

SNMP Attacks and Security

1

CYBERDEFENCE SEMINAR

MAUNO PIHELGAS

Introduction

2

- What is SNMP?
- How can SNMP be exploited?
- How to make SNMP more secure?

Intro to SNMP

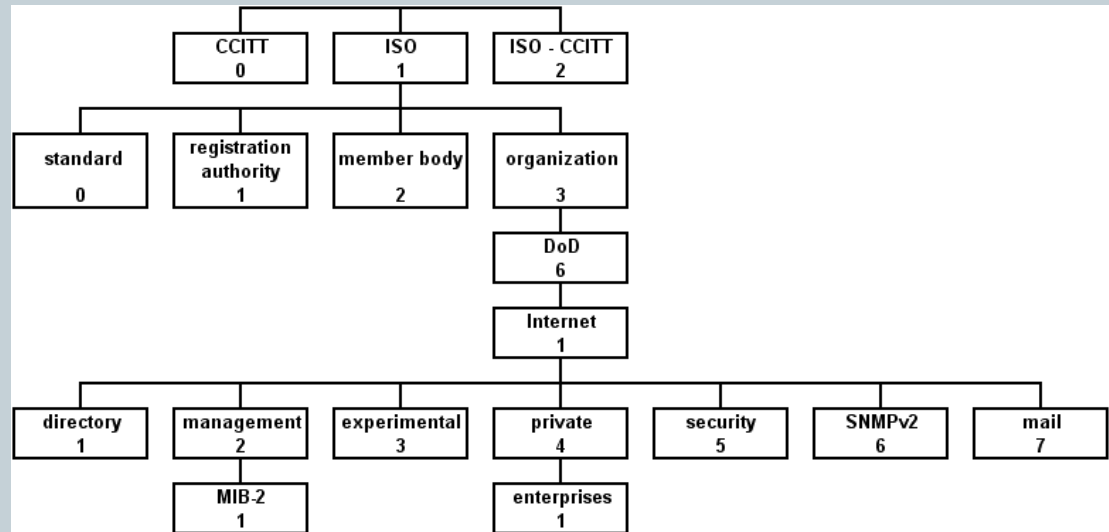
3

- **Simple Network Management Protocol**
- Used to monitor and manage network devices remotely
- Is now a standard protocol for network management
- Developed since 1987
 - Version 1
 - ✦ Initial implementation
 - ✦ Plain text password (community string)
 - Version 2c
 - ✦ Improved performance
 - Version 3
 - ✦ Encryption, message integrity, authentication
- **However all versions are still in use today**

Intro to SNMP

4

- SNMP is just a protocol
- Available information defined in MIB (**M**anagement **I**nformation **B**ase)
 - Differs per device and manufacturer
 - Hierarchically structured data
 - Object identifier (OID)



Intro to SNMP

5

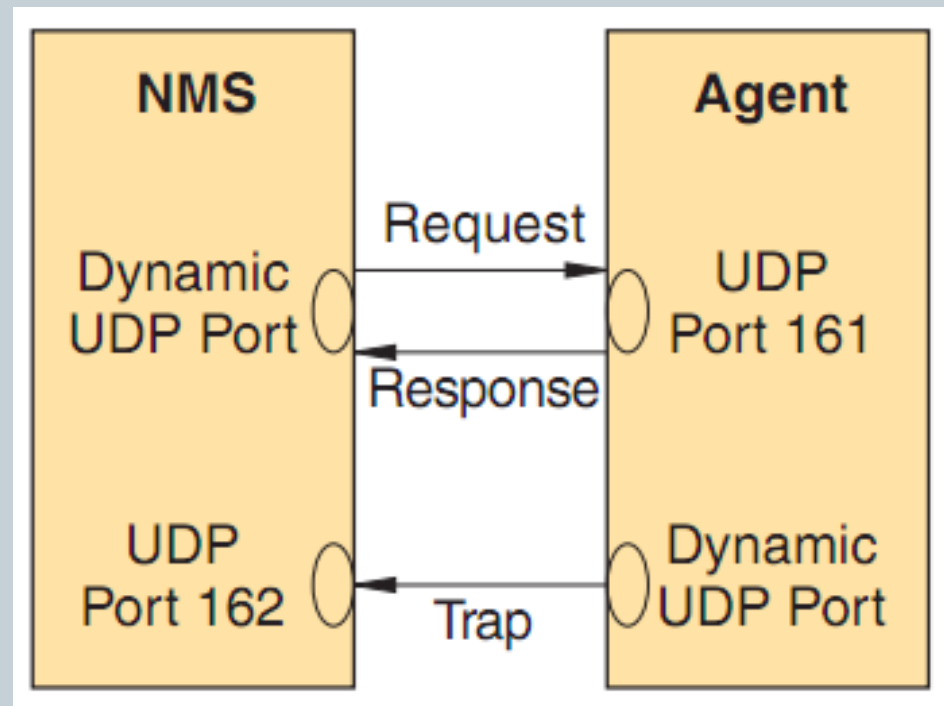
- How it works

- Polling

- ✦ GetRequest
 - Read-only
 - ✦ SetRequest
 - Read-write
 - ✦ Response

- Traps

- ✦ Trap message



SNMP vulnerabilities

6

- Systems often come preinstalled with SNMP
 - Administrator not aware
- Use of default configuration → **attacker can gain access to the system**
 - „public“ community string for read-only access
 - „private“ community string for read-write access
 - IP-based ACL often not used
- SNMP v1 and v2 are still widely used → **plain text password could be sniffed from network traffic**
- Packet header can be easily modified → **send false data**
 - UDP is connectionless
 - Source address spoofing

SNMP vulnerabilities

7

- After gaining read-only access
 - Practically all data in MIB can be read
 - ✦ System name, administrator → Social Engineering
 - ✦ Network interfaces, routing info, connections → Network layout
 - ✦ System type/version, uptime → Known vulnerabilities
 - ✦ Running processes, load, memory, mountpoints → System usage
 - ✦ etc

```
IP-MIB::ipNetToMediaPhysAddress.2.172.20.20.1 = STRING: 0:15:17:6f:60:27
IP-MIB::ipNetToMediaPhysAddress.2.172.20.20.2 = STRING: 0:13:46:f1:bf:57
IP-MIB::ipNetToMediaPhysAddress.2.172.20.20.122 = STRING: 0:1c:23:8d:3c:dc
IP-MIB::ipNetToMediaPhysAddress.2.172.20.20.129 = STRING: 0:1d:f:21:2:ce
IP-MIB::ipNetToMediaPhysAddress.2.172.20.20.130 = STRING: 0:c:29:9b:b8:f4
IP-MIB::ipNetToMediaNetAddress.2.172.20.20.1 = IpAddress: 172.20.20.1
IP-MIB::ipNetToMediaNetAddress.2.172.20.20.2 = IpAddress: 172.20.20.2
IP-MIB::ipNetToMediaNetAddress.2.172.20.20.122 = IpAddress: 172.20.20.122
IP-MIB::ipNetToMediaNetAddress.2.172.20.20.129 = IpAddress: 172.20.20.129
IP-MIB::ipNetToMediaNetAddress.2.172.20.20.130 = IpAddress: 172.20.20.130
```

SNMP vulnerabilities

8

- After gaining read-write access
 - Many attributes can be modified
 - ✦ Network interfaces can be set to „down“ state → Denial of Service attack
 - ✦ Routing could be manipulated → Gain access to other systems
 - ✦ etc

IF-MIB::ifDescr.1 = STRING: lo

IF-MIB::ifDescr.2 = STRING: eth0

IF-MIB::ifType.1 = INTEGER: softwareLoopback(24)

IF-MIB::ifType.2 = INTEGER: ethernetCsmacd(6)

IF-MIB::ifSpeed.1 = Gauge32: 10000000

IF-MIB::ifSpeed.2 = Gauge32: 10000000

IF-MIB::ifPhysAddress.1 = STRING:

IF-MIB::ifPhysAddress.2 = STRING: 0:c:29:68:ba:b6

IF-MIB::ifAdminStatus.1 = INTEGER: up(1)

IF-MIB::ifAdminStatus.2 = INTEGER: up(1)

Making SNMP more secure

9

1. Scan your network for SNMP-enabled devices
2. Only have SNMP enabled when it is necessary
3. Always change default community strings
 - Disable write access altogether when not required
4. Set up IP-based ACL
 - Additionally, configure your firewalls so that only necessary hosts have access to SNMP
5. Use SNMPv3 where possible
6. On some devices SNMP can be configured to use TCP
 - More reliable and difficult to tamper
 - Unfortunately not always supported

Conclusion

10

- SNMP is a standard monitoring and management protocol
 - Security has been an afterthought
- Extremely unsecure in its default configuration
- Fortunately can be configured to be quite secure

References

11

- Intrusion Detection FAQ: Using SNMP for Reconnaissance
<http://www.sans.org/security-resources/idfaq/snmp.php>
- Multiple Vulnerabilities in SNMP
<http://www.ists.dartmouth.edu/library/9.pdf>

Thank you for listening

12

ANY QUESTIONS?