BANGKOK UNIVERSITY

THE CREATIVE UNIVERSITY

โครงการ

ตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ(จำลอง)

เสนอ

นาวาอากาศตรี ดร.เอก โอสถหงษ์

จัดทำโดย

นายณัฐนนท์ ตานสานสินทร์ 1640704761

นายเจษฎา สิงห์ลอ 1640704910

นายณัฐสิทธิ์ ทุศีริ 1640706576

นางสาวอมรรัตน์ จันทโกวิท 1640705487

ภาคการศึกษาที่ 1 ปีการศึกษา 2566

ภาควิชาวิทยาการคอมพิวเตอร์ มุ่งเน้นวิทยาการข้อมูลและความมั่นคงปลอดภัยไซเบอร์

มหาวิทยาลัยกรุงเทพ

คำนำ

โครงการ เรื่อง การตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ(จำลอง)เป็นส่วนหนึ่งของวิชา Cybersecurity (CS448) การตรวจสอบความปลอดภัยของระบบสารสนเทศเป็นประจำเพื่อรักษาความมั่นคงและป้องกันการโจมตีทางไซเบอร์ซึ่งเป็นเรื่องสำคัญที่ไม่ควรละเลยโครงการนี้มุ่งเน้นในการวิเคราะห์และตรวจสอบระบบสารสนเทศที่มีผลกระทบต่อความปลอดภัยของข้อมูลและการดำเนินงานขององค์กรโดยมีวัตถุประสงค์หลักคือการป้องกันความเสียหายทางไซเบอร์และการรั่วไหลของข้อมูลที่อาจส่งผลต่อความลับโดยมีวัตถุประสงค์หลักเพื่อศึกษา การออกแบบเครือข่ายให้มีความปลอดภัย การประเมินความเสี่ยง การตรวจสอบ Vulnerability Assessment และการดำเนินการทดสอบเจาะระบบ

คณะผู้จัดทำคาดหวังเป็นอย่างยิ่งว่าการจัดทำเอกสารฉบับนี้จะมีตัวอย่างที่เป็นประโยชน์ต่อผู้ที่สนใจศึกษา การตรวจสอบการรักษาความปลอดภัยสำหรับระบบสารสนเทศ เป็นอย่างดี

คณะผู้จัดทำ

ณัฐนนท์ ตานสานสินทร

เจษฎา สิงห์ลอ

ณัฐสิทธิ์ ทุศิริ

อมรรัตน์ จันทโกวิท

สารบัญ

บทที่ **หน้า**

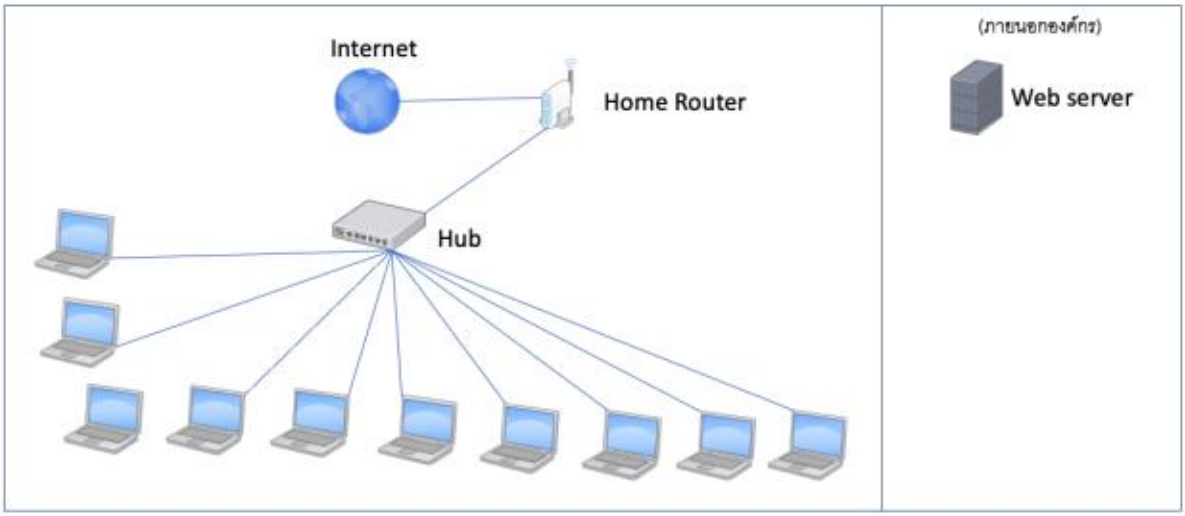
บทที่ 1

การออกแบบเครือข่ายรักษาความปลอดภัย

1.1 รายละเอียดปัญหาด้านความปลอดภัยของแผนผังเครือข่ายในปัจจุบัน

ข้อมูลเบื้องต้น

บริษัท A เป็นบริษัทขายสินค้าทางอินเตอร์เน็ตขนาดเล็กที่เพิ่งก่อตั้ง ได้รับการสนับสนุนทุนอุดหนุนจากภาครัฐเพื่อพัฒนา ระบบของบริษัทให้มีความปลอดภัยมากขึ้น โดยบริษัทมีพนักงานและผู้บริหารรวมทั้งสิ้น 10 คน ประกอบไปด้วย ผู้จัดการ 1 คน พนักงานบัญชี 1 คน ฝ่ายบุคคล 2 คน พนักงานขายจำนวน 5 คน และ พนักงานไอที 1 คน เนื่องจากบริษัทได้พัฒนามาจาก Home Office จึงไม่มีความรู้ทางด้านการออกแบบเครือข่ายและการรักษาความปลอดภัยของเว็บไซต์ เว็บไซต์ที่ใช้งานในปัจจุบัน ได้ทำการเช่า Hosting ภายนอกองค์กรไว้ โดยต้องการย้าย Web Server เข้ามาพร้อมกับการดำเนินการในครั้งนี้ โดยมีแผนผังเครือข่ายในปัจจุบันดังต่อไปนี้



แผนผังเครือข่ายปัจจุบัน

จากแผนผังเครือข่ายในปัจจุบันของบริษัท A พบปัญหาด้านความปลอดภัย ดังนี้

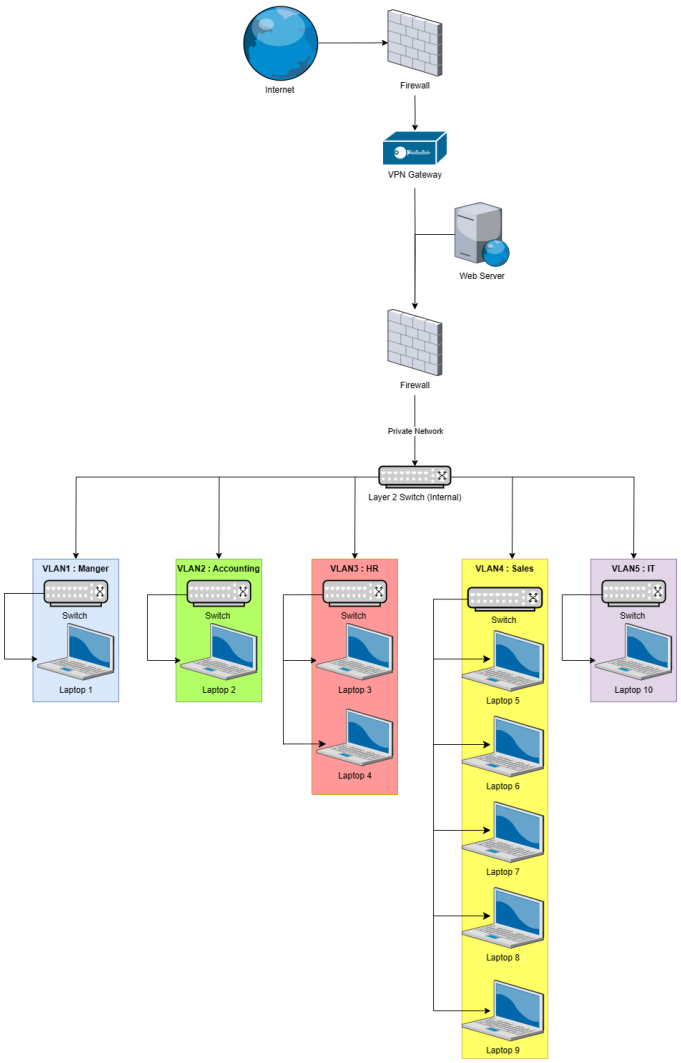
- ระบบเครือข่ายไม่ได้แยกส่วนอย่างชัดเจน อุปกรณ์ต่างๆ ในเครือข่ายเชื่อมต่อกันโดยตรง ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลได้อย่างง่ายดาย
- มีการใช้งาน Home Router ซึ่งไม่เหมาะกับการใช้งานในองค์กร
- ไม่มีการใช้ Firewall Firewall เป็นอุปกรณ์สำคัญในการรักษาความปลอดภัยเครือข่าย โดยมีหน้าที่ในการกรองและควบคุมการเข้าใช้งานเครือข่าย

1.2 แผนผังเครือข่ายใหม่ เมื่อทำการย้าย Web Server เข้ามาในเครือข่าย

แผนผังเครือข่ายใหม่ของบริษัท A ควรมีการปรับปรุงดังนี้

- แยกส่วนระบบเครือข่ายอย่างชัดเจน หรือการทำ Network Segment โดยใช้ VLAN (Virtual Local AreaNetwork) แบ่งออกแผนกอย่างชัดเจน เช่น VLAN1 : manager , VLAN3 : sales เป็นต้น โดยใช้ Switchให้การแบ่ง Segment และใช้ Layer 2 Switch ในการรวมทุกอย่างเข้าด้วยกัน
- ติดตั้ง Firewall Firewall ควรติดตั้งไว้ที่จุดเชื่อมต่อระหว่างเครือข่ายภายในและเครือข่ายภายนอก
- ติดตั้ง VPN ควรติดตั้งไว้สำหรับพนักงานที่ต้องการเข้าถึงข้อมูลภายในเครือข่ายจากภายนอก
- เพิ่ม DMZ (Demilitarized Zone) เพื่อแยกพื้นที่ที่เป็นพื้นที่สาธารณะหรือไม่ปลอดภัยจากเครือข่ายภายใน

แผนผังเครือข่ายใหม่ของบริษัท A มีดังนี้



แผนผังเครือข่ายหลังจากปรับปรุงแก้ไข

1.3 ระบุรายชื่ออุปกรณ์ควรมีในเครือข่าย เพื่อใช้ในการรักษาความปลอดภัย

- การเพิ่ม VPN Gateway เพื่อตรวจสอบและควบคุมการเข้าถึงเครือข่าย
- เปลี่ยนแปลงโครงสร้างเครือข่ายโดยการใช้ Switch แทน Hub เพื่อลดความเสี่ยงจากการโจมตี
- เพิ่ม DMZ (Demilitarized Zone)
  เพื่อแยกพื้นที่ที่เป็นพื้นที่สาธารณะหรือไม่ปลอดภัยจากเครือข่ายภายใน

บทที่ 2

การประเมินความเสี่ยง

2.1 การประเมินความเสี่ยงของระบบเครือข่ายใหม่

ทีมทดสอบจะใช้ตารางประเมินความเสี่ยงเพื่อประเมินความเสี่ยงอาจเกิดขึ้นจากการเช่า Hosting ภายนอกองค์กร โดยการใช้ตารางจะช่วยให้ทีมทดสอบทราบถึงความเสี่ยงที่เป็นไปได้ในแต่ล่ะส่วน ได้แก่ Web Server , work staion, Malwere และ Hacker

ตารางอ้างอิงเกณฑความเสี่ยง

Probability (โอกาสที่เกิดขึ้น)

Low	**Low**	**Medium**	**High**
	Low	**Low**	**Medium**
Medium	**Low**	**Medium**	**High**
High	**Medium**	**High**	**High**

Impact (ผลกระทบ)

2.2 ตารางการประเมินความเสี่ยง

#	Risk description	Asset/ Process	Threat	Consequence	Evaluat	Risk Mltigation	Resi-duel Risk
Risk ID	อธิบายความเสี่ยงที่เกิดขึ้นได้	สินทรัพย์หรือ ระบบที่มีผลกระทบ	ภัยคุกคาม	ผลกระทบ (Impact)	โอกาสที่เกิดขึ้น (Probability)	คำแนะนำเพื่อลดความเสี่ยง	ระดับความเสี่ยงหลังการแก้ไข
1	เครื่องภายในบริษัทติดมัลแวร์จากเครือข่ายภายนอกหรือเข้าเว็บไซต์	Work station	Mal ware	M	M	-เปลี่ยนแปลงโครงสร้างเครือข่ายโดยการใช้ Switch แทน Hub เพื่อลดความเสี่ยงจากการโจมตี -ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์เพื่อป้องกันการเข้าเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด	L

2	เกิดปัญหา traffic เว็บล่ม เมื่อมีผู้คนเข้าเว็บไซต์จำนวนมาก	Server	Network	M	M	- อัพเดตแพทช์ตลอดเพื่อตรวจสอบว่ามีปัญหาอะไรบ้าง -เลือกบริษัทที่ดูแลแบบ one-stop service	L
3	เครือข่ายภายในไม่มีแยกชัดเจน ทำให้สามารถเข้าถึงข้อมูลได้	Server	Hacker	H	H	-ใช้ Switch แทน Hub เพื่อลดความเสี่ยงจากการโจมตี -แบ่งการเข้าถึงข้อมูลเครื่องตามตำแหน่งพนักงาน	L
4	การป้องกันของ server ภายในบริษัทไม่เพียงพอ	Server	Hacker	H	H	- โหลด firewall กับ Vpn Gateway ป้องกันการเกิดมัลแวร์หรือผู้โจมตี	L

บทที่ 3

ผลการตรวจสอบ Vulnerability Assessment

3.1 ข้อมูลสรุปการตรวจสอบทั่วไปถึงสิ่งที่ถูกพบ

จากการตรวจสอบช่องโหว่ด้วย Basic Network Scan จาก IP Address target จะพบช่องโหว่ดังนี้

Critical จำนวน 1

High จำนวน 1

Medium จำนวน 2

Low จำนวน 0

3.2 สรุปผลรายชื่อช่องโหว่ที่ตรวจพบ แบ่งตามระดับความรุนแรงของช่องโหว่

Unsupported Windows OS (remote) ระดับ Critical

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) ระดับ High

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) ระดับ Medium

SMB Signing not required ระดับ Medium

3.3 ข้อแนะนำในการดำเนินการเพื่อแก้ไขช่องโหว่

Unsupported Windows OS (remote) Solution :

อัปเกรด Windows OS เป็นเวอร์ชันที่ได้รับการรองรับหรือติดตั้ง Service Pack เพื่อแก้ไขช่องโหว่ Unsupported Windows OS (remote).

ในเดือนธันวาคม 2566 Windows OS ที่ยังคงได้รับการสนับสนุนจาก Microsoft มีดังต่อไปนี้:

- Windows 11 เวอร์ชัน 22H2 หรือใหม่กว่า
- Windows 10 เวอร์ชัน 21H2 หรือใหม่กว่า
- Windows Server 2022 เวอร์ชัน 22H2 หรือใหม่กว่า
- Windows Server 2019 เวอร์ชัน 1909 หรือใหม่กว่า

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) Solution :

เพื่อแก้ไขช่องโหว่ MS17-010 ใน Microsoft Windows SMB Server

- อัปเดตระบบปฏิบัติการและติดตั้ง KB 4013389 หรือการอัปเดตความปลอดภัยที่เกี่ยวข้อง
- ใช้ Microsoft Update เพื่อตรวจสอบและติดตั้งอัพเดททั้งหมดที่มีอยู่
- ปฏิบัติตามแนวทางการป้องกันของ Microsoft
- ตรวจสอบการติดตั้งและแพทช์ระบบที่ไม่ได้รับการอัปเดต

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) Solution :

แนวทางแก้ไขหลักและมีประสิทธิภาพที่สุดคือการติดตั้งการอัปเดตความปลอดภัยที่เผยแพร่โดย Microsoft สำหรับระบบที่ได้รับผลกระทบ

SMB Signing not required Solution :

แนวทางแก้ไขที่แนะนำคือการติดตั้งการอัปเดตความปลอดภัยที่เผยแพร่โดย Microsoft การอัปเดตความปลอดภัยจะแก้ไขช่องโหว่นี้อย่างสมบูรณ์และมีประสิทธิภาพที่สุด

หากไม่สามารถติดตั้งการอัปเดตความปลอดภัยได้ คุณสามารถเปิดใช้งาน Message signing SMB ด้วยตนเอง วิธีนี้จะช่วยป้องกันช่องโหว่ได้ แต่อาจจำกัดฟังก์ชันการทำงานบางอย่างของ SMB

วิธีเปิดใช้งาน Message signing

1. เปิด Command Prompt ด้วย Run as administrator
2. พิมพ์คำสั่งต่อไปนี้ :

```
regadd“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services”\LanmanServer\Parameters” /v EnableSecuritySignature /t REG_DWORD /d1
```

3. กด Enter
4. รีสตาร์ทคอมพิวเตอร์

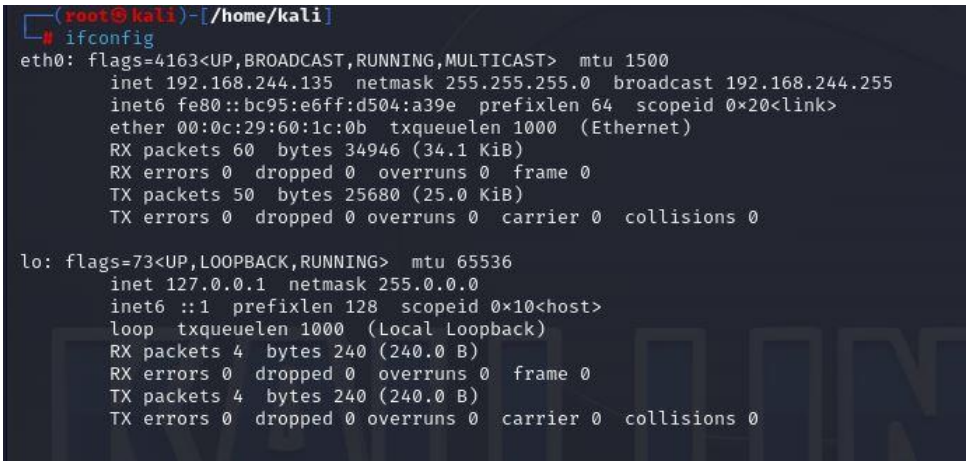
นอกจากแนวทางแก้ไขข้างต้นแล้ว คุณสามารถพิจารณาใช้กลยุทธ์การบรรเทาผลกระทบเพิ่มเติม เช่นการแบ่งเครือข่ายและการติดตั้งระบบตรวจจับ/ป้องกันการบุกรุก กลยุทธ์เหล่านี้สามารถช่วยเพิ่มความปลอดภัยของระบบของคุณและลดความเสี่ยงจากการโจมตีช่องโหว่ SMB Signing not required

บทที่ 4

Penetration Testing

4.1. Host Discovery

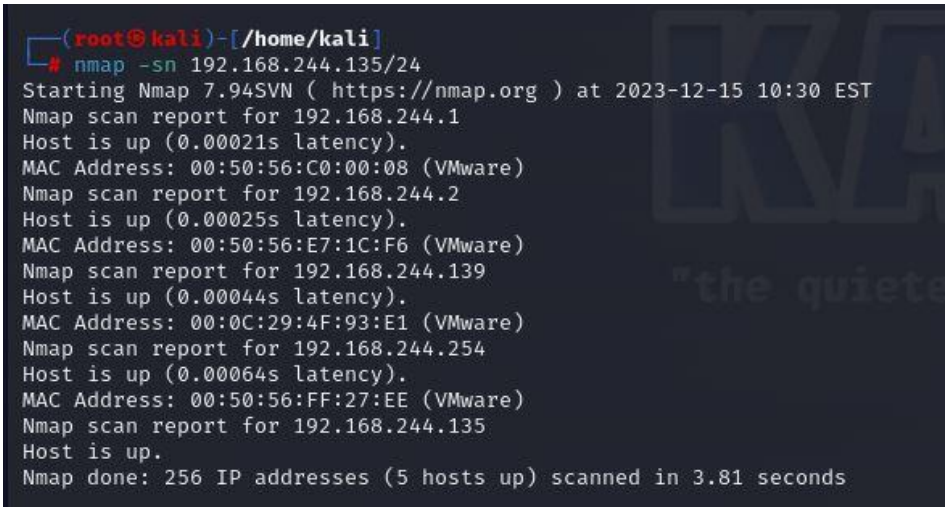
4.1.1ใช้คำสั่ง ifconfig เพื่อดู IP เครื่องตัวเอง



รูปแสดงการใช้คำสั่ง ifconfig

IP ที่ได้คือ 192.168.244.135

4.1.2ใช้คำสั่ง nmap –sn <IPเครื่องตัวเอง>/24 เพื่อหา ip เครื่องเป้าหมาย

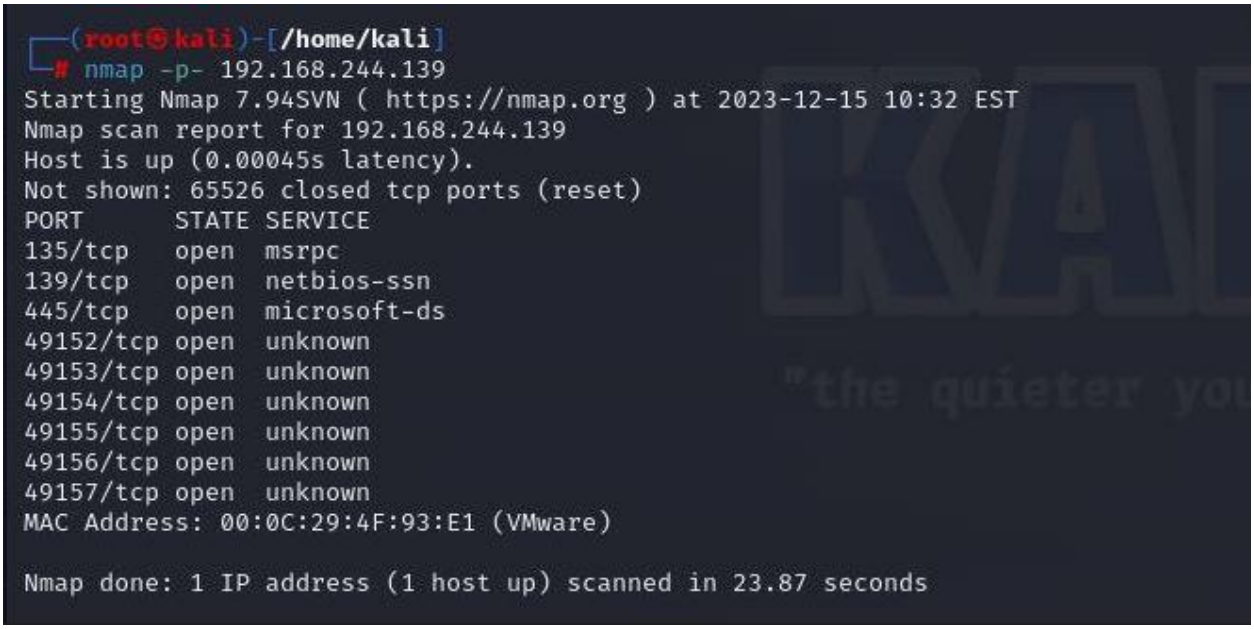


รูปแสดงการใช้คำสั่ง nmap –sn <IPเครื่องตัวเอง>/24

IP เครื่องเป้าหมายที่ได้คือ 192.168.244.139

4.2. Fingerprinting

4.2.1 ใช้คำสั่ง nmap -p- <ip เครื่องเป้าหมาย> เพื่อหา Post ทั้งหมด



รูปที่แสดงการใช้คำสั่ง nmap -p- <ip เครื่องเป้าหมาย>

Post ที่เปิดอยู่มี 9 post ได้แก่

Post 135 Service msrpc

Post 139 Service netbios-ssn

Post 445 Service microsoft-ds

Post 49152 Service unknown

Post 49153 Service unknown

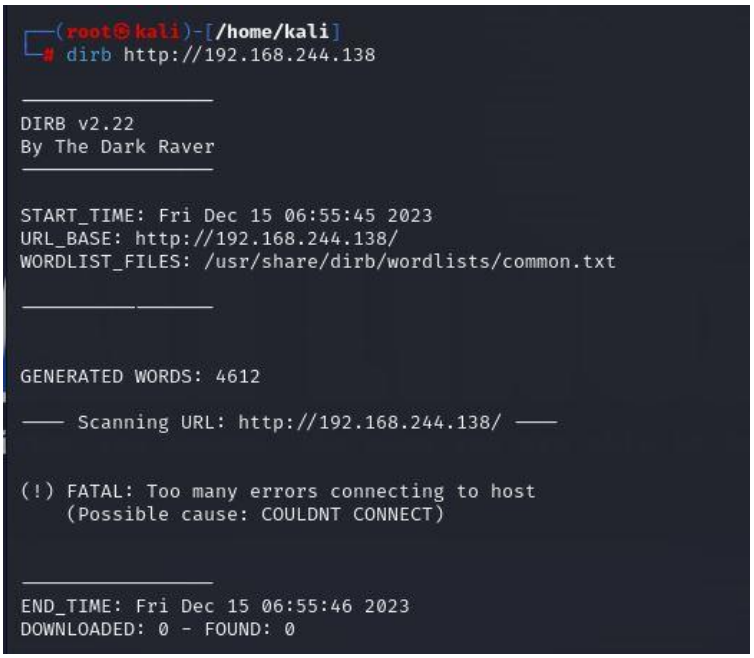
Post 49154 Service unknown

Post 49155 Service unknown

Post 49156 Service unknown

Post 49157 Service unknown

4.2.2 ใช้คำสั่ง dirb <http://ip เครื่องเป้าหมาย> เพื่อหาหา File, Folder และ shared folder



รูปที่แสดงการใช้คำสั่ง dirb <http://ip เครื่องเป้าหมาย>

จากการใช้คำสั่ง dirb ไม่พบไฟล์

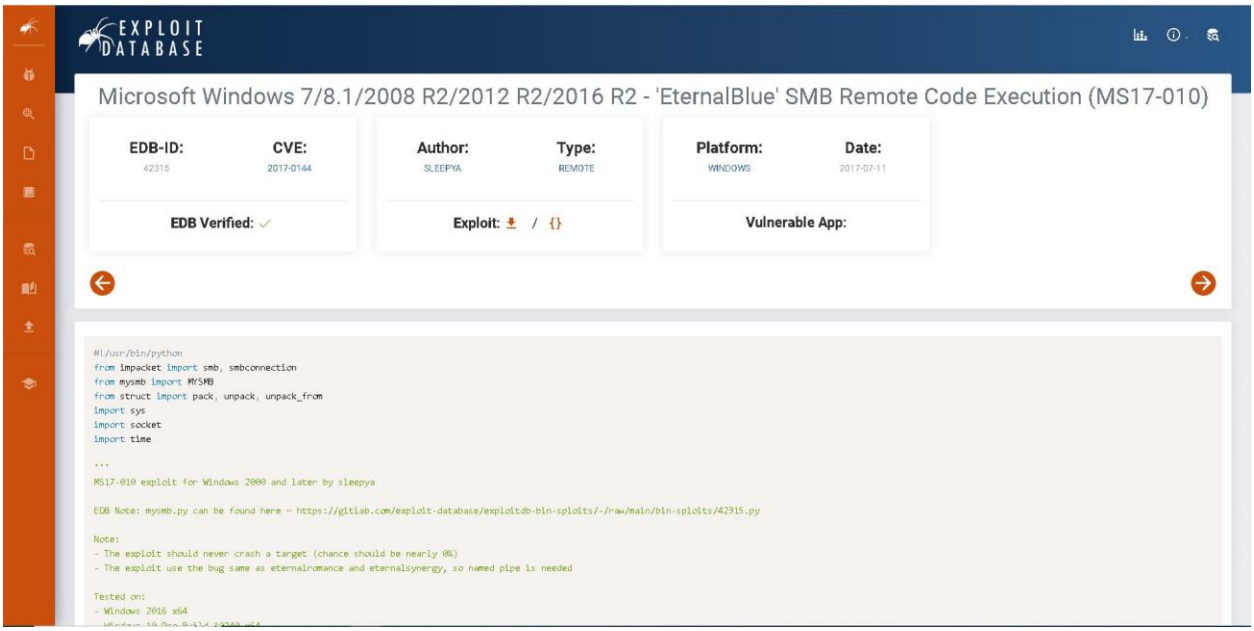
4.2.3 ใช้คำสั่ง namp -p <Post ที่ต้องการสแกน> -A <ip เครื่องเป้าหมาย>
เพื่อตรวจสอบเซอร์วิสที่ทำงานอยู่ในพอร์ต,ระบบปฏิบัติการ,และเวอร์ชันของซอฟต์แวร์ที่ทำงานบนเครื่องเป้าหมาย

รูปที่ 4.2.2 แสดงการใช้คำสั่ง namp -p <Post ที่เปิดอยู่> -A <ip เครื่องเป้าหมาย>

Os ที่ได้คือ windows 7

4.3. Exploit Database

4.3.1 นำชื่อ version ที่ตรวจพบบน port 445 ค้นหาบนเว็บไซต์ https://www.exploit-db.com/ เพื่อค้นหารหัส Code ที่ใช้ในการโจมตีช่องโหว่

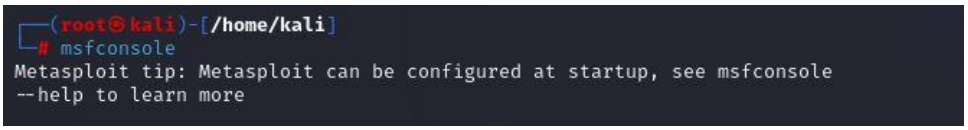


รูปแสดงการค้นหาบนเว็บ exploit database

Codeที่ได้คือ MS17-010

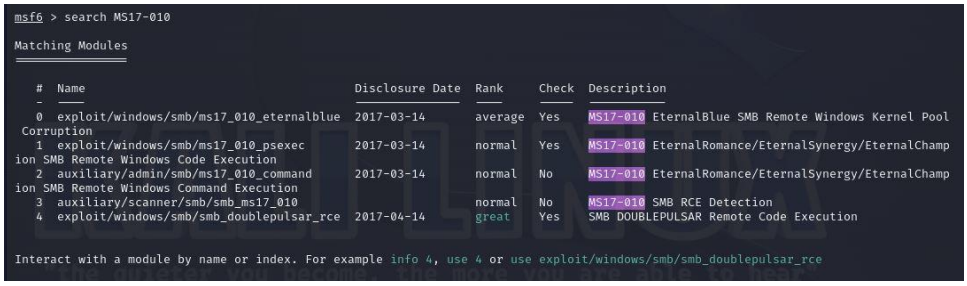
4.4. Exploitation

4.4.1 ใช้คำสั่ง msfconsole เพื่อเปิด Metasploit Framework



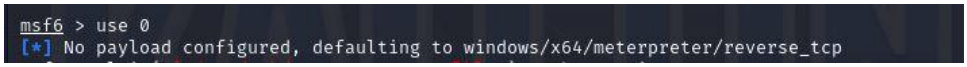
รูปแสดงการใช้คำสั่ง msfconsole

4.4.2 ทำการโดยใช้คำสั่ง search MS17-010 เพื่อค้นหาข้อมูลเกี่ยวกับช่องโหว่ MS17-010 คำสั่งนี้จะให้ผลลัพธ์จากฐานข้อมูล Metasploit Framework ที่เกี่ยวข้องกับชื่อโค้ด MS17-010



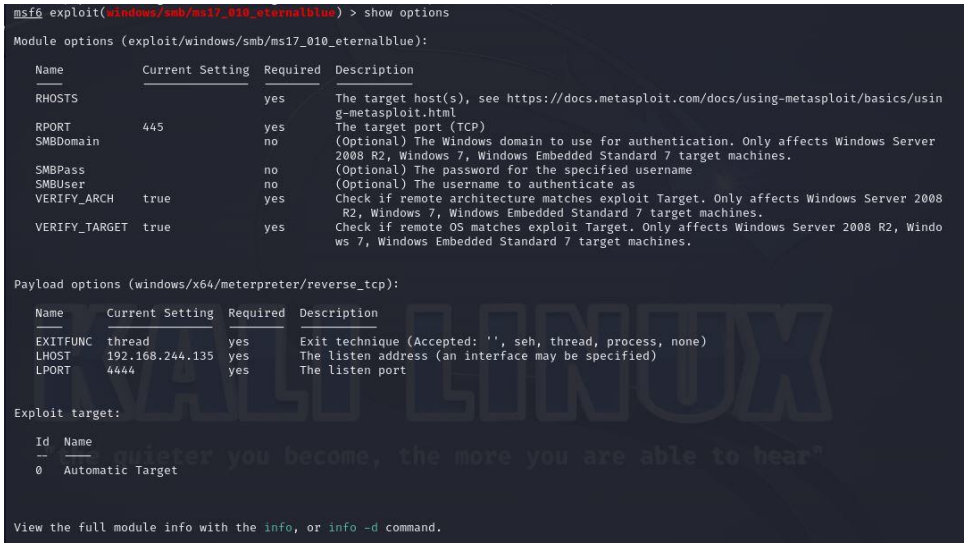
รูปแสดงการใช้คำสั่ง search MS17-010

4.4.3 เลือกโมดูลที่ 0 ด้วยคำสั่ง use 0 หรือ use exploit/windows/smb/ms17_010_eternalblue หลังจากใช้คำสั่งนี้ Metasploit จะโปรแกรมตามโมดูลที่ 0



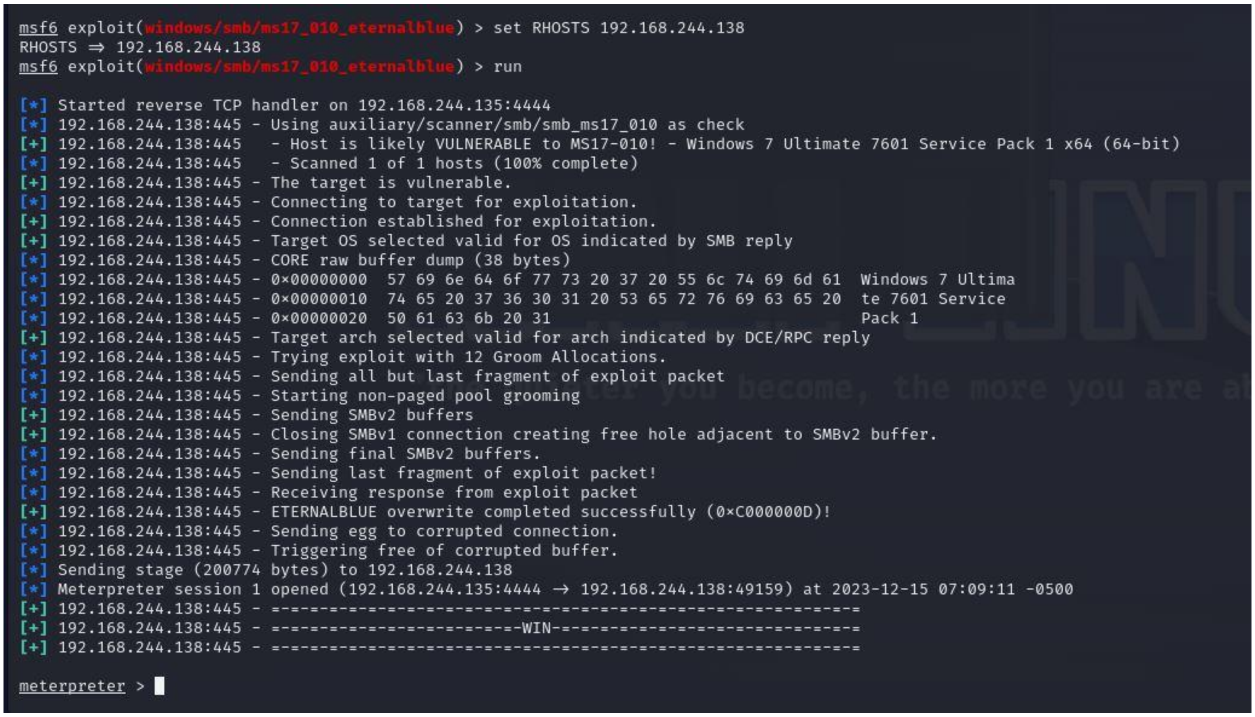
รูปแสดงการใช้คำสั่ง use 0

4.4.4 ใช้คำสั่ง show options เพื่อแสดงรายการตัวเลือกที่สามารถกำหนดค่าได้ในโมดูลปัจจุบันที่กำลังใช้



รูปแสดงการใช้คำสั่ง show options

4.4.5 ใช้คำสั่ง set RHOSTS <ip เครื่องเป้าหมาย> เพื่อกำหนดค่า Host (RHOSTS) ที่เป็นเครื่องเป้าหมายของการโจมตี และ ทำการ run หรือ exploit เพื่อเปิดการโจมตีด้วย exploit ที่ถูกเลือก



รูปแสดงการใช้คำสั่ง set RHOSTS<IP เครื่องเป้าหมาย> และทำการ run

4.4.6 ใช้คำสั่ง getuid เพื่อดูชื่อ Sever username

รูปแสดงการใช้คำสั่ง getuid

Sever username ที่ได้คือ NT AUTHORITY\SYSTEM

บท 5

ภาคผนวก

Project2

Wed, 13 Dec 2023 23:39:02 SE Asia Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.208.131

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	2	0	34

Scan Information

Start time:	Wed Dec 13 23:34:11 2023
End time:	Wed Dec 13 23:39:02 2023

Host Information

Netbios Name:	WIN-845Q99OO4PP
IP:	192.168.208.131
MAC Address:	00:0C:29:BC:0C:54
OS:	Microsoft Windows 7 Ultimate

Vulnerabilities

108797 - Unsupported Windows OS (remote) -

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

XREF IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2023/07/27

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows 7 Ultimate
```

97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) -

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

See Also

http://www.nessus.org/u?68fc8eff
http://www.nessus.org/u?321523eb
http://www.nessus.org/u?065561d0
http://www.nessus.org/u?d9f569cf
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/u?59db5b5b

Solution

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.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.7

CVSS v2.0 Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Severity

I

References

BID	96703
BID	96704
BID	96705
BID	96706
BID	96707
BID	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212
MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XREF	EDB-ID:41891
XREF	EDB-ID:41987
XREF	MSFT:MS17-010
XREF	IAVA:2017-A-0065
XREF	CISA-KNOWN-EXPLOITED:2022/05/03
XREF	CISA-KNOWN-EXPLOITED:2022/08/10
XREF	CISA-KNOWN-EXPLOITED:2022/04/15
XREF	CISA-KNOWN-EXPLOITED:2022/04/27
XREF	CISA-KNOWN-EXPLOITED:2022/06/14

Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

Plugin Information

Published: 2017/03/20, Modified: 2022/05/25

Plugin Output

tcp/445/cifs

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000008ccdf0008000110000000
00ffffffff000000000000000000000054000005400020023000001100005c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c80000000000000000000000008ccdf00080001000000
```

90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) -

Synopsis

The remote Windows host is affected by an elevation of privilege vulnerability.

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

See Also

http://www.nessus.org/u?52ade1e9
http://badlock.org/

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSS v2.0 Temporal Score

4.3 (CVSS2#E:U/RL:OF/RC:C)

STIG Severity

I

References

BID	86002

CVE	CVE-2016-0128
MSKB	3148527
MSKB	3149090
MSKB	3147461
MSKB	3147458
XREF	MSFT:MS16-047
XREF	CERT:813296
XREF	IAVA:2016-A-0093

Plugin Information

Published: 2016/04/13, Modified: 2019/07/23

Plugin Output

tcp/49157/dce-rpc

57608 - SMB Signing not required -

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

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: 2023/10/16

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

cpe:/o:microsoft:windows_7:::ultimate -> Microsoft Windows 7
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown
```

```
Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc087800

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc087800

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-e1b88367fc018b18eb

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc08A771

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc08A771

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-0c7e1c4bd7fa1eb58e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 8174bb16-571b-4c38-8386-1102b449044a, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a4a975378dc878fb91

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a2d47257-12f7-4beb-8981-0ebfa935c407, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a4a975378dc878fb91

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3f31c91e-2545-4b7b-9311-9529e8bffef6, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-a4a975378dc878fb91

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LRPC-f58af8af71cbda35dd

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
```

```
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : LRPC-7c8a39c92d53417bdd

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : OLE3FC71EDC327A42CB82F63AC03DCC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0767a036-0d22-48aa-ba69-b619480f38cb, version 1.0
Description : Unknown RPC service
Annotation : PcaSvc
Type : Local RPC service
Named pipe : LRPC-2d0b284a7c7006adae

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE3FC71EDC327A42CB82F63AC03DCC

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : LRPC-2d0b284a7c7006adae

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : trkwks

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-877338c14d9c004f3e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-877338c14d9c004f3e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
```

```
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-877338c14d9c004f3e

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLE6CB46C5CD81D4816AC8E1DC9C2CA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-ed3ff9316ea56f389b

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : OLE6CB46C5CD81D4816AC8E1DC9C2CA

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-ed3ff9316ea56f389b

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 6c637067-6569-746e-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838
```

```
Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
```

```
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : OLE91C46E4D6FB34AE8B95DF577C838

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : AudioClientRpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : Audiosrv

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : dhcpcsvc6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Local RPC service
Named pipe : OLE129FAE7FD10C4CCCAD118B3AE758
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-845Q99OO4PP

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\WIN-845Q99OO4PP
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \pipe\trkwks
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\browser
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\browser
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\browser
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
Named pipe : \PIPE\browser
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-845Q99OO4PP
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-845Q99OO4PP

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\WIN-845Q99OO4PP
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.208.131
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.208.131
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.208.131
```


10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49155/dce-rpc

```
The following DCERPC services are available on TCP port 49155 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49155
IP : 192.168.208.131
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49156/dce-rpc

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.208.131

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.208.131
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49157/dce-rpc

```
The following DCERPC services are available on TCP port 49157 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49157
IP : 192.168.208.131
```

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 : 99
```

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:BC:0C:54 : 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:BC:0C:54
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution -

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.208.131 resolves as WIN-845Q99OO4PP.
```

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

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

icmp/0

```
The ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -967 seconds.
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 7 Ultimate 7601 Service Pack 1
The remote native LAN manager is : Windows 7 Ultimate 6.1
The remote SMB Domain Name is : WIN-845Q99OO4PP
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry -

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection -

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

```
An SMB server is running on this port.
```

11011 - Microsoft Windows SMB Service Detection -

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
SMBv1
SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) -

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_ _introduced in windows version_
2.0.2 Windows 2008
2.1 Windows 7

The remote host does NOT support the following SMB dialects :
_version_ _introduced in windows version_
2.2.2 Windows 8 Beta
2.2.4 Windows 8 Beta
3.0 Windows 8
3.0.2 Windows 8.1
3.1 Windows 10
3.1.1 Windows 10
```

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: 2023/09/25

Plugin Output

tcp/135/epmap

```
Port 135/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: 2023/09/25

Plugin Output

tcp/139/smb

```
Port 139/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: 2023/09/25

Plugin Output

tcp/445/cifs

```
Port 445/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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202312131218
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Project2
Scan policy used : Basic Network Scan
Scanner IP : 192.168.208.1
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 10.002 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
```

```
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/12/13 23:34 SE Asia Standard Time
Scan duration : 281 sec
Scan for malware : no
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges -

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\WIN-845Q99OO4PP\ADMIN$' with the supplied credentials.
```

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: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 7 Ultimate
Confidence level : 99
Method : MSRPC

Not all fingerprints could give a match. If you think some or all of
the following could be used to identify the host's operating system,
please email them to os-signatures@nessus.org. Be sure to include a
brief description of the host itself, such as the actual operating
system or product / model names.

SinFP:!:
P1:B11113:F0x12:W8192:O0204ffff:M1460:
P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:190704_7_p=139


The remote host is running Microsoft Windows 7 Ultimate
```

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 SMB service.
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) -

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, 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.

Risk Factor

None

References

XREF	IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

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: 2023/02/13

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB 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 192.168.208.1 to 192.168.208.131 :
192.168.208.1
192.168.208.131

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.
```

135860 - WMI Not Available -

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2023/11/14

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure -

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :

WIN-845Q99OO4PP = File Server Service
WIN-845Q99OO4PP = Computer name
WORKGROUP = Workgroup / Domain name
WORKGROUP = Browser Service Elections
WORKGROUP = Master Browser
__MSBROWSE__ = Master Browser

The remote host has the following MAC address on its adapter :

00:0c:29:bc:0c:54
```