation, allowing them to continue working even if the main servers have failed.

## 3.3 Improvements and Changes

Given more time and resources, the following would have been implemented:

* The use of a larger password text file (1 million – 10 million entries), and in the event that does not find the correct details, a rainbow table to run until the necessary details are found to prove that just because a login is not present in a ‘top passwords’ list does not mean it is safe to use.
* A physical network scenario instead of a virtual one to prevent several issues from arising (machine not accepting logins after restart), which would also have been more realistic to real world examples of penetration tests.
* More research into vulnerabilities associated with the various open ports, programs, and systems in the network machines, to allow for more attacks and exploits being used against the machines.
* The use of a more sophisticated vulnerability exploitation program to allow for more options for attacks and more control over the attacks themselves, rather than using the simplified GUI-based Armitage.
* Testing Armitage’s ‘kill’ option, which was discussed but never put to use. This would have allowed for a demonstration of what it is like to try and log into a shut-down server.
* Investigation into why the servers were so stubborn to enumerate, by gaining access to the servers’ firewall and policy programs.
* Attempting to open RDP port 3389 to allow for a clear view of what the server looks like to an administrative user and navigating its folders without any “Access denied” errors.
* Producing a comprehensive teaching outline for businesses to use to teach workers about online safety to prevent phishing and social engineering attacks, as well as improving general knowledge about the subject.

# Bibliography

Acronis, 2017. *The NHS cyberattack.* [Online]   
Available at: https://www.acronis.com/en-gb/articles/nhs-cyber-attack/  
[Accessed 19 January 2021].

Bowes, R., 2015. *Passwords - SkullSecurity.* [Online]   
Available at: https://wiki.skullsecurity.org/Passwords  
[Accessed 19 January 2021].

Cisco, 2020. *Cisco Annual Internet Report (2018–2023) White Paper.* [Online]   
Available at: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html  
[Accessed 19 January 2021].

Cision, 2017. *Thousands of Organizations Run the Majority of their Computers on Outdated Operating Systems, Nearly Tripling Chances of a Data Breach.* [Online]   
Available at: https://www.prnewswire.com/news-releases/thousands-of-organizations-run-the-majority-of-their-computers-on-outdated-operating-systems-nearly-tripling-chances-of-a-data-breach-300470678.html  
[Accessed 19 January 2021].

EU Parliament, 2016. *General Data Protection Regulation.* [Online]   
Available at: https://gdpr-info.eu/  
[Accessed 19 January 2021].

Hacksplaining, 2021. *Preventing User Enumeration.* [Online]   
Available at: https://www.hacksplaining.com/prevention/user-enumeration  
[Accessed 19 January 2021].

Intersoft Consulting, 2016. *GDPR.* [Online]   
Available at: https://gdpr-info.eu/  
[Accessed 19 January 2021].

Kaspersky, 2019. *The long goodbye: 41% of consumers still use unsupported and near end-of-life OS..* [Online]   
Available at: https://www.kaspersky.com/about/press-releases/2019\_consumers-still-use-unsupported-and-near-end-of-life-os  
[Accessed 19 January 2021].

Lake, J., 2019. *ARP poisoning/spoofing: How to detect & prevent it.* [Online]   
Available at: https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent/  
[Accessed 19 January 2021].

Lund, J., 2021. *What is GDPR and How Does It Impact Your Business?.* [Online]   
Available at: https://www.superoffice.com/blog/gdpr/  
[Accessed 19 January 2021].

Microsoft, 2020. *Support for Windows 7 has ended.* [Online]   
Available at: https://www.microsoft.com/en-gb/microsoft-365/windows/end-of-windows-7-support  
[Accessed 19 January 2021].

Microsoft, 2020. *Support for Windows Server 2008 has ended.* [Online]   
Available at: https://www.microsoft.com/en-us/cloud-platform/windows-server-2008  
[Accessed 19 January 2021].

Proofpoint, 2017. *The Great Disconnect (Perception and Reality of GDPR readiness in the UK, France, and Germany),* Sunnyvale, California: Proofpoint.

Surur, 2017. *Microsoft release Wannacrypt patch for unsupported Windows XP, Windows 8 and Windows Server 2003.* [Online]   
Available at: https://mspoweruser.com/microsoft-release-wannacrypt-patch-unsupported-windows-xp-windows-8-windows-server-2003/  
[Accessed 19 January 2021].

Trend Micro, 2017. *How do I block NMAP port scans?.* [Online]   
Available at: https://success.trendmicro.com/solution/TP000087920-How-do-I-block-NMAP-port-scans  
[Accessed 19 January 2021].

UK Government, 1990. *Computer Misuse Act 1990.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents  
[Accessed 19 January 2021].

UK Government, 1998. *Human Rights Act 1998.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents  
[Accessed 19 January 2021].

UK Government, 2006. *Human Rights Act 2006.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/2006/48/contents  
[Accessed 19 January 2021].

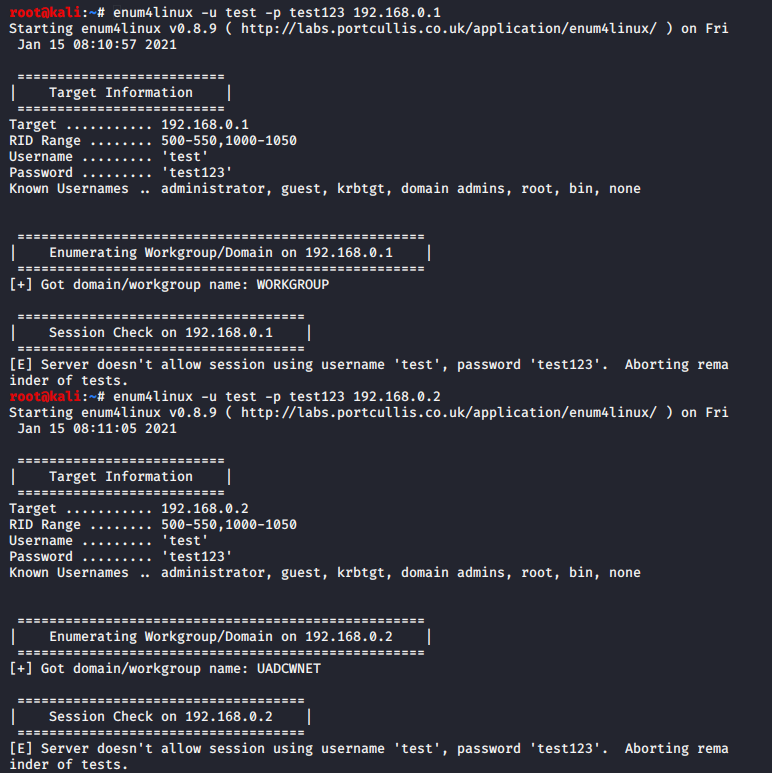
UK Government, 2018. *Data Proteciton Act 1998.* [Online]   
Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted  
[Accessed 19 January 2021].

University of Illinois, 2020. *Networking, Firewall, Vulnerable Networking Ports Blocked.* [Online]   
Available at: https://answers.uillinois.edu/illinois/page.php?id=47646  
[Accessed 19 January 2021].

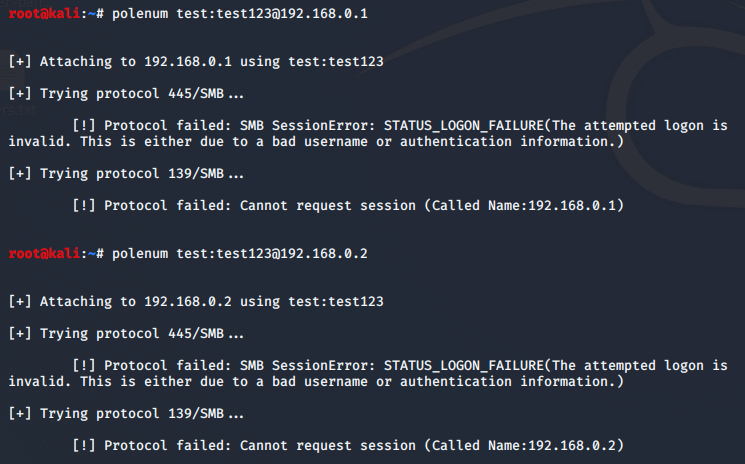
Various Authors, 2021. *Vulnerability list: NTP.* [Online]   
Available at: https://www.cvedetails.com/vulnerability-list/vendor\_id-2153/NTP.html  
[Accessed 19 January 2021].

# Appendices

Appendix 1: enum4linux enumeration scan giving back very little information.



Appendix 2: Polenum returning no policies during enumeration



Appendix 3: NSlookup zone transfer failure

