Abertay University

Company Network Investigation

Name: Jacek Jajko

ID: 1705032

Module Code: CMP210

Module Title: Ethical Hacking 1

Academic year: 2020/21

Abstract

Penetration testing is one of the basic ways to protect information systems from attacks by intruders. The purpose of the tests is to identify as many vulnerabilities and shortcomings as possible that may pose a threat to the security of the organization's ICT infrastructure.

This document shows the methods and tools that were used in the information gathering process. Our discoveries are alarming.

These findings have significant implications for the company. It appears that the network is insecure and there are many vulnerabilities which can be exploited by an attacker.

Contents

Introduction

The latest report of the World Economic Forum entitled “Regional Risks for Doing Business 2019” indicates that cyber risk remains the largest identified risk of doing business across Europe. (Regional Risks for Doing Business, 2019)

The costs of cyber-attacks are increasing every year. This is due to the data contained in both the report "Economic Impact of Cybercrime - No Slowing Down" (The Economic Impact of Cybercrime— No Slowing Down, 2018), prepared by the Center for Strategic and International Studies (CSIS) in cooperation with the cybersecurity company McAffe and the report "Cost of Cyber Crime Study " (THE COST OF CYBERCRIME, 2019), prepared by Ponemon Institute in cooperation with the consulting company Accenture.

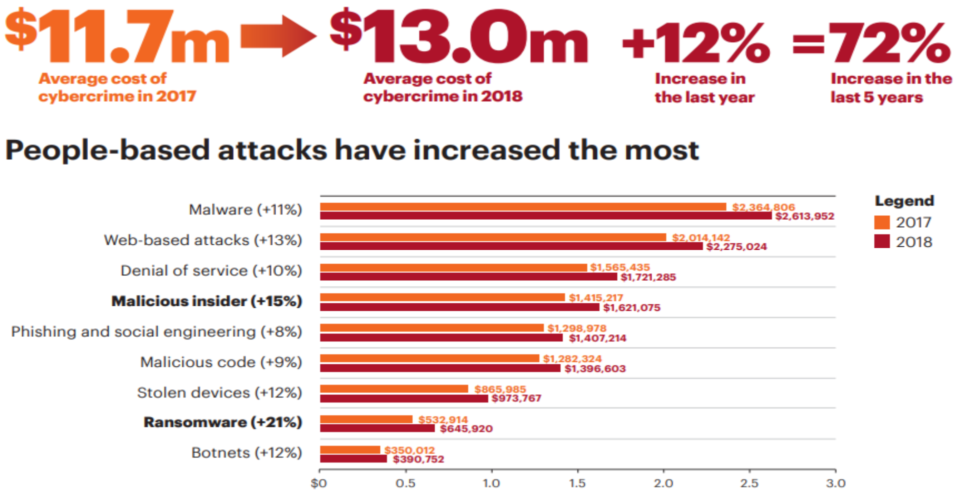


Figure 1 Accenture, (2020), Cost of cybercrime is rising

Our company was contracted to conduct a penetration test on a client’s network in order to evaluate the level of resistance and susceptibility of the ICT system to attempts to break through the barriers protecting it. Penetration tests make it possible to assess the risk associated with technical problems and weaknesses of the system or equipment and allow it to verify the correctness of the ICT system configuration. You must bear in mind the fact that hackers do not have a fixed working time, and anyone can be the target of their attacks, regardless of whether it is a large corporation, a small company, or an individual.

The purpose of this document is to create a detailed outline of identified security risks with all the technical aspects of each finding, cover the tools and methods used to perform the test.

Confidentiality Statement

This document is the exclusive property of X Company and Red Team. This document contains proprietary and confidential information. To use, duplicate or redistribute this document in any form, consent is required both from X Company and the Autor.

The X Company may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance as some of the information security standards regularly require monitoring, testing networks, security systems, and processes.

Disclaimer

The findings and recommendations made in this document are made based on information gathered during the assessment.

Penetration tests are limited to providing a security snapshot of the point in time in which they are conducted; therefore, it is advised to regularly perform an evaluation of network security to ensure there is no weakness an attacker would easily exploit.

Contact Information

Name	Title	Contact Information
Demo Company		
Name Surname	Senior IT Technician	Office: 05555 123456 Email: demo@demo.co.uk
Red Team		
Jacek Jajko	Penetration Tester	Office: 05555 123456 Email: 1705032@uad.ac.uk

Assessment Overview

Red Team was asked to evaluate the security risks of the Demo company network. We have allocated 25 hours to carry out an investigation. Penetration testing consists of conducting a controlled attack or diagnosis on an information network, website, service, or web application in order to detect vulnerabilities, configuration errors, and security holes. (Definition of a penetration test, 2017)

Penetration tests may be performed:

from outside the organization - usually carried out over the Internet, they best reflect an attack that can be carried out by any Internet user

from inside the organization - they provide a full picture of threats; they also indicate threats from their own employees.

In this assessment, we are focused on performing the penetration tests from inside the organization. We have been provided with a pent tester account for our own use.

In each project, we can distinguish general stages of penetration testing:

- Determining the scope of the tests
- Performing the initial analysis and recognition of the test subject
- Vulnerability identification
- Verification and exploitation of identified vulnerabilities
- Development of recommendations and reporting

(A Complete Guide to the Phases of Penetration Testing - Cipher, n.d.)

Common Vulnerability Scoring System

The **Common Vulnerability Scoring System** (**CVSS**) is a universal way to convey vulnerability level and help determine urgency and priority of responses by providing a numerical score which reflects its severity. (Common Vulnerability Scoring System version 3.1 User Guide, n.d.)

CVSS is currently used by the most popular vulnerability databases (NVD, OSVDB, VUPEN, Secunia) and vulnerability scanners (Qualys, CORE Impact, **Nessus**, IBM Internet Scanner).

Severity	CVSS Score Range	Definition
Critical	9.0-10.0	Indicates vulnerability which exploitation allows to compromise the target and gain a remote access to the machine. The exploitation is often straightforward. Vulnerabilities marked as 'critical' must be fixed urgently.
High	7.0-8.9	Indicates vulnerability which exploitation is more difficult than the "critical' ones and the negative effects are slightly limited. It still allows to gain access to high-value data, and it should be fixed as soon as possible.
Moderate	4.0-6.9	This type of vulnerability is not exploitable, or exploitation might occur depending on external factors like social engineering. It is advised to approach and patch this type of vulnerabilities once the most important problems have been fixed.
Low	0.1-3.9	This type of vulnerabilities typically has very low impact. Exploitation of such usually requires a physical access to the machine.
Informational	N/A	Issues marked as "INFO" are not security vulnerabilities. They are informing about items noticed during testing.

Scope

Assessment	Details
Internal Penetration Test	192.168.0.0/24 Network 192.168.0.1/24 Server1 192.168.0.2/24 Server2 192.168.0.10/24 Client

Scanning

Conducting a penetration test requires the use of appropriate tools that are helpful in activities aimed at discovering as much information about the system as possible that can be used at a later stage of the test. This section contains a brief description of the various tools used during this assessment together with findings regarding security issues.

Kali Linux is a Debian-based operating system distribution that has many tools that are extremely useful for conducting penetration testing. (What is Kali Linux? n.d)

Nmap

The very first tool that is used during a penetration test is **Nmap** - ("Network Mapper") is an open-source network exploration and security audit tool. It is designed to scan large networks but also works well for single addresses. Nmap uses low-level IP packets to discover which addresses are available on the network, which services provide (application name and version), what operating systems they run on (system version), what types of firewall systems are used, and dozens of other features. Nmap is widely used for security audits, and many network and system administrators use it to perform routine tasks such as inventorying network resources, managing software updates, and monitoring systems and their uptime. (Nmap: the Network Mapper - Introduction, n.d.)

Scans performed

- Used to discover open ports; “(-sS)”
- Enables OS & version detection; “-T4(Aggressive (4) speeds scans) -A(os detection) -p(discovered open ports)”
- Used to compare with **Nessus** results; “--script vuln (scripts that checks for specific known vulnerabilities) “(see Figure 2, 3).

Results

- **Both** servers are running **Windows Server 2008 R2 SP1**
  On January 14, 2020, **support for Windows Server 2008 and 2008 R2 ended.** This marks the end of regular security updates. Final release Service Pack 1 with Platform Update or later update rollup (build 6.1.7601) / August 27, 2013; 7 years ago **(CVSS 10.0)**
- **Both** servers are vulnerable to **Remote Code Execution** by vulnerability in SMBv1. (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption, n.d.) **(CVSS 9.3)**

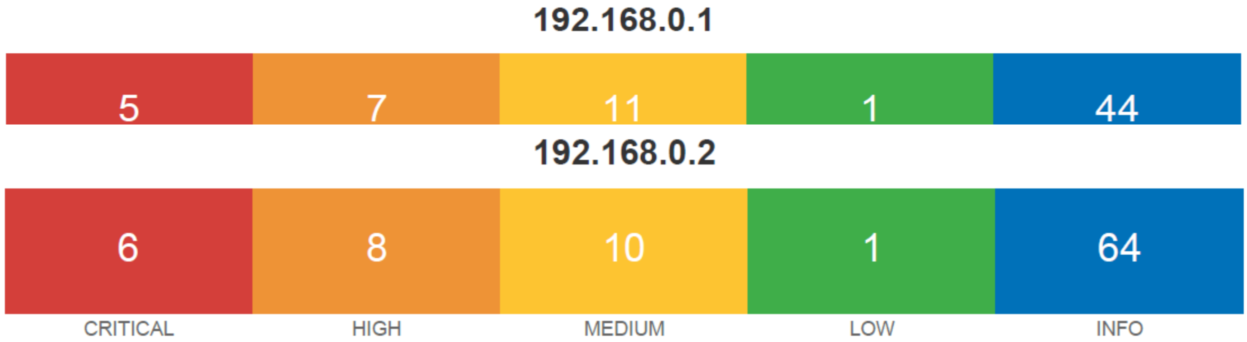
Nessus

One of the steps of the initial analysis was to perform a Nessus Scan.

Nessus Essentials, is a free version of the industry's most widespread vulnerability assessment solution, helps reduce your organization's attack surface and ensure compliance. The Nessus scanner offers fast asset discovery, configuration checks, target profiling, malware detection, sensitive data searching and much more.

Report generated after performing ‘basic network scan’ provided with user credentials (test\test123) by Nessus shows that there are multiple vulnerabilities on both servers.

Statistical breakdown of detected vulnerabilities



Results

Both servers are vulnerable to:

- *MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (**CVSS 10.0**)*
- *MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check) (**CVSS 10.0**)*
- *Microsoft DNS Server Remote Code Execution (SIGRed)(**CVSS 10.0**)*

Full report of Nessus scans (see Figure 4,5).

Enumeration

Enumeration is the process of finding valid user accounts or badly secured shared resources. Enumeration is an invasive technique. It involves active connections and targeted queries. Most of the information collected in this way usually seems trivial. However, they can be very dangerous. After obtaining the correct username or resource, it is only a matter of time before an attacker obtains the appropriate password or finds a vulnerability in the resource sharing protocol. (Enumeration (Attack Vectors), n.d.)

Findings

- *Weak password policy not meeting Microsoft password policy guidelines* (see Figure 6).
- *Web server allowing access to "zp-data "folder with security log file.* (see Figure 7).
- *Directory indexing found on web server.*
- Active Directory description field contains a password
- Password to the database has been found in configuration file inside shared folder.

Information found in the user accounts description

Password found in Active Directory description field!

Account: M.Mills	Name: Marty Mills	Desc: password:vbQ8CcW7BEVRzAS

Information found in shares

Password found in shares:

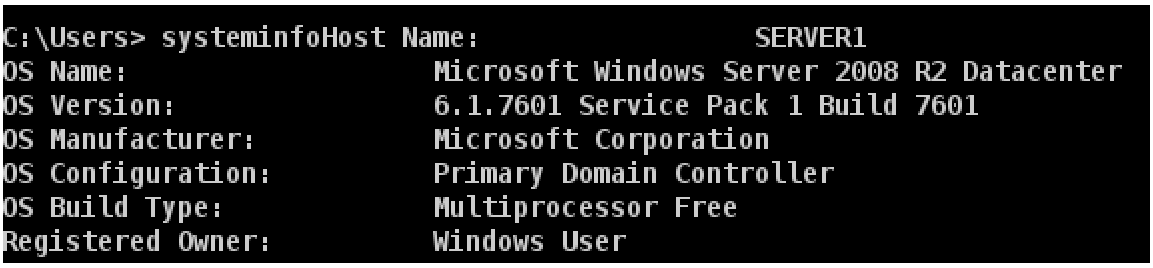
File: DatabaseAccess_MOD

Uid = pihj	PWD = Okcoge2103

Exploitation

This section contains information gathered during exploitation stage.

EternalBlue: Used to get a remote access on both servers. Allows **Remote Code Execution**



```
C:\Users> systeminfoHost Name:                SERVER1
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
```

PowerShell was used to upload a Mimikatz to the server.

Mimikatz: Used to extract NTLM password hashes from the memory and extract plain text passwords from Local Security Authority Subsystem Service process (mimikatz, 2014)

Password from LSASS:

Username : admin	Password : Thisisverysecret2020

John the ripper: password cracking tool included in Kali used to crack passwords. This tool was used to crack hashed passwords.

Not all the passwords have been cracked because it is a time-consuming process.

Username	Password
C.Griffin	devisee
S.Fleming	paramedic
K.Vaughn	ambulatory
D.Ingram	phenotype
C.Mendoza	nomogram
M.Carter	nomogram
S.Page	immense60
C.Morris	merrymake

Discussion

We were able to get a NT AUTHORITY\SYSTEM user access which is the most powerful account on a Windows local instance. It would not happen if the operating system was kept updated. We were able to discover passwords during the enumeration process. We were able to crack passwords using a dictionary attack due to the weak password being used. The password for the ‘admin’ account has been compromised.

The above information allows a potential hacker to gain complete access to the company's servers.

Recommendations

Windows Server 2008 is an old operating system no longer supported by Microsoft. The operating system must be kept up to date to reduce the risks associated with exploiting security vulnerabilities. We recommend the implementation of the Windows Server 2019 which is the latest version of the Windows Server OS by Microsoft. It can be an expensive solution, but it will ensure the security of the corporate network for future years.

Password protection is very important! Password policy should meet Microsoft password policy guidelines.

To ensure network security follow the basic rules:

- Replace the default passwords with unique ones
- Use different passwords for different accounts
- Keep your passwords safe and not write them down
- Create strong passwords with a combination of letters, numbers, and symbols

It is important to keep the administrator account safe. The built-in local Administrator should be used only during the initial setup. After that, it should be disabled. Windows Server should never be used with the default configuration. Microsoft has released a “Summary of Best Practices” which implementation can reduce most exploited vulnerabilities. Make sure you read this document.

Best practices should be considered when implementing any kind of service. This also applies to the Apache Web Server or any other type of server.

The weakest link in the security chain is the human element! Therefore, employees should be aware of the risk. To do this, provide them with training to increase their level of safety knowledge. As new cyberthreats are constantly dragging on, the training is continuous so that they are always known as sovereignty in the face of cyberattack danger.

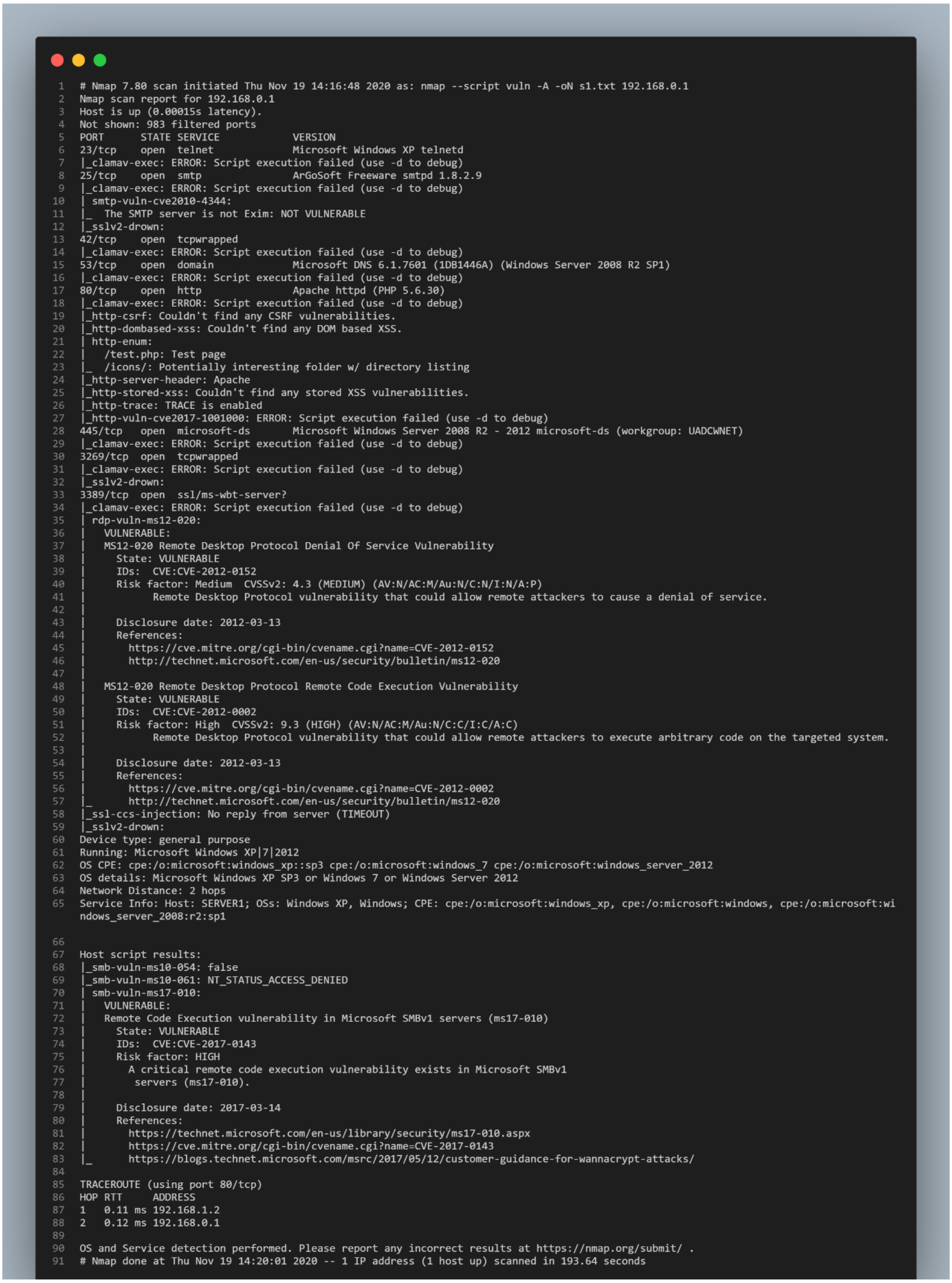
Conclusion

The company network is easily exploitable even by a person with a little knowledge. The main problem with the network was an outdated operating system which allowed us to gain full administrator access. Make sure your company's operating systems and applications are updated regularly. Thanks to this, security patches will be installed on an ongoing basis. Also, control the operation of anti-virus software and firewalls.

A cyberattack can have various consequences. The effect of such cybercrime may be, for example, a direct theft of real money, but also losses caused by a break in the functioning of the enterprise.

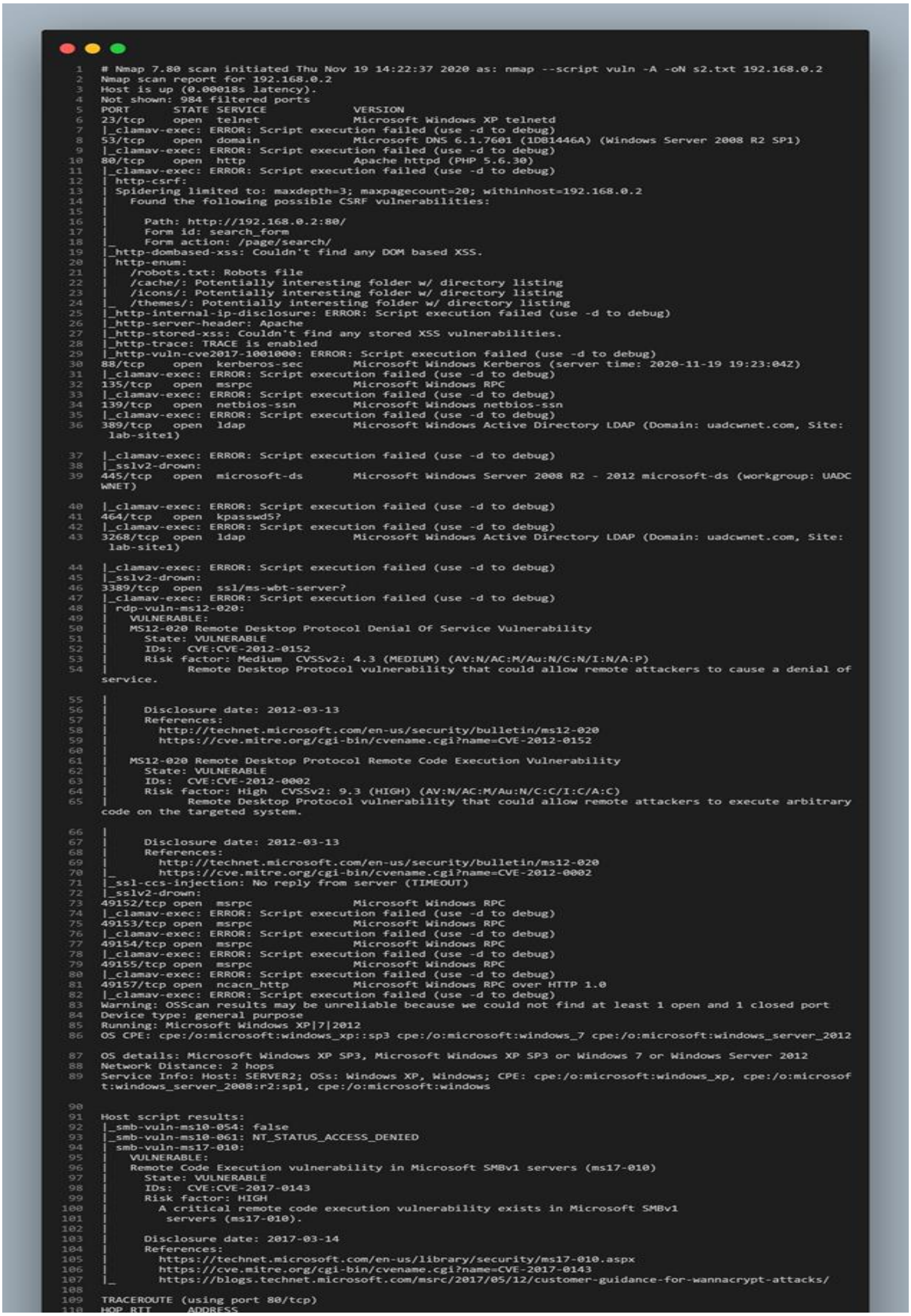
The best way to avoid such situations is to be careful and follow security rules before a cybercrime occurs. For full security, it is worth investing in the services of professionals - larger companies should have their internal department at their disposal, while medium and small enterprises can use outsourcing services.

APPENDICES



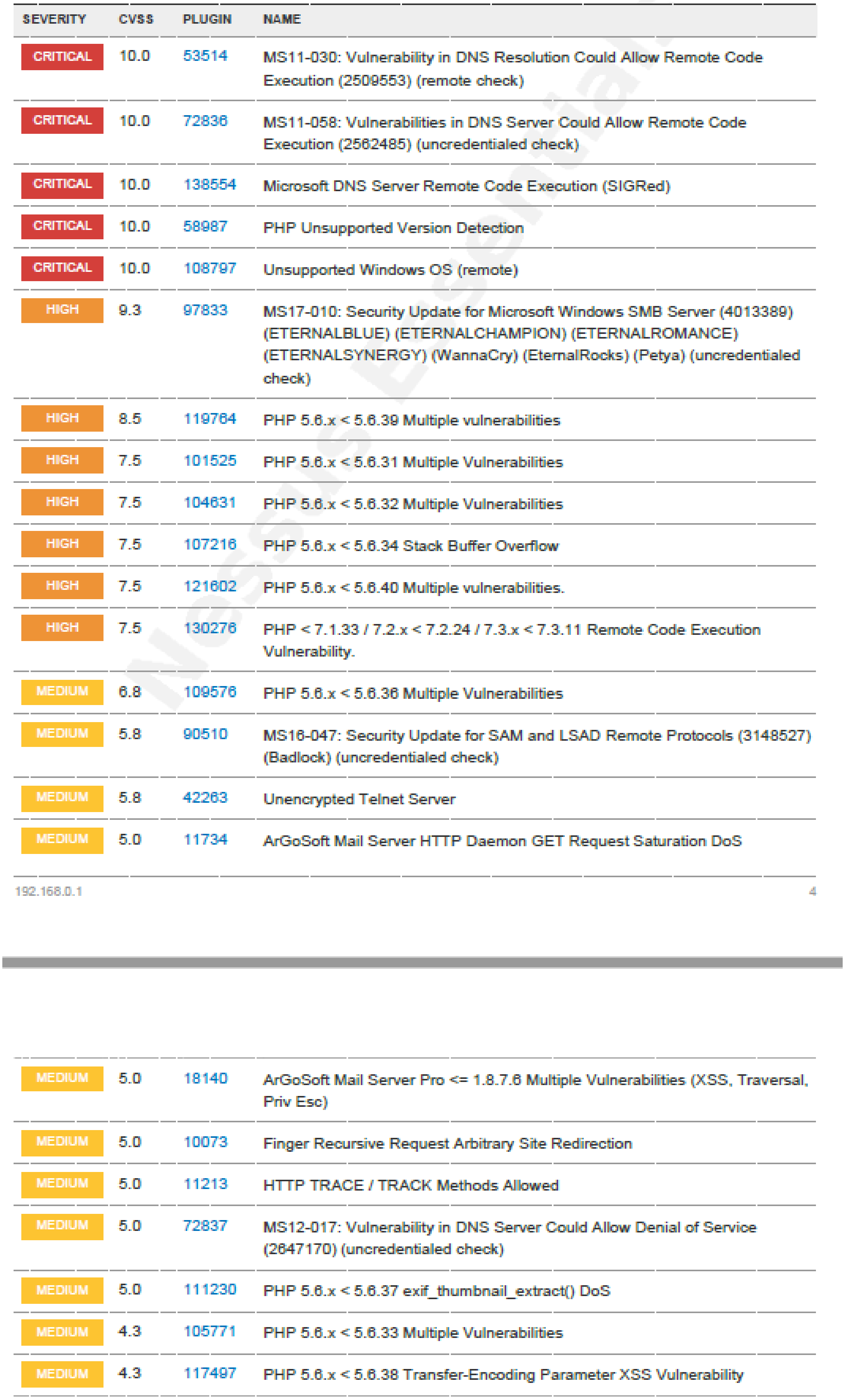
```
# Nmap 7.80 scan initiated Thu Nov 19 14:16:48 2020 as: nmap --script vuln -A -oN s1.txt 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up (0.00015s latency).
Not shown: 983 filtered ports
PORT      STATE SERVICE            VERSION
23/tcp    open  telnet             Microsoft Windows XP telnetd
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp    open  smtp               ArGoSoft Freeware smtpd 1.8.2.9
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
42/tcp    open  tcpwrapped
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp    open  domain             Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http               Apache httpd (PHP 5.6.30)
|_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-server-header: Apache
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  tcpwrapped
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3389/tcp  open  ssl/ms-wbt-server?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: Host: SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:microsoft:wi
ndows_server_2008:r2:sp1


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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.11 ms 192.168.1.2
2   0.12 ms 192.168.0.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Nov 19 14:20:01 2020 -- 1 IP address (1 host up) scanned in 193.64 seconds
```

Figure 2 Scanned Open Ports agains known vulnerabilities on Server1



```
# Nmap 7.80 scan initiated Thu Nov 19 14:22:37 2020 as: nmap --script vuln -A -oN s2.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up (0.00018s latency).
Not shown: 984 filtered ports
PORT      STATE SERVICE           VERSION
23/tcp    open  telnet            Microsoft Windows XP telnetd
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp    open  domain            Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http              Apache httpd (PHP 5.6.30)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.2:80/
|     Form id: search_form
|_    Form action: /page/search/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|   /cache/: Potentially interesting folder w/ directory listing
|   /icons/: Potentially interesting folder w/ directory listing
|_  /themes/: Potentially interesting folder w/ directory listing
|_http-internal-ip-disclosure: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time: 2020-11-19 19:23:04Z)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc             Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap              Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site:
 lab-site1)

|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADC
WNET)

|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3268/tcp  open  ldap              Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site:
 lab-site1)

|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3389/tcp  open  ssl/ms-wbt-server?
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of
service.

|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary
code on the targeted system.

|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
49152/tcp open  msrpc             Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  msrpc             Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  msrpc             Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  msrpc             Microsoft Windows RPC
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012

OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsof
t:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows


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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
```

Figure 3 Scanned Open Ports agains known vulnerabilities on Server2

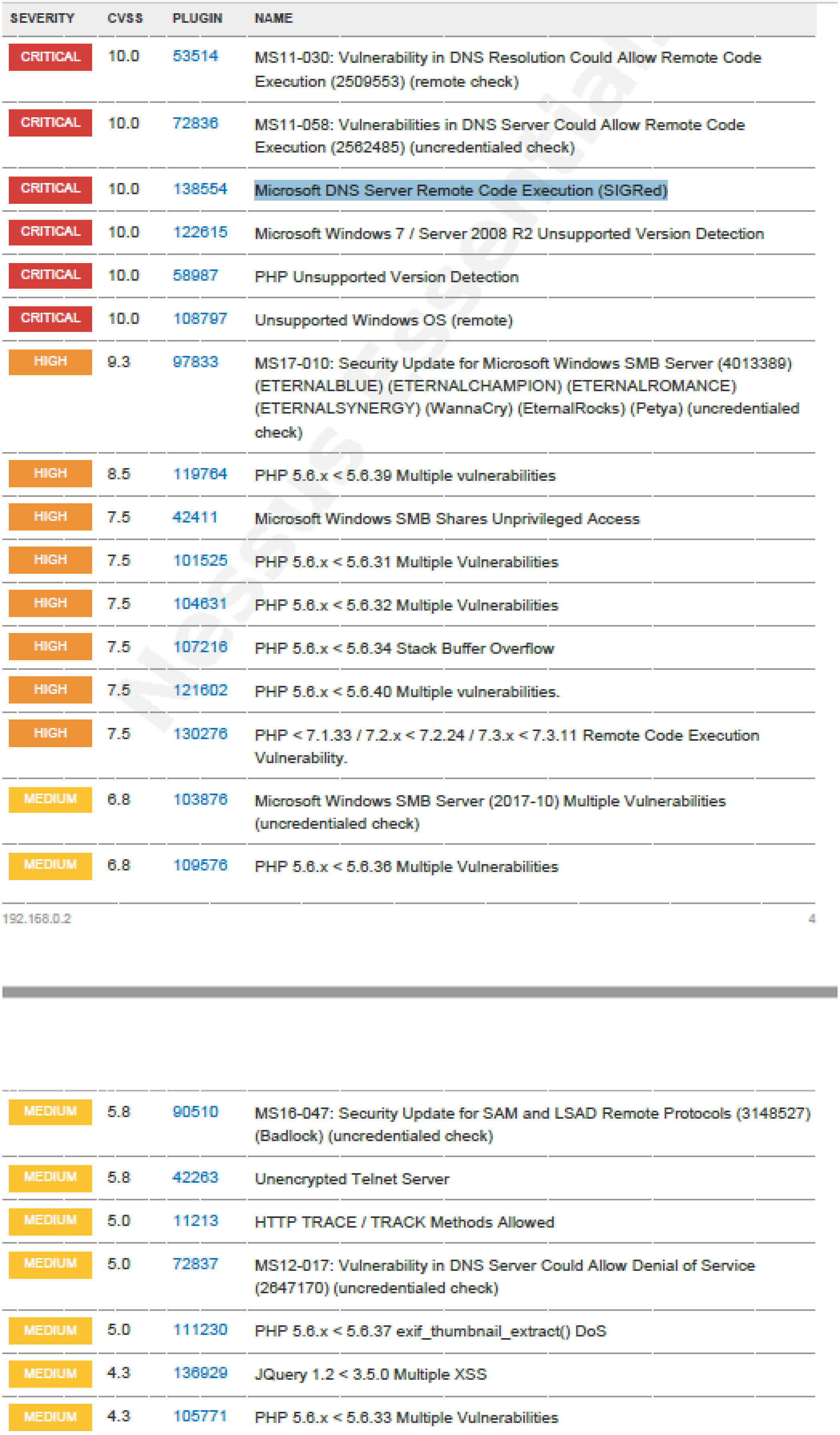


SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
HIGH	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11734	ArGoSoft Mail Server HTTP Daemon GET Request Saturation DoS

192.168.0.1 4

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	18140	ArGoSoft Mail Server Pro <= 1.8.7.6 Multiple Vulnerabilities (XSS, Traversal, Priv Esc)
MEDIUM	5.0	10073	Finger Recursive Request Arbitrary Site Redirection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability

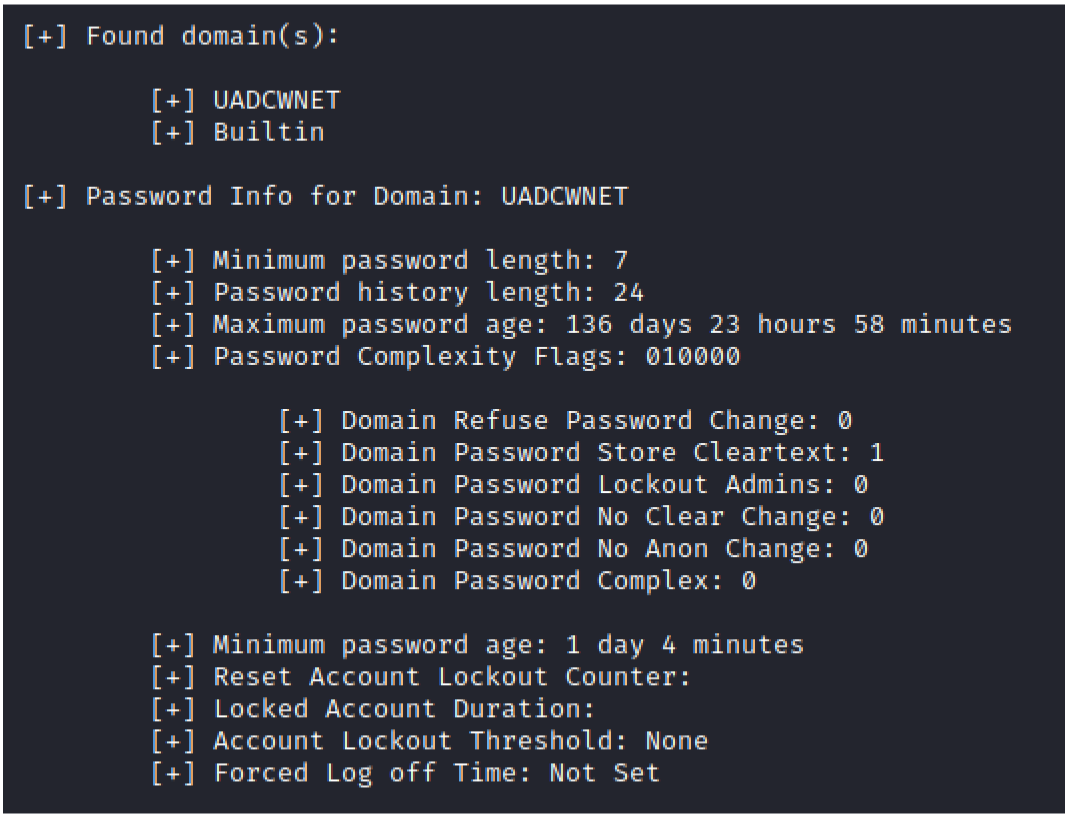
Figure 4 Nessus Server 1 scan report



SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	122615	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
HIGH	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
MEDIUM	6.8	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities

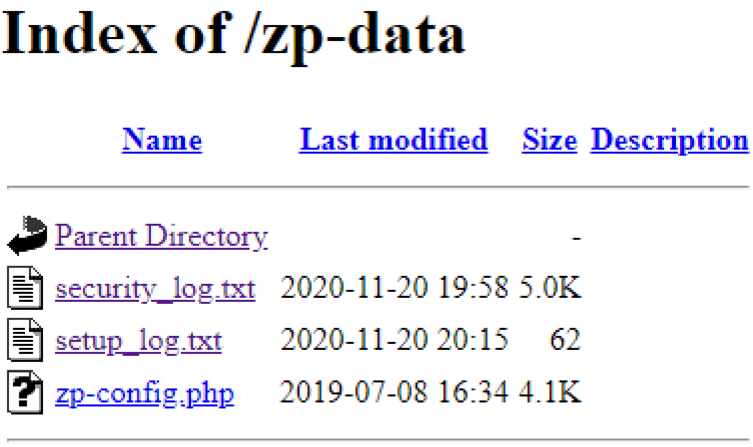
192.168.0.2 4

Figure 5 Nessus Server2 scan report



```
[+] 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 6 Password Policy



Index of /zp-data

Name	Last modified	Size	Description
Parent Directory		-	
security_log.txt	2020-11-20 19:58	5.0K	
setup_log.txt	2020-11-20 20:15	62	
zp-config.php	2019-07-08 16:34	4.1K	

Figure 7 Folder zp-data is public

References

Accenture.com. 2019. THE COST OF CYBERCRIME. [online] Available at: <https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50> [Accessed 15 November 2020].

Cipher. n.d. A Complete Guide To The Phases Of Penetration Testing - Cipher. [online] Available at: <https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/> [Accessed 17 November 2020].

Crest-approved.org. 2017. Definition Of A Penetration Test. [online] Available at: <https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf> [Accessed 13 November 2020].

Evolution-sec.com. n.d. Enumeration (Attack Vectors) | Penetration Testing, Security Audits, Security Checks, Analysis & IT Security Services - Hessen Kassel Deutschland. [online] Available at: <https://www.evolution-sec.com/en/products/enumeration-attack-vectors> [Accessed 22 November 2020].

First.org. n.d. Common Vulnerability Scoring System Version 3.1 User Guide. [online] Available at: <https://www.first.org/cvss/v3-1/cvss-v31-user-guide_r1.pdf> [Accessed 15 November 2020].

GitHub. 2014. Gentilkiwi/Mimikatz. [online] Available at: <https://github.com/gentilkiwi/mimikatz> [Accessed 22 November 2020].

Kali.org. n.d. What Is Kali Linux?. [online] Available at: <https://www.kali.org/docs/introduction/what-is-kali-linux/> [Accessed 13 November 2020].

Mcafee.com. 2018. The Economic Impact Of Cybercrime— No Slowing Down. [online] Available at: <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf> [Accessed 15 November 2020].

Nmap.org. n.d. Nmap: The Network Mapper - Introduction. [online] Available at: <https://nmap.org/> [Accessed 13 November 2020].

Rapid7. n.d. MS17-010 Eternalblue SMB Remote Windows Kernel Pool Corruption. [online] Available at:

<https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/> [Accessed 22 November 2020].

www.sophos.com. 2020. THE STATE OF RANSOMWARE 2020. [online] Available at: <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf> [Accessed 15 November 2020].

Www3.weforum.org. 2019. Regional Risks For Doing Business. [online] Available at: <http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2019.pdf> [Accessed 13 November 2020].