SNMP Enumeration Assessment Report

1. Introduction

The SNMP Enumeration Assessment Report provides an analysis of the findings from the SNMP enumeration conducted using the metasploits freamework tool. The assessment aimed to identify SNMP-enabled devices, gather system information, and assess security vulnerabilities within the target network.

2. Scope

The assessment focused on enumerating SNMP-enabled devices within the target network. The assessment was conducted within the context of a security audit to evaluate the effectiveness of SNMP security controls.

3. Methodology

The SNMP enumeration was performed using **snmp_enum** module in Metasploit tool with the following configuration:

- Target IP: 192.168.1.69
- SNMP Community Strings: Public, Private
- Output Format: Text

The tool was executed with appropriate command-line options to enumerate SNMP-enabled devices and gather system information.

4.Findings

System Information

Host IP address : 192.168.1.69
Hostname : DESKTOP-HD9NDSI
Description : Hardware: Intel64 Family 6 Model 158 Stepping 10 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 19045 Multiprocessor Free)
Contact : -
Location : -
Uptime snmp : 01:00:24.23
Uptime system : 00:37:02.96
System date : 2024-3-27 03:07:49.3
Domain : WORKGROUP

Network information:

IP forwarding enabled : no
Default TTL : 128
TCP segments received : 626095

TCP segments sent	: 232498
TCP segments retrans	: 177
Input datagrams	: 628201
Delivered datagrams	: 628458
Output datagrams	: 233480

Network IP:

Id	IP Address	Netmask	Broadcast
1	127.0.0.1	255.0.0.0	1
9	192.168.1.69	255.255.255.0	1

Routing information:

Destination	Next hop	Mask	Metric
0.0.0.0	192.168.1.254	0.0.0.0	25
127.0.0.0	127.0.0.1	255.0.0.0	331
127.0.0.1	127.0.0.1	255.255.255.255	331
127.255.255.255	127.0.0.1	255.255.255.255	331
192.168.1.0	192.168.1.69	255.255.255.0	281
192.168.1.69	192.168.1.69	255.255.255.255	281
192.168.1.255	192.168.1.69	255.255.255.255	281
224.0.0.0	127.0.0.1	240.0.0.0	331
255.255.255.255	127.0.0.1	255.255.255.255	331

TCP connections and listening ports:

Local address	Local port	Remote address	Remote port	State
0.0.0.0	135	0.0.0.0	0	listen
0.0.0.0	445	0.0.0.0	0	listen
0.0.0.0	5040	0.0.0.0	0	listen
0.0.0.0	5357	0.0.0.0	0	listen
0.0.0.0	49664	0.0.0.0	0	listen
0.0.0.0	49665	0.0.0.0	0	listen
0.0.0.0	49666	0.0.0.0	0	listen
0.0.0.0	49667	0.0.0.0	0	listen
0.0.0.0	49668	0.0.0.0	0	listen
0.0.0.0	49672	0.0.0.0	0	listen
0.0.0.0	49673	0.0.0.0	0	listen
192.168.1.69	139	0.0.0.0	0	listen
192.168.1.69	49725	20.198.118.190	443	established
192.168.1.69	49796	20.198.118.190	443	established
192.168.1.69	49925	40.99.31.178	443	established
192.168.1.69	49941	20.205.115.81	443	established
192.168.1.69	49944	103.211.149.26	443	established
192.168.1.69	49945	103.211.150.184	443	established
192.168.1.69	49946	103.211.150.146	443	established

Listening UDP ports:

Local address	Local port
0.0.0.0	123
0.0.0.0	161
0.0.0.0	162
0.0.0.0	500
0.0.0.0	3702
0.0.0.0	4500
0.0.0.0	5050
0.0.0.0	5353
0.0.0.0	5355
0.0.0.0	50594
0.0.0.0	50600
0.0.0.0	61195
127.0.0.1	1900
127.0.0.1	50599
127.0.0.1	62593
192.168.1.69	137
192.168.1.69	138
192.168.1.69	1900
192.168.1.69	50598

Network services:

Index	Name
0	Power
1	Server
2	Themes
3	SysMain
4	IP Helper
5	SNMP Trap
6	DNS Client
7	Data Usage
8	DHCP Client
9	Time Broker
10	Workstation
11	SNMP Service
12	User Manager
13	Windows Time
14	AVCTP service
15	CoreMessaging
16	Plug and Play
17	Print Spooler
18	Windows Audio
19	SSDP Discovery
20	Task Scheduler
21	Windows Search
22	Windows Update
23	Security Center
24	Storage Service

25 Sync Host_e0523
26 Computer Browser
27 CNG Key Isolation
28 COM+ Event System
29 Windows Event Log
30 Credential Manager
31 IPsec Policy Agent
32 Microsoft Passport
33 Geolocation Service
34 Group Policy Client
35 RPC Endpoint Mapper
36 Web Account Manager
37 Network List Service
38 System Events Broker
39 User Profile Service
40 Base Filtering Engine
41 Local Session Manager
42 TCP/IP NetBIOS Helper
43 Cryptographic Services
44 Diagnostic System Host
45 Display Policy Service
46 Application Information
47 Diagnostic Service Host
48 Radio Management Service
49 Shell Hardware Detection
50 State Repository Service
51 Windows Security Service
52 Diagnostic Policy Service
53 Network Connection Broker
54 Security Accounts Manager
55 Windows Biometric Service
56 Windows Defender Firewall
57 Windows Modules Installer
58 Device Association Service
59 Network Location Awareness
60 Windows Connection Manager
61 Remote Procedure Call (RPC)
62 Update Orchestrator Service
63 Clipboard User Service_e0523
64 DCOM Server Process Launcher
65 Microsoft Passport Container
66 Windows Update Medic Service
67 Windows Audio Endpoint Builder
68 Microsoft Store Install Service
69 Network Store Interface Service
70 Windows Image Acquisition (WIA)
71 Windows License Manager Service
72 Distributed Link Tracking Client
73 Function Discovery Provider Host
74 Remote Access Connection Manager
75 AppX Deployment Service (AppXSVC)
76 Capability Access Manager Service

77	System Event Notification Service
78	Connected Devices Platform Service
79	Windows Management Instrumentation
80	IKE and AuthIP IPsec Keying Modules
81	System Guard Runtime Monitor Broker
82	Microsoft Defender Antivirus Service
83	Network Connected Devices Auto-Setup
84	Background Tasks Infrastructure Service
85	Function Discovery Resource Publication
86	Connected User Experiences and Telemetry
87	Secure Socket Tunneling Protocol Service
88	WinHTTP Web Proxy Auto-Discovery Service
89	Windows Push Notifications System Service
90	Touch Keyboard and Handwriting Panel Service
91	Connected Devices Platform User Service_e0523
92	Windows Push Notifications User Service_e0523
93	Microsoft Defender Antivirus Network Inspection Service

Processes:

Id	Status	Name	Path	Parameters
1	running	System Idle Process		
4	running	System		
72	running	Registry		
264	running	svchost.exe	C:\Windows\system32\	-k UnistackSvcGroup
328	running	smss.exe		
356	running	svchost.exe	C:\Windows\system32\	-k LocalService -p
376	running	svchost.exe	C:\Windows\System32\	-k LocalServiceNetworkRestricted -p
380	running	svchost.exe	C:\Windows\system32\	-k LocalServiceNoNetwork -p
424	running	csrss.exe		
428	running	svchost.exe	C:\Windows\System32\	-k LocalServiceNetworkRestricted
492	running	wininit.exe		
500	running	csrss.exe		
560	running	winlogon.exe		
584	running	services.exe		
616	running	snmptrap.exe	C:\Windows\System32\	
620	running	lsass.exe	C:\Windows\system32\	
712	running	fontdrvhost.exe		
720	running	fontdrvhost.exe		
728	running	svchost.exe	C:\Windows\system32\	-k DcomLaunch -p
816	running	svchost.exe	C:\Windows\system32\	-k RPCSS -p
888	running	svchost.exe	C:\Windows\system32\	-k netsvcs -p
892	running	dwm.exe		
988	running	MoUsoCoreWorker.exe	C:\Windows\System32\	-Embedding
1008	running	svchost.exe	C:\Windows\System32\	-k LocalSystemNetworkRestricted -p
1076	running	ctfmon.exe		
1128	running	RuntimeBroker.exe	C:\Windows\System32\	-Embedding
1132	running	Memory Compression		
1304	running	svchost.exe	C:\Windows\System32\	-k NetworkService -p
1332	running	taskhostw.exe		{222A245B-E637-4AE9-A93F-A59CA119A75E}
1368	running	svchost.exe	C:\Windows\system32\	-k LocalService
1392	running	svchost.exe		
1408	running	svchost.exe	C:\Windows\System32\	-k LocalServiceNetworkRestricted -p
1484	running	svchost.exe	C:\Windows\system32\	-k imgsvc
1488	running	svchost.exe	C:\Windows\system32\	-k appmodel -p
1508	running	svchost.exe	C:\Windows\System32\	-k LocalServiceNetworkRestricted -p
1520	running	svchost.exe	C:\Windows\system32\	-k LocalServiceNetworkRestricted -p
1672	running	spoolsv.exe	C:\Windows\System32\	
1708	running	svchost.exe	C:\Windows\system32\	-k LocalServiceNoNetworkFirewall -p

```
 1820           running          TiWorker.exe         C:\Windows\winsxs\amd64_microsoft-windows-
servicingstack_31bf3856ad364e35_10.0.19041.4163_none_7e304ec47c735f2e\  -Embedding
 1868           running          sihost.exe
 1960           running          svchost.exe          C:\Windows\system32\  -k ClipboardSvcGroup -p
 1996           running          svchost.exe          C:\Windows\system32\  -k NetworkServiceNetworkRestricted -p
 2040           running          svchost.exe          C:\Windows\System32\  -k utcsvc -p
 2092           running          MsMpEng.exe
 2148           running          svchost.exe          C:\Windows\System32\  -k netsvcs
 2276           running          RuntimeBroker.exe    C:\Windows\System32\  -Embedding
 2292           running          WinStore.App.exe     C:\Program
Files\WindowsApps\Microsoft.WindowsStore_11910.1002.5.0_x64__8wekyb3d8bbwe\  -
ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca
 2328           running          RuntimeBroker.exe    C:\Windows\System32\  -Embedding
 2412           running          dasHost.exe                        {b7535c25-9f4f-4082-bdbee223aa49671c}
 2460           running          svchost.exe          C:\Windows\system32\  -k LocalServiceAndNoImpersonation -p
 2496           running          SearchIndexer.exe    C:\Windows\system32\  /Embedding
 2848           running          msedge.exe           C:\Program Files (x86)\Microsoft\Edge\Application\  --
type=gpu-process --no-appcompat-clear --gpu-
preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAABgAAAAAAA4AAAAAAAAAAAAAAAEAAAAAAAAA
 2952           running          SecurityHealthSystray.exe  C:\Windows\System32\
 2968           running          NisSrv.exe
 3240           running          SearchApp.exe
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\  -
ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca
 3468           running          RuntimeBroker.exe    C:\Windows\System32\  -Embedding
 3556           running          SgrmBroker.exe
 3588           running          svchost.exe          C:\Windows\System32\  -k netsvcs -p
 3804           running          TrustedInstaller.exe  C:\Windows\servicing\
 3912           running          SearchApp.exe
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\  -
ServerName:ShellFeedsUI.AppX88fpyyrd21w8wqe62wzsjh5agex7tf1e.mca
 3916           running          UserOOBEBroker.exe   C:\Windows\System32\oobe\  -Embedding
 3940           running          SecurityHealthService.exe
 4184           running          svchost.exe          C:\Windows\system32\  -k WbioSvcGroup
 4192           running          OneDrive.exe         C:\Users\par3i\AppData\Local\Microsoft\OneDrive\
/background
 4324           running          RuntimeBroker.exe    C:\Windows\System32\  -Embedding
 4440           running          RuntimeBroker.exe    C:\Windows\System32\  -Embedding
 4452           running          mmc.exe              C:\Windows\system32\  "C:\Windows\system32\wf.msc"
 4516           running          SkypeApp.exe         C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\  -
ServerName:App.AppXffn3yxqvgawq9fpmnhy90fr3y01d1t5b.mca
 4540           running          SkypeBackgroundHost.exe  C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\  -ServerName:SkypeBackgroundHost
 4552           running          ShellExperienceHost.exe
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\  -
ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
 4580           running          StartMenuExperienceHost.exe
C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\  -
ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
 4584           running          explorer.exe         C:\Windows\
 4712           running          SkypeBridge.exe      C:\Program
Files\WindowsApps\Microsoft.SkypeApp_14.53.77.0_x64__kzf8qxf38zg5c\SkypeBridge\  /InvokerPRAID: App
 4836           running          conhost.exe          \??\C:\Windows\system32\  0x4
 4944           running          msedge.exe           C:\Program Files (x86)\Microsoft\Edge\Application\  --
type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --no-
appcompat-clear --
 5036           running          ApplicationFrameHost.exe  C:\Windows\system32\  -Embedding
 5136           running          dllhost.exe          C:\Windows\system32\  /Processid:{973D20D7-562D-44B9-B70B-
5A0F49CCDF3F}
 5212           running          svchost.exe
 5488           running          msedge.exe           C:\Program Files (x86)\Microsoft\Edge\Application\  --
type=renderer --instant-process --no-appcompat-clear --first-renderer-process --lang=en-US --js-flags=--ms-user-
locale= --dev
 6140           running          snmp.exe             C:\Windows\System32\
```

6152 running TextInputHost.exe C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\ -ServerName:InputApp.AppXjd5de1g66v206tj52m9d0dtpppx4cgpn.mca
6888 running Microsoft.Photos.exe C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2019.19071.12548.0_x64__8wekyb3d8bbwe\ -ServerName:App.AppXzst44mncqdg84v7sv6p7yznqwssy6f7f.mca
6952 running wuauclt.exe C:\Windows\system32\ /UpdateDeploymentProvider UpdateDeploymentProvider.dll /ClassId 0d7c0d9e-81aa-48bf-94be-7570247803ed /RunHandlerComServer
8024 running msedge.exe C:\Program Files (x86)\Microsoft\Edge\Application\ --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --no-appcompat-clear
8220 running msedge.exe
8316 running cmd.exe C:\Windows\system32\
9224 running msedge.exe C:\Program Files (x86)\Microsoft\Edge\Application\ --type=renderer --no-appcompat-clear --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=1 -
10212 running msedge.exe C:\Program Files (x86)\Microsoft\Edge\Application\ --flag-switches-begin --flag-switches-end --no-startup-window
11076 running taskhostw.exe

Storage information:

Description : ["C:\\ Label: Serial Number c4ea2440"]
Device id : [#<SNMP::Integer:0x00007f14bc4d6598 @value=1>]
Filesystem type : ["Fixed Disk"]
Device unit : [#<SNMP::Integer:0x00007f14bc4d4838 @value=4096>]
Memory size : 49.41 GB
Memory used : 21.22 GB

Description : ["D:\\"]
Device id : [#<SNMP::Integer:0x00007f14bc4d8078 @value=2>]
Filesystem type : ["Compact Disc"]
Device unit : [#<SNMP::Integer:0x00007f14bc4de388 @value=0>]
Memory size : 0 bytes
Memory used : 0 bytes

Description : ["Virtual Memory"]
Device id : [#<SNMP::Integer:0x00007f14bc4e1c40 @value=3>]
Filesystem type : ["Virtual Memory"]
Device unit : [#<SNMP::Integer:0x00007f14bc4e7dc0 @value=65536>]
Memory size : 4.47 GB
Memory used : 2.71 GB

Description : ["Physical Memory"]
Device id : [#<SNMP::Integer:0x00007f14bc4bb630 @value=4>]
Filesystem type : ["Ram"]
Device unit : [#<SNMP::Integer:0x00007f14bc4b98a8 @value=65536>]
Memory size : 3.16 GB
Memory used : 2.44 GB

File system information:

Index : 1
Mount point :
Remote mount point : -
Type : NTFS
Access : 1
Bootable : 0

Device information:

Id	Type	Status	Descr
1	Printer	running	Microsoft XPS Document Writer v4
2	Printer	running	Microsoft Print To PDF
3	Printer	running	Microsoft Shared Fax Driver
4	Processor	running	Unknown Processor Type
5	Network	unknown	Software Loopback Interface 1
6	Network	unknown	Microsoft 6to4 Adapter
7	Network	unknown	WAN Miniport (IPv6)
8	Network	unknown	WAN Miniport (L2TP)
9	Network	unknown	WAN Miniport (Network Monitor)
10	Network	unknown	WAN Miniport (SSTP)
11	Network	unknown	Microsoft IP-HTTPS Platform Adapter
12	Network	unknown	WAN Miniport (PPTP)
13	Network	unknown	Intel(R) PRO/1000 MT Desktop Adapter
14	Network	unknown	Microsoft Kernel Debug Network Adapter
15	Network	unknown	WAN Miniport (PPPOE)
16	Network	unknown	Microsoft Teredo Tunneling Adapter
17	Network	unknown	WAN Miniport (IP)
18	Network	unknown	WAN Miniport (IKEv2)
19	Network	unknown	Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightW
20	Network	unknown	Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
21	Network	unknown	Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWe
22	Network	unknown	WAN Miniport (IP)-WFP Native MAC Layer LightWeight Filter-0000
23	Network	unknown	WAN Miniport (IP)-QoS Packet Scheduler-0000
24	Network	unknown	WAN Miniport (IPv6)-WFP Native MAC Layer LightWeight Filter-0000
25	Network	unknown	WAN Miniport (IPv6)-QoS Packet Scheduler-0000
26	Network	unknown	WAN Miniport (Network Monitor)-WFP Native MAC Layer LightWeight
27	Network	unknown	WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000
28	Disk Storage	unknown	D:\
29	Disk Storage	running	Fixed Disk
30	Keyboard	running	IBM enhanced (101- or 102-key) keyboard, Subtype=(0)

Software components:

Index	Name
1	Update for Windows 10 for x64-based Systems (KB5001716)
2	Microsoft Edge
3	Microsoft Edge Update
4	Microsoft Edge WebView2 Runtime

5. Vulnerabilities

1. Open UDP Ports:
Open UDP ports, particularly port 161 for SNMP, could be exploited by attackers to launch SNMP-based attacks, including enumeration of network devices, brute-force attacks on community strings, and even denial-of-service (DoS) attacks.

2. Information Disclosure:
SNMP enumeration reveals sensitive information about network devices, including system details, network configuration, routing tables, and installed software components. This information could be leveraged by attackers to conduct reconnaissance and plan targeted attacks.

3. Insecure SNMP Access Controls:
Inadequate access controls, such as the absence of proper authentication and authorization mechanisms, may allow unauthorized users to query SNMP-enabled devices, retrieve sensitive data, or perform unauthorized actions.

4. Weak SNMP Configuration:
Misconfigured SNMP settings, such as overly permissive access controls or excessive SNMP privileges granted to users, may increase the attack surface and expose devices to exploitation.

5. Lack of SNMP Monitoring:
Failure to actively monitor SNMP-enabled devices for unauthorized access attempts, abnormal behavior, or security incidents leaves the network vulnerable to exploitation and compromises.

6. Recommendations

- Upgrade SNMP to a more secure version (e.g., SNMPv3) with encryption and authentication capabilities.
- Implement robust access controls, including strong authentication mechanisms and granular authorization policies.
- Regularly audit SNMP configurations and monitor SNMP traffic for anomalies.
- Apply patches and updates to address known security vulnerabilities in SNMP implementations.
- Employ network segmentation and firewall rules to restrict access to SNMP services from trusted sources only.

Conclusion:

The assessment revealed vulnerabilities in SNMP-enabled devices, including default community strings and open ports. To enhance security, implement robust access controls, utilize SNMPv3 with strong authentication, and conduct regular audits. Vigilant monitoring is crucial to detect and respond to threats effectively, fortifying network resilience against potential attacks.