Vulnerability Assessment

Prepared by Alexander Marek

for GBI

Table of Contents

Scope of Work:

We Will perform a black box penetration test on the 192.168.0.128/29 network. We will scan the network to identify and attempt to exploit any vulnerabilities that may be on the network.

Tools used:

We will identify the hosts on this network and use several tools to conduct scans and vulnerability assessments on the network. These tools may include but are not limited to: nmap, Nessus, and Metasploit

Executive Overview:

There are 5 hosts on the network:

Host #	Host IP	Operating System
1	192.168.0.129	Microsoft Windows 2000|XP
2	192.168.0.130	Microsoft Windows 7|2008|8.1
3	192.168.0.131	Cisco IOS 12.X
4	192.168.0.132	Microsoft Windows 7|2008|8.1
5	192.168.0.133	Sun Solaris 9|10, Sun OpenSolaris

Vulnerabilities:

Severity Level	IP address	Description
Critical	192.168.0.129	MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)
Critical	192.168.0.129	MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution (902400)
Info	192.168.0.129	DCE Services Enumeration

Info	192.168.0.129	Microsoft Windows SMB2 Dialects Supported (remote check)
Critical	192.168.0.130	Microsoft Windows Vista Unsupported Installation Detection
Critical	192.168.0.130	Host 2 is exposed to a SMB flaw that can be used to execute code
Medium	192.168.0.130	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)
Medium	192.168.0.130	SMB Signing Disabled
Info	192.168.0.130	DCE Services Enumeration
Info	192.168.0.130	Link-Local Multicast Name Resolution (LLMNR) Detection
High	192.168.0.131	SSH Protocol Version 1 Session Key Retrieval
Medium	192.168.0.131	Unencrypted Telnet Server
Info	192.168.0.131	Common Platform Enumeration (CPE)
Info	192.168.0.131	Ethernet Card Manufacturer Detection
Critical	192.168.0.132	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution
Critical	192.168.0.132	MS17-010: Security Update for Microsoft Windows SMB Server (4013389)
High	192.168.0.132	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution
Medium	192.168.0.132	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium	192.168.0.132	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527)
Low	192.168.0.132	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	192.168.0.132	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	192.168.0.132	DCE Services Enumeration
Info	192.168.0.132	Microsoft Windows SMB Service Detection
Critical	192.168.0.133	SunSSH < 1.1.1 / 1.3 CBC Plaintext Disclosure
High	192.168.0.133	VNC Server Unauthenticated Access
Medium	192.168.0.133	Multiple Mail Server EXPN/VRFY Information Disclosure

Medium	192.168.0.133	SSH Weak Algorithms Supported
Low	192.168.0.133	SSH Server CBC Mode Ciphers Enabled
Low	192.168.0.133	SSH Weak MAC Algorithms Enabled
Info	192.168.0.133	RPC Services Enumeration
Info	192.168.0.133	SMTP Server Detection

Detailed Analysis

1) Host 192.168.0.129 - The following TCP ports were discovered:

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

25/tcp open smtp Microsoft ESMTP 6.0.2600.1

80/tcp open http Microsoft IIS httpd 5.1

135/tcp open msrpc Microsoft Windows RPC

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

443/tcp open https?

445/tcp open microsoft-ds Windows XP microsoft-ds

1025/tcp open msrpc Microsoft Windows RPC

1026/tcp open msrpc

3389/tcp open ms-wbt-server?

5000/tcp open upnp?

12345/tcp open netbus NetBus trojan 1.70

The following recommendations should be considered:

1. Critical - MS03-043: Buffer Overrun in Messenger Service (828035)

Microsoft has released a set of patches for Windows NT, 2000, XP and 2003.
http://technet.microsoft.com/en-us/security/bulletin/ms03-043

2. MS05-051: Vulnerabilities in MSDTC Could Allow Remote Code Execution

Microsoft has released a set of patches for Windows 2000, XP and 2003.

http://technet.microsoft.com/en-us/security/bulletin/ms05-051

3.

Check port 12345 for trojan

Close port 80 - no web server running

2) Host 192.168.0.130 - The following TCP ports were discovered:

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 7.0

135/tcp open tcpwrapped

139/tcp open tcpwrapped

445/tcp open microsoft-ds Windows Vista (TM) Business 6000 microsoft-ds (workgroup: WORKGROUP)

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

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

49157/tcp open msrpc Microsoft Windows RPC

The following recommendations should be considered:

1. Critical - Microsoft Windows Vista Unsupported Installation Detection

   Upgrade to a version of Microsoft Windows that is currently supported.

2. MS07-063: Vulnerability in SMBv2 Could Allow Remote Code Execution

   Microsoft has released a set of patches for Windows Vista.
   http://technet.microsoft.com/en-us/security/bulletin/ms07-063

3) **192.168.0.131** - No Critical Vulnerabilities. The Following TCP ports were discovered:

PORT STATE SERVICE VERSION

22/tcp open ssh Cisco SSH 1.25 (protocol 1.5)

23/tcp open telnet Cisco IOS telnetd

80/tcp open http Cisco IOS http config

The following recommendations should be considered:

1. Disable Telnet
2. Change default password
3. enable wpa2 authentication

4) **192.168.0.132** - The following TCP ports were discovered:

80/tcp open http Microsoft IIS httpd 7.5

135/tcp open msrpc Microsoft Windows RPC

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

445/tcp open microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)

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

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

49157/tcp open msrpc Microsoft Windows RPC

The following recommendations should be considered:

1. Critical - MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution
   Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.
   http://technet.microsoft.com/en-us/security/bulletin/ms11-030

2. Critical - MS17-010: Security Update for Microsoft Windows SMB Server (4013389)
   Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8. For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 /

139 and UDP ports 137 / 138 on all network boundary devices.
https://technet.microsoft.com/library/security/MS17-010

5) **192.168.0.133** - The following TCP ports were discovered:

PORT STATE SERVICE VERSION

21/tcp open ftp Solaris ftpd

22/tcp open ssh SunSSH 1.2 (protocol 2.0)

25/tcp open smtp Sendmail 8.14.2+Sun/8.14.2

587/tcp open smtp Sendmail 8.14.2+Sun/8.14.2

5800/tcp open vnc-http

5900/tcp open vnc VNC (protocol 3.7)

48737/tcp open xfce-session XFCE Session Manager

The following recommendations should be considered:

1. SunSSH < 1.1.1 / 1.3 CBC Plaintext Disclosure
   Upgrade to SunSSH 1.1.1 / 1.3 or later
2. Close port 22

Conclusion

Most critical flaws could have been avoided simply by patching and updating operating systems, software, and infrastructure. Legacy operating systems should be upgraded. Default passwords should be changed. Refer to the policies below and follow best practice.

1) There should only be one web server however there are web servers running on: 192.168.0.130, 192.168.0.131, and 192.168.0.132, as well as an open port 80 on 192.168.0.129.
2) There should be no SNMP however SNMP is open on 192.168.0.130
3) 192.168.0.131 has the device default password “Cisco” set.
4) 192.168.0.131 is not using any authentication and should be using WPA2
5) Telnet is enabled on 192.168.0.131 and port 22 is open on 192.168.0.133 both should be disabled as no telnet should be allowed.
6) Remote desktop is enabled on 192.168.0.129 and 192.168.0.132 and should be disabled.
7) There should only be one DNS server & no DNS zone transfers should be allowed
8) There should be no write access to FTP sites
9) There should only be one read only FTP site however FTP is enabled on both 192.168.0.129 and 192.168.0.133
10) All IPs should be static
11) All devices should be patched to the latest version.