Open SNMP Report

A scan report on your network or constituency

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG

Presentation Aims & Objectives

- Introduce what we mean by an Open SNMP service
- Introduce Shadowserver scans and methodology
- Highlight a sample Open SNMP report
- Describe key features of the report
- Demonstrate how a National CERT or network owner can action an Open SNMP report
- Offer guidance on how to protect and secure SNMP
- Provide a key list of Shadowserver online resources to enable report subscription and use

Internet-wide Scanning

- Shadowserver scans the entire IPv4 Internet for over 90 different network protocols every day (as of 2022-04-27), and also performs IPv6 scans based on IPv6 hitlists for selected protocols

- These are primarily "hello" type application scans

- Shadowserver does not exploit any vulnerability

- Scans allow for identifying misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or are simply just population enumeration

- Read more on why we scan at: https://www.shadowserver.org/news/the-scannings-will-continue-until-the-internet-improves/

Open SNMP

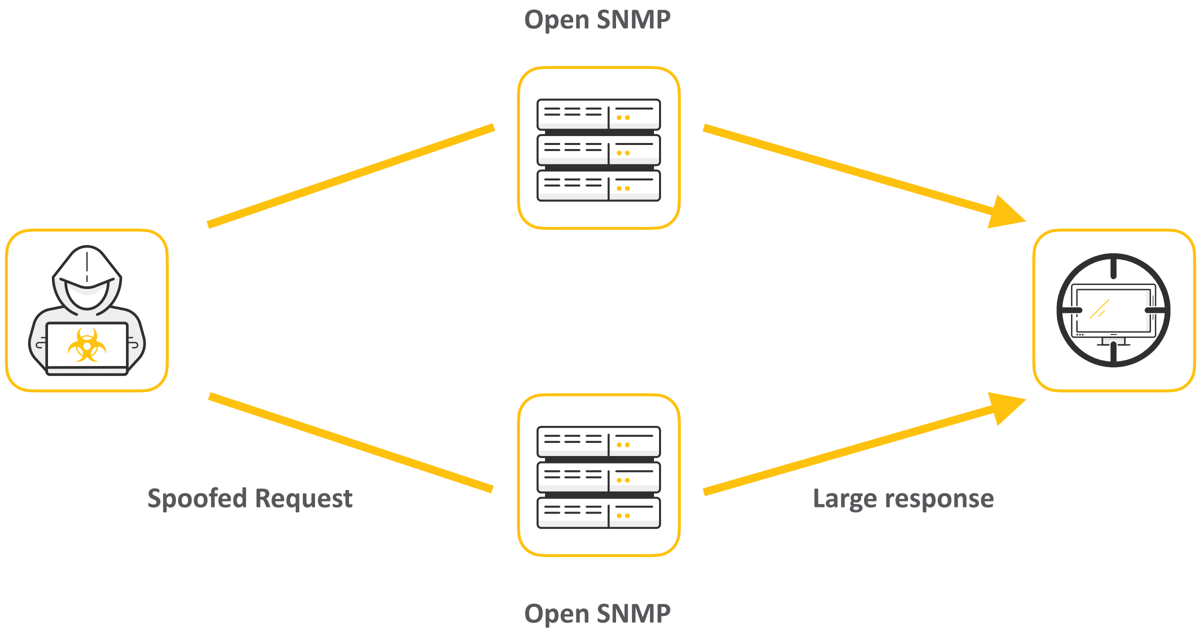
- SNMP (Simple Network Management Protocol) is deployed in networks for collecting information and managing network devices

- Devices such as routers, switches, servers and printers receive update queries from SNMP agents to monitor network performance and their configuration

- Publicly exposed SNMP services can be abused reflection-based distributed denial-of-service attack (DDoS)

- Publicly exposed SNMP services can lead to information leakage/ information disclosure

- IP address spoofing generates large responses to significantly smaller SNMP network queries, tricking servers to respond and flood the victim with data



SHADOWSERVER

Internet-wide Scanning - Open SNMP

- A project to search for publicly available Open SNMP servers: https://scan.shadowserver.org/snmp/

- These servers have the potential to be used in amplification attacks and if at all possible, we would like to see these services made un-available to attackers that would abuse these resources

- We are querying all computers with routable IPv4 addresses that are not firewalled from the internet on port 161/udp with a request for the System Description and System Name OIDs using the community "public" and snmp version 2c commands

- The OID being probed for is 1.3.6.1.2.1.1.1.0 (sysDescr) and if the host responds to that probe, the host is then probed for OID 1.3.6.1.2.1.1.5.0 (sysName)

- For an overview of UDP DNS amplification attacks please read:

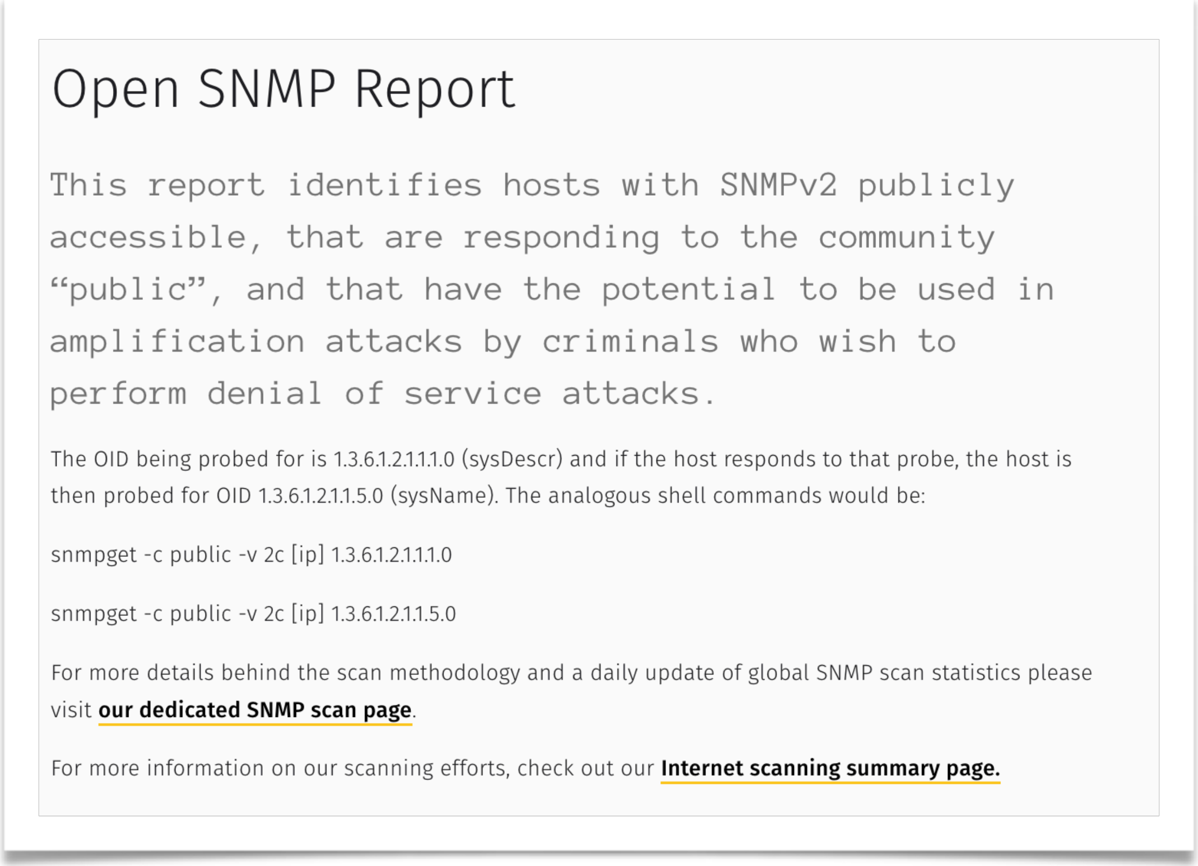
https://www.cisa.gov/uscert/ncas/alerts/TA14-017A

Open SNMP Report

- Open SNMP Report: https://www.shadowserver.org/what-we-do/network-reporting/open-snmp-report/
- This report identifies hosts with SNMPv2 publicly accessible, that are responding to the community "public", and that have the potential to be used in amplification attacks by criminals who wish to perform denial of service attacks.
- Report is available as a file in CSV format
- The report filename contains `scan_snmp`
- Reports can be sent as e-mail attachments, or downloaded via HTTP or obtained via a RESTful API
- All timestamps are in UTC
- For more documentation on API access, please visit the below URLs and send a request for access to contact@shadowserver.org

https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

Open SNMP Report Example



Open SNMP Report

This report identifies hosts with SNMPv2 publicly accessible, that are responding to the community “public”, and that have the potential to be used in amplification attacks by criminals who wish to perform denial of service attacks.

The OID being probed for is 1.3.6.1.2.1.1.1.0 (sysDescr) and if the host responds to that probe, the host is then probed for OID 1.3.6.1.2.1.1.5.0 (sysName). The analogous shell commands would be:

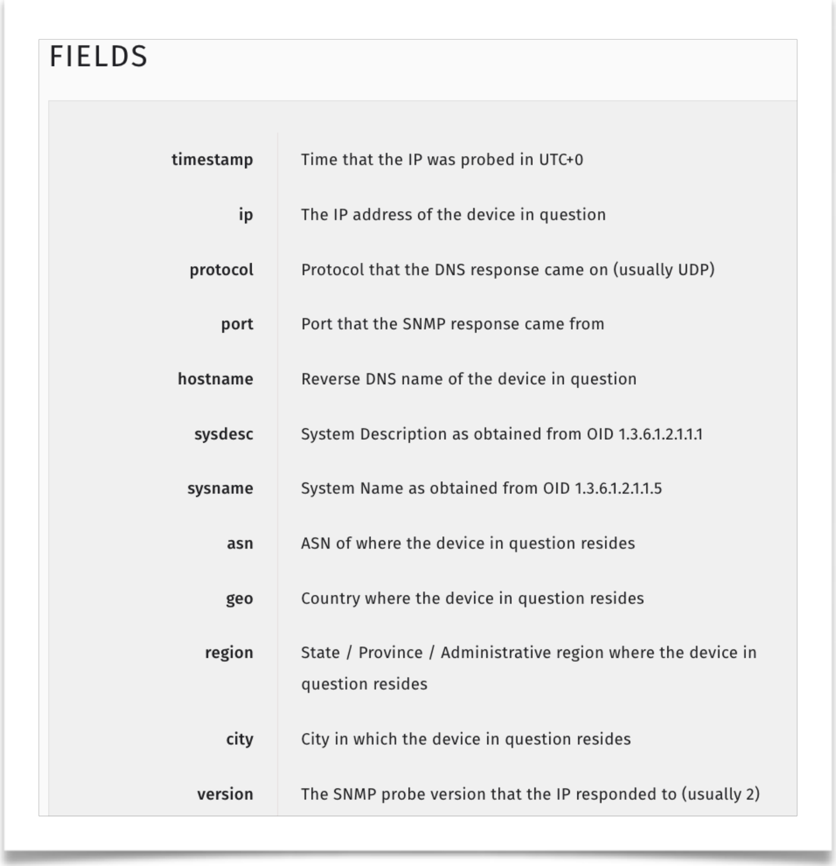
```
snmpget -c public -v 2c [ip] 1.3.6.1.2.1.1.1.0
```

```
snmpget -c public -v 2c [ip] 1.3.6.1.2.1.1.5.0
```

For more details behind the scan methodology and a daily update of global SNMP scan statistics please visit **our dedicated SNMP scan page**.

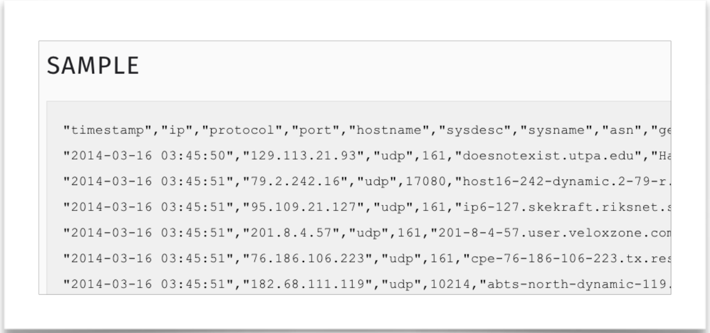
For more information on our scanning efforts, check out our **Internet scanning summary page.**

https://www.shadowserver.org/what-we-do/network-reporting/open-snmp-report/



FIELDS

timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the DNS response came on (usually UDP)
port	Port that the SNMP response came from
hostname	Reverse DNS name of the device in question
sysdesc	System Description as obtained from OID 1.3.6.1.2.1.1.1
sysname	System Name as obtained from OID 1.3.6.1.2.1.1.5
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides
version	The SNMP probe version that the IP responded to (usually 2)



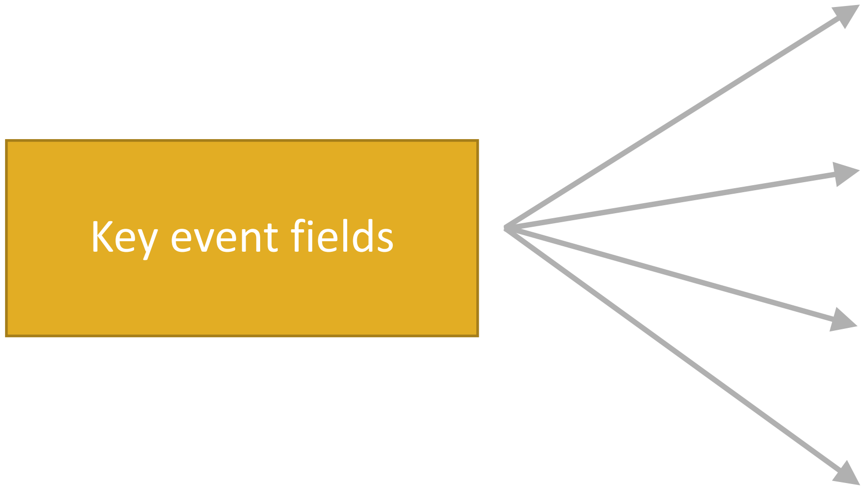
SAMPLE

```
"timestamp","ip","protocol","port","hostname","sysdesc","sysname","asn","ge
"2014-03-16 03:45:50","129.113.21.93","udp",161,"doesnotexist.utpa.edu","Ha
"2014-03-16 03:45:51","79.2.242.16","udp",17080,"host16-242-dynamic.2-79-r.
"2014-03-16 03:45:51","95.109.21.127","udp",161,"ip6-127.skekraft.riksnet.s
"2014-03-16 03:45:51","201.8.4.57","udp",161,"201-8-4-57.user.veloxzone.com
"2014-03-16 03:45:51","76.186.106.223","udp",161,"cpe-76-186-106-223.tx.res
"2014-03-16 03:45:51","182.68.111.119","udp",10214,"abts-north-dynamic-119.
```

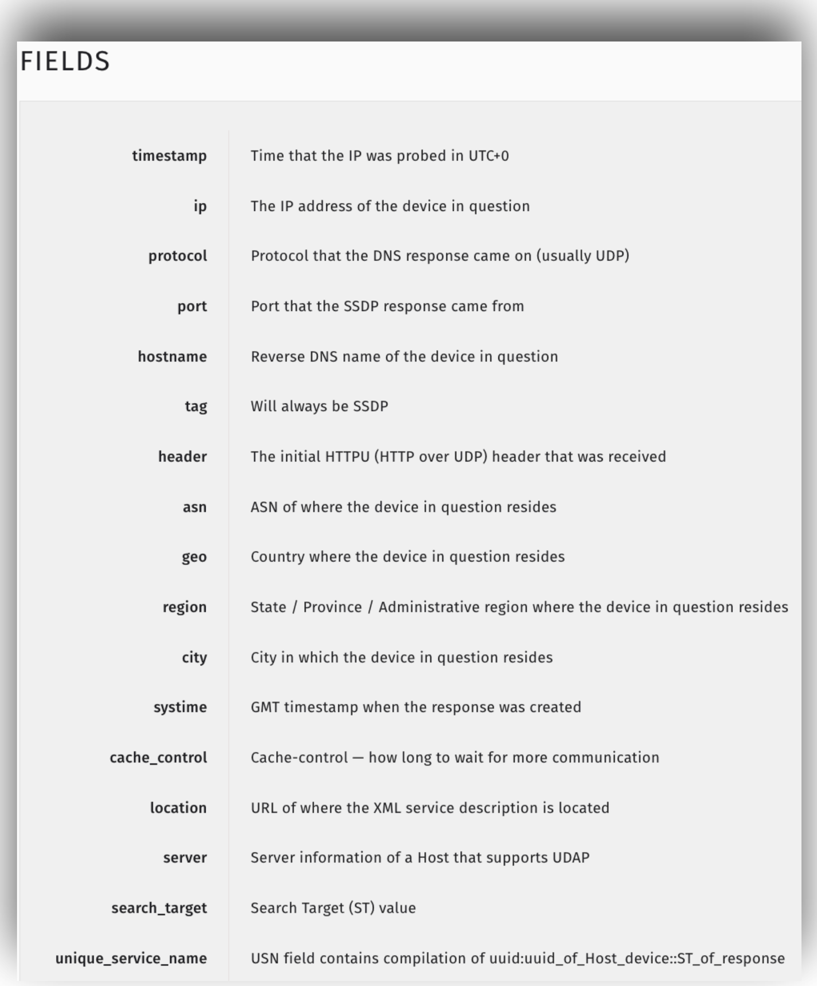
SHADOWSERVER

Action an Open SNMP report

timestamp	ip	protocol	port	hostname	sysdesc	sysname	asn	geo
05/03/2022 00:02	84.3.X,X	udp	161	54035b58.catv.pool.telekom.hu	D-Link Wireless Voice Gateway	CableHome	5483	HU



Key event fields

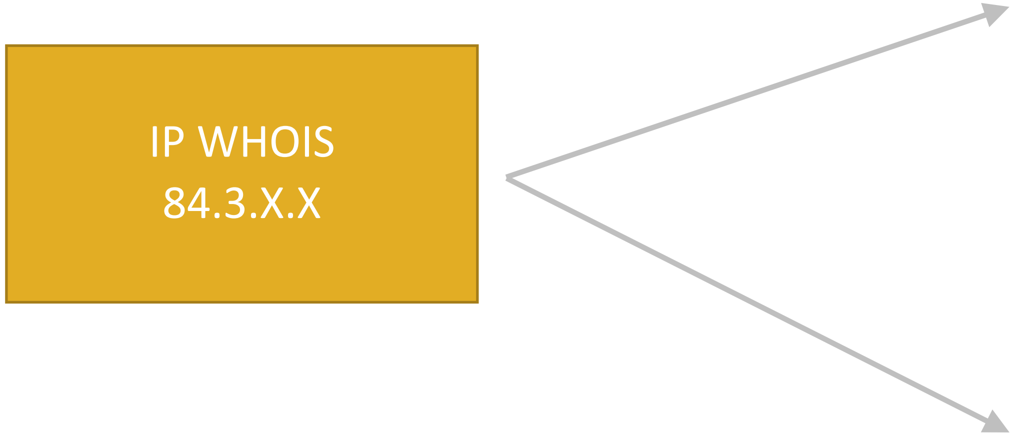


FIELDS

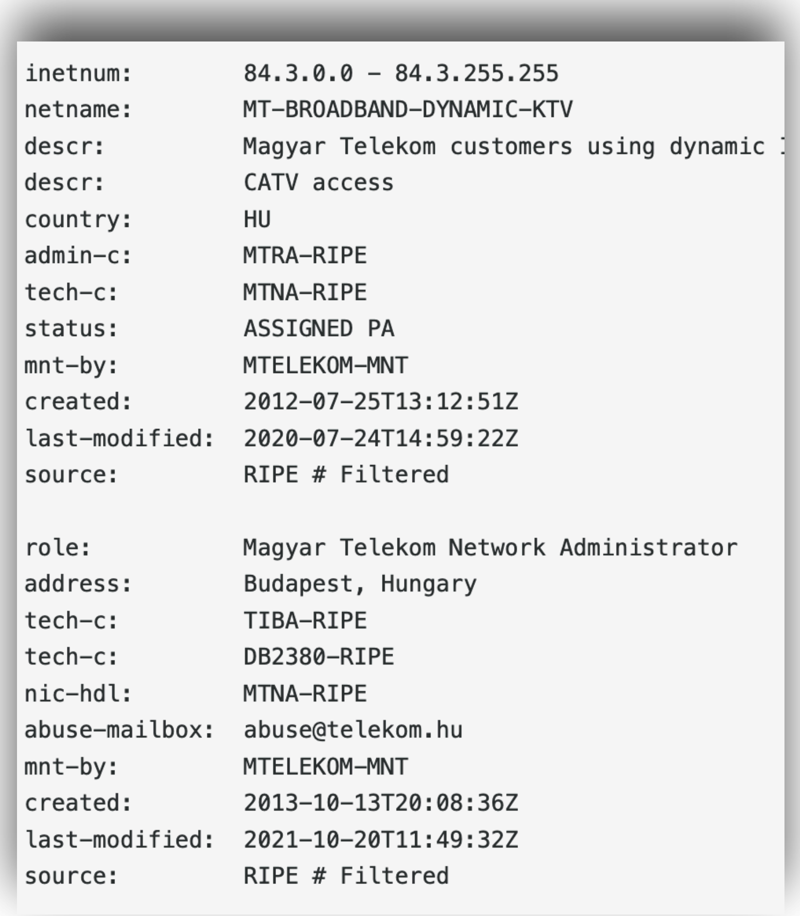
timestamp	Time that the IP was probed in UTC+0
ip	The IP address of the device in question
protocol	Protocol that the DNS response came on (usually UDP)
port	Port that the SSDP response came from
hostname	Reverse DNS name of the device in question
tag	Will always be SSDP
header	The initial HTTPU (HTTP over UDP) header that was received
asn	ASN of where the device in question resides
geo	Country where the device in question resides
region	State / Province / Administrative region where the device in question resides
city	City in which the device in question resides
systime	GMT timestamp when the response was created
cache_control	Cache-control — how long to wait for more communication
location	URL of where the XML service description is located
server	Server information of a Host that supports UDAP
search_target	Search Target (ST) value
unique_service_name	USN field contains compilation of uuid:uuid_of_Host_device::ST_of_response

Action an Open SNMP report

timestamp	ip	protocol	port	hostname	sysdesc	sysname	asn	geo
05/03/2022 00:02	84.3.X,X	udp	161	54035b58.catv.pool.telekom.hu	D-Link Wireless Voice Gateway	CableHome	5483	HU



IP WHOIS
84.3.X.X



```
inetnum:        84.3.0.0 - 84.3.255.255
netname:        MT-BROADBAND-DYNAMIC-KTV
descr:          Magyar Telekom customers using dynamic
descr:          CATV access
country:        HU
admin-c:        MTRA-RIPE
tech-c:         MTNA-RIPE
status:         ASSIGNED PA
mnt-by:         MTELEKOM-MNT
created:        2012-07-25T13:12:51Z
last-modified:  2020-07-24T14:59:22Z
source:         RIPE # Filtered

role:           Magyar Telekom Network Administrator
address:        Budapest, Hungary
tech-c:         TIBA-RIPE
tech-c:         DB2380-RIPE
nic-hdl:        MTNA-RIPE
abuse-mailbox:  abuse@telekom.hu
mnt-by:         MTELEKOM-MNT
created:        2013-10-13T20:08:36Z
last-modified:  2021-10-20T11:49:32Z
source:         RIPE # Filtered
```

Verifying our results

- The scan results may contain false positives if an actor attempts to spoof UDP replies to our scans

- In some cases when hosts have multiple interfaces we may register a scan response from another interface with another IP, but report it out as the IP we scanned for

- If you would like verify our results and to see if an SNMP aware device is open, try using the commands:
  - `snmpget -c public -v 2c [ip] 1.3.6.1.2.1.1.1.0`
  - `snmpget -c public -v 2c [ip] 1.3.6.1.2.1.1.5.0`
  - you will obtain device details if SNMP is open
  - if you are getting a timeout, make sure your queries are not being filtered

- Remember the scan results we share are for the previous day (up to 24 hour delay)

Open SNMP - PROTECT

- Configure a 'private' community with mandatory authentication instead of using the default 'public' community
- SNMP traffic probably has no viable need to leave your network so block access accordingly
- Disable SNMP on hosts when not in use and block SNMP traffic to ports 161/UDP and 162/UDP
- Create Access Control Lists (ACLs) and firewall management to restrict SNMP sessions by IP address
- Ensure network devices are up to date and patched
- Continuously monitor your network space for anomalous detections to ports 161 and 162 e.g. repeated failed attempts from external IP access

Summary & Key Report Pages

Reports overview

- https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
- https://www.shadowserver.org/what-we-do/network-reporting/
- https://www.shadowserver.org/what-we-do/network-reporting/open-snmp-report/

Report Updates

- https://www.shadowserver.org/news-insights/
- Twitter @shadowserver
- Mailing list access send request to contact@shadowserver.org and request access to public@shadowserver.org
- Or subscribe directly at https://mail.shadowserver.org/mailman/listinfo/public

Reports API

- Request access to contact@shadowserver.org
- https://www.shadowserver.org/what-we-do/network-reporting/api-documentation/
- https://www.shadowserver.org/what-we-do/network-reporting/api-reports-query/

SHADOWSERVER

Lighting the way to a more secure Internet

@shadowserver

contact@shadowserver.org

SHADOWSERVER.ORG