runZero

runZero IoT/OT Scanning

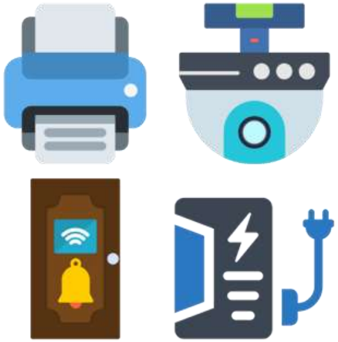
Huxley Barbee, Security Evangelist

What is IT vs IoT vs OT

IT

What is IT vs IoT vs OT

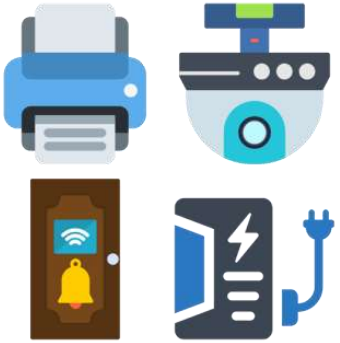
IoT



IT

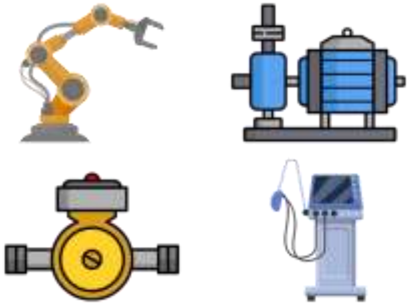
What is IT vs IoT vs OT

IoT



IT

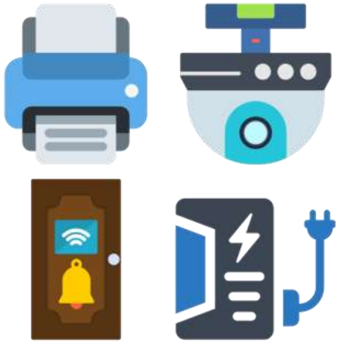
OT*



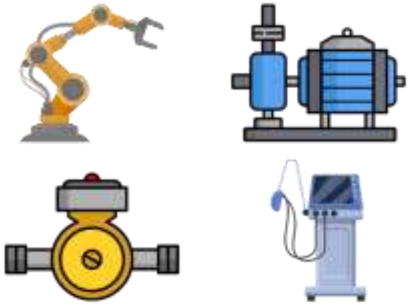
*Also IoMT

What is IT vs IoT vs OT

IoT



OT



Intro

- OT environments: crown jewels without the fortress
- Is OT recon this easy?
- Passively failing defensive scanning
- Five Principles of Active OT Scanning
- IoT: everywhere, anywhere, and right here

OT environments: crown jewels without the fortress

IT vs OT

IT	OT
Moving data	Moving machinery

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows, BSD	RTOS, >65 listed on wikipedia

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL
Periodic updates, even automated	Rare

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL
Periodic updates, even automated	Rare
Secure by design	Insecure by design

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL
Periodic updates, even automated	Rare
Secure by design	Insecure by design
Many security controls	Some to none, depending on industry

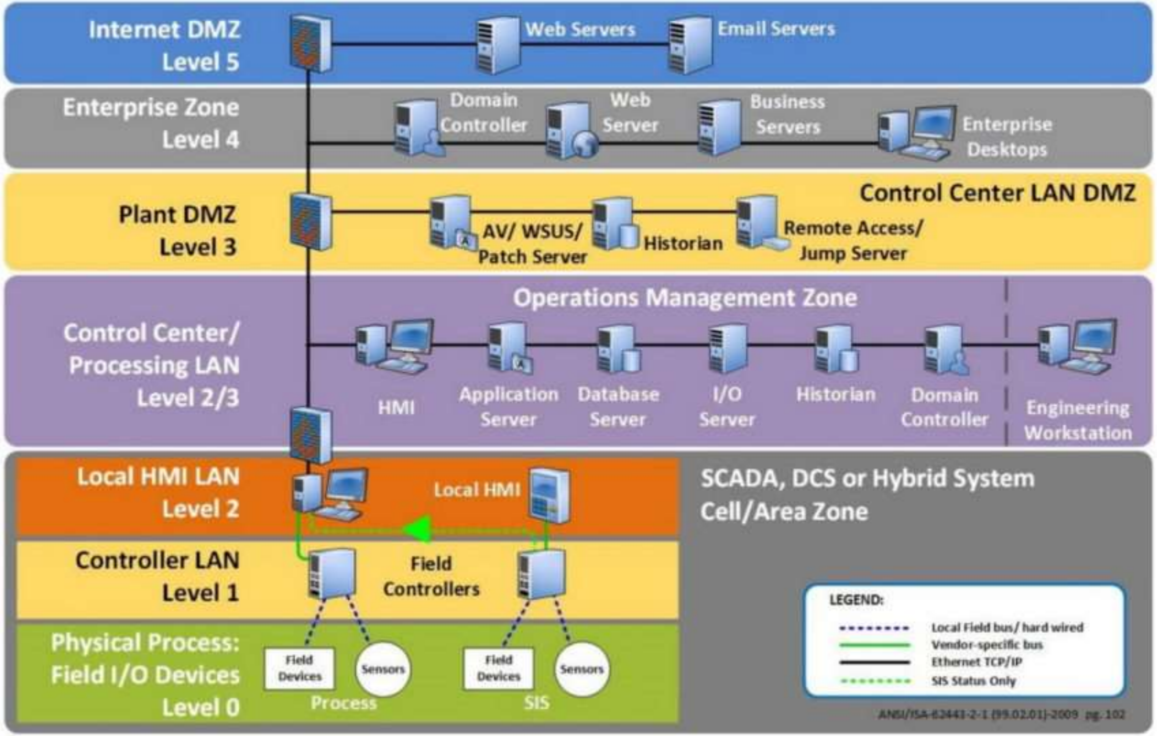
IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL
Periodic updates, even automated	Rare
Secure by design	Insecure by design
Many security controls	Some to none, depending on industry
High exposure	Mostly isolated

IT vs OT

IT	OT
Moving data	Moving machinery
3 - 5 years	20 - 30 years
Confidentiality	Availability*
Linux, OSX, Windows	RTOS, >65 listed on wikipedia
Python, Java, JavaScript, C++, Go	LD, FBD, SFC, ST, IL
Periodic updates, even automated	Rare
Secure by design	Insecure by design
Many security controls	Some to none, depending on industry
High exposure	Mostly isolated
IP, TCP, UDP	DNP3, ModBus

Security through isolation, but not really

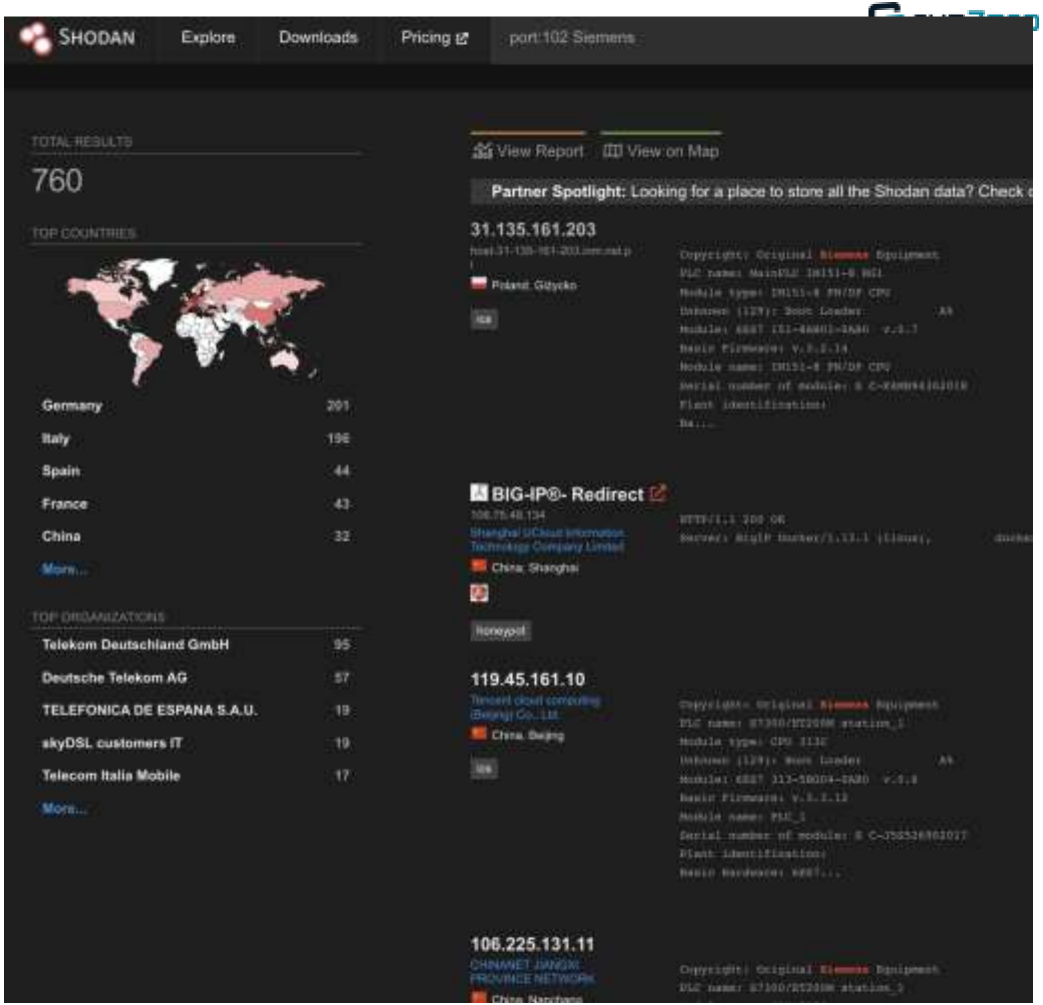


ANSI/ISA-62443-2-1 (99.02.01)-2009 pg. 102

Is offense OT this easy?

Security through isolation?

Shodan



TOTAL RESULTS

760

TOP COUNTRIES

Germany	201
Italy	196
Spain	44
France	43
China	32

More...

TOP ORGANIZATIONS

Telekom Deutschland GmbH	95
Deutsche Telekom AG	57
TELEFONICA DE ESPANA S.A.U.	19
skyDSL customers IT	19
Telecom Italia Mobile	17

More...

Partner Spotlight: Looking for a place to store all the Shodan data? Check

31.135.161.203

host-31-135-161-203.[illegible].net.pl

Poland, Giżycko

ics

```
Copyright: Original Siemens Equipment
PLC name: MainPLC IM151-8 HG1
Module type: IM151-8 PN/DP CPU
Unknown (129): Boot Loader          A?
Module: 6ES7 151-8AB01-0AB0  v.3.?
Basic Firmware: v.3.2.14
Module name: IM151-8 PN/DP CPU
Serial number of module: S C-X4M094162016
Plant identification:
Ba...
```

BIG-IP®- Redirect

106.75.48.134

Shanghai UCloud Information Technology Company Limited

China, Shanghai

honeypot

```
HTTP/1.1 200 OK
Server: BigIP Docker/1.13.1 (Linux),        docker
```

119.45.161.10

Tencent cloud computing (Beijing) Co., Ltd.

China, Beijing

ics

```
Copyright: Original Siemens Equipment
PLC name: S7300/ET200M station_1
Module type: CPU 313C
Unknown (129): Boot Loader          A?
Module: 6ES7 313-5BG04-0AB0  v.3.3
Basic Firmware: v.3.3.12
Module name: PLC_1
Serial number of module: S C-J5S526902017
Plant identification:
Basic Hardware: 6ES7...
```

106.225.131.11

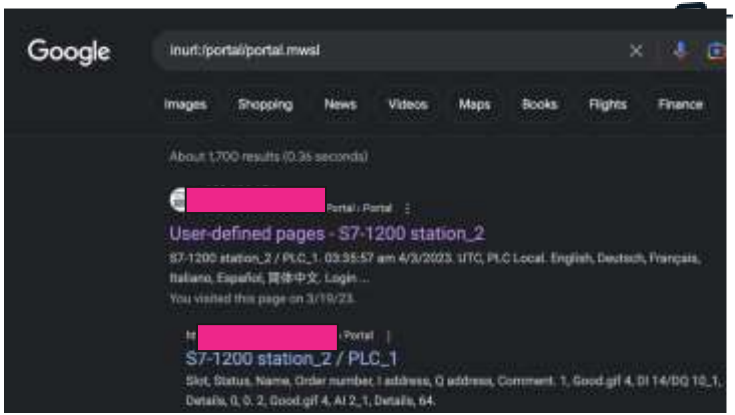
CHINANET JIANGXI PROVINCE NETWORK

China, Nanchang

```
Copyright: Original Siemens Equipment
PLC name: S7300/ET200M station_1
```

Security through isolation?

Google



inurl:/portal/portal.mwsl

About 1,700 results (0.36 seconds)

[redacted] › Portal › Portal

User-defined pages - S7-1200 station_2

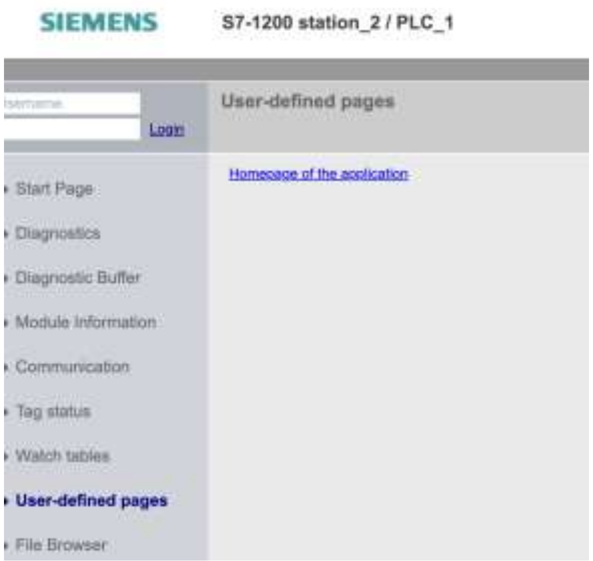
S7-1200 station_2 / PLC_1. 03:35:57 am 4/3/2023. UTC, PLC Local. English, Deutsch, Français, Italiano, Español, 简体中文. Login ...

You visited this page on 3/19/23.

ht[redacted] › Portal

S7-1200 station_2 / PLC_1

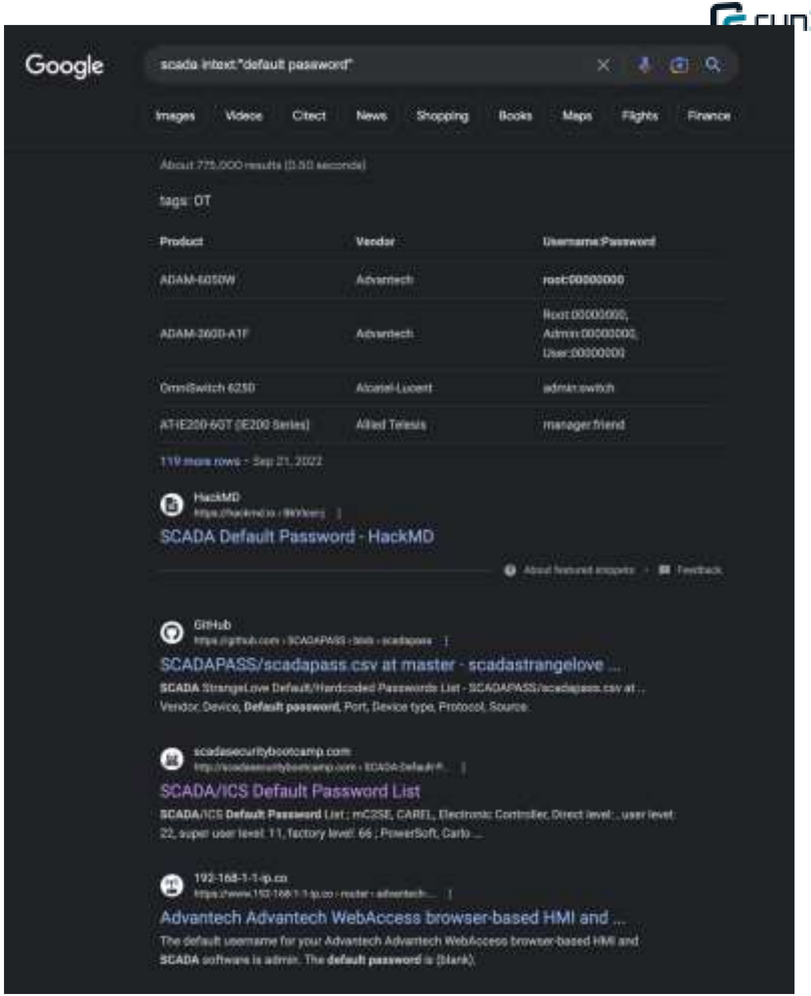
Slot, Status, Name, Order number, I address, Q address, Comment. 1, Good.gif 4, DI 14/DQ 10_1, Details, 0, 0. 2, Good.gif 4, AI 2_1, Details, 64.



Default passwords

Default users

Default settings



scada intext:"default password"

About 775,000 results (0.50 seconds)

tags: OT

Product	Vendor	Username:Password
ADAM-6050W	Advantech	**root:00000000**
ADAM-3600-A1F	Advantech	Root:00000000, Admin:00000000, User:00000000
OmniSwitch 6250	Alcatel-Lucent	admin:switch
AT-IE200-6GT (IE200 Series)	Allied Telesis	manager:friend

119 more rows · Sep 21, 2022

HackMD
https://hackmd.io › [illegible]

SCADA Default Password - HackMD

About featured snippets · Feedback

GitHub
https://github.com › SCADAPASS › blob › scadapass

SCADAPASS/scadapass.csv at master · scadastrangelove ...

SCADA StrangeLove Default/Hardcoded Passwords List - SCADAPASS/scadapass.csv at ... Vendor, Device, **Default password**, Port, Device type, Protocol, Source.

scadasecuritybootcamp.com
http://scadasecuritybootcamp.com › SCADA-Default-P...

SCADA/ICS Default Password List

SCADA/ICS **Default Password** List ; mC2SE, CAREL, Electronic Controller, Direct level: , user level: 22, super user level: 11, factory level: 66 ; PowerSoft, Carlo ...

192-168-1-1-ip.co
https://www.192-168-1-1-ip.co › router › advantech-...

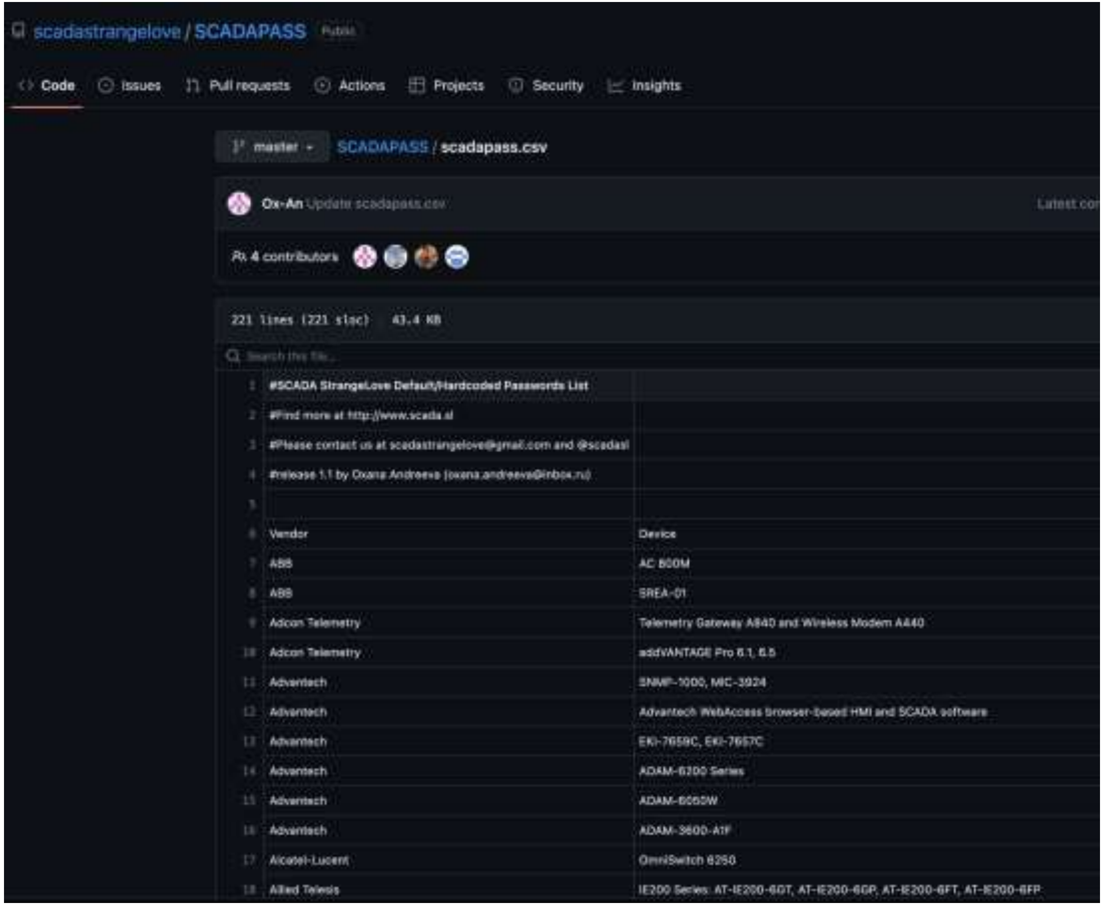
Advantech Advantech WebAccess browser-based HMI and ...

The default username for your Advantech Advantech WebAccess browser-based HMI and **SCADA** software is admin. The **default password** is (blank).

Default passwords

Default users

Default settings



scadastrangelove / SCADAPASS

SCADAPASS / scadapass.csv

Ox-An Update scadapass.csv

Latest co

4 contributors

221 lines (221 sloc) 43.4 KB

#SCADA StrangeLove Default/Hardcoded Passwords List

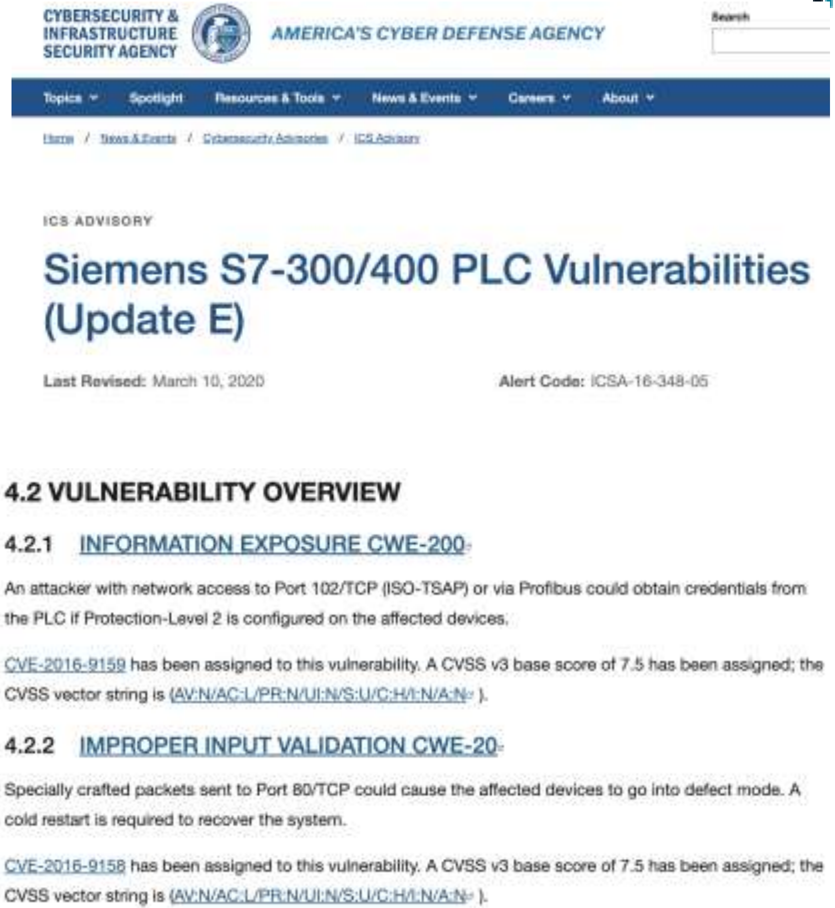
#Find more at http://www.scada.sl

#Please contact us at scadastrangelove@gmail.com and @scadasl

#release 1.1 by Oxana Andreeva (oxana.andreeva@inbox.ru)

Vendor	Device
ABB	AC 800M
ABB	SREA-01
Adcon Telemetry	Telemetry Gateway A840 and Wireless Modem A440
Adcon Telemetry	addVANTAGE Pro 6.1, 6.5
Advantech	SNMP-1000, MIC-3924
Advantech	Advantech WebAccess browser-based HMI and SCADA software
Advantech	EKI-7659C, EKI-7657C
Advantech	ADAM-6200 Series
Advantech	ADAM-6050W
Advantech	ADAM-3600-A1F
Alcatel-Lucent	OmniSwitch 6250
Allied Telesis	IE200 Series: AT-IE200-6GT, AT-IE200-6GP, AT-IE200-6FT, AT-IE200-6FP

Vulnerabilities



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / News & Events / Cybersecurity Advisories / ICS Advisory

ICS ADVISORY

Siemens S7-300/400 PLC Vulnerabilities (Update E)

Last Revised: March 10, 2020

Alert Code: ICSA-16-348-05

4.2 VULNERABILITY OVERVIEW

4.2.1 INFORMATION EXPOSURE CWE-200

An attacker with network access to Port 102/TCP (ISO-TSAP) or via Profibus could obtain credentials from the PLC if Protection-Level 2 is configured on the affected devices.

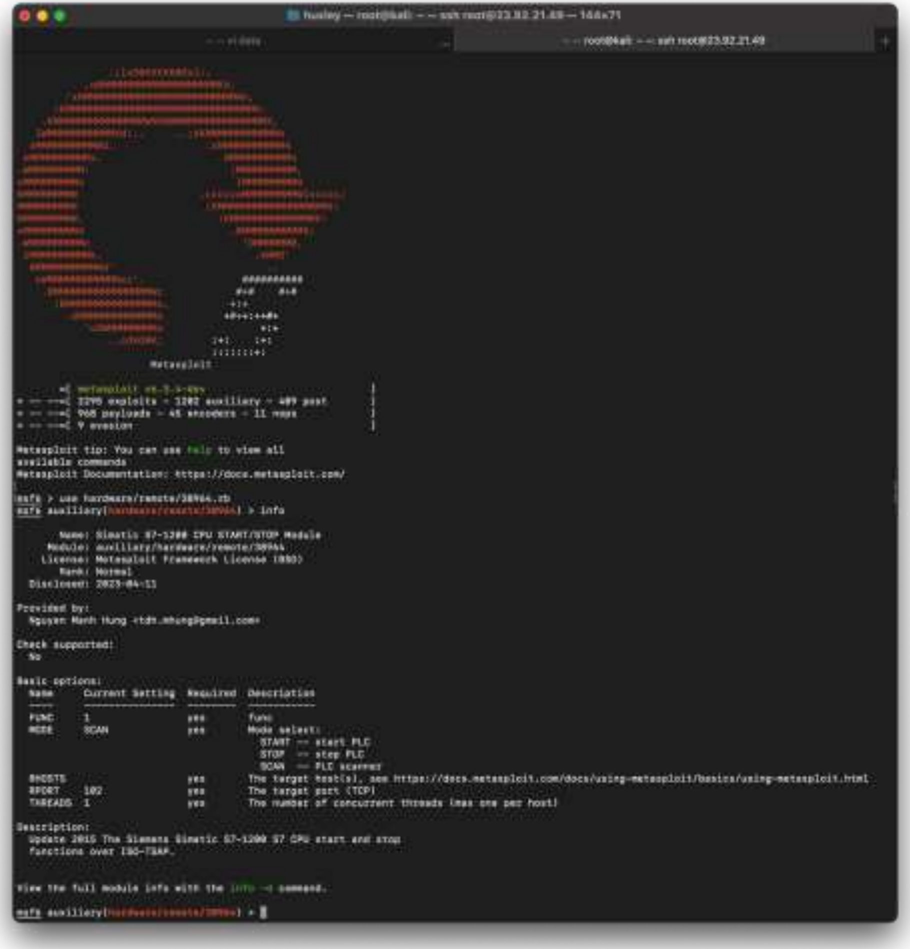
CVE-2016-9159 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

4.2.2 IMPROPER INPUT VALIDATION CWE-20

Specially crafted packets sent to Port 80/TCP could cause the affected devices to go into defect mode. A cold restart is required to recover the system.

CVE-2016-9158 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

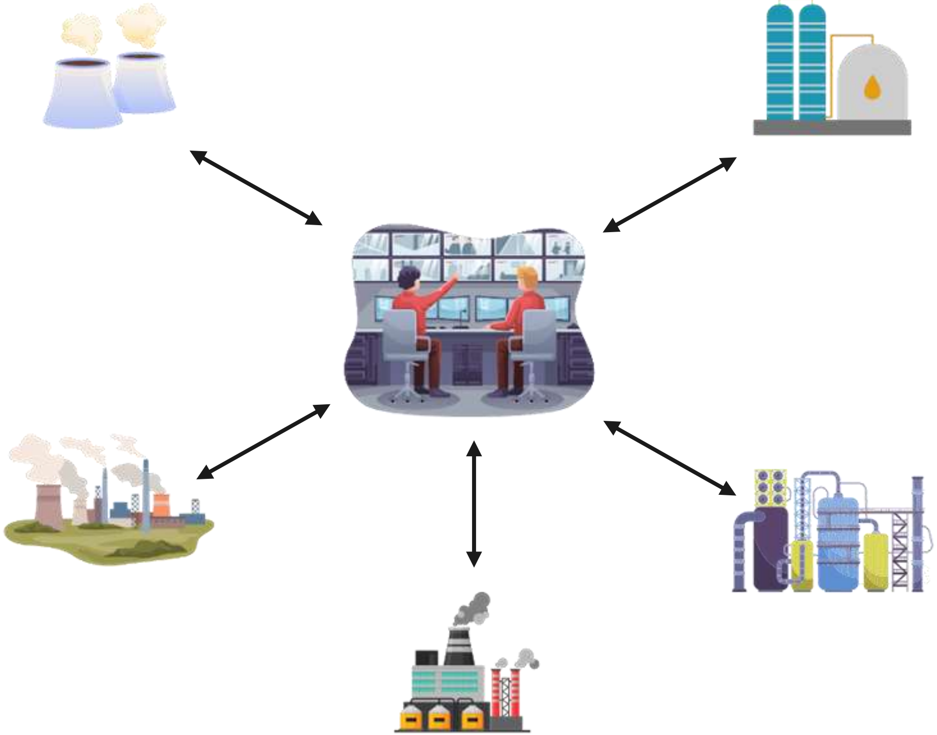
Exploit



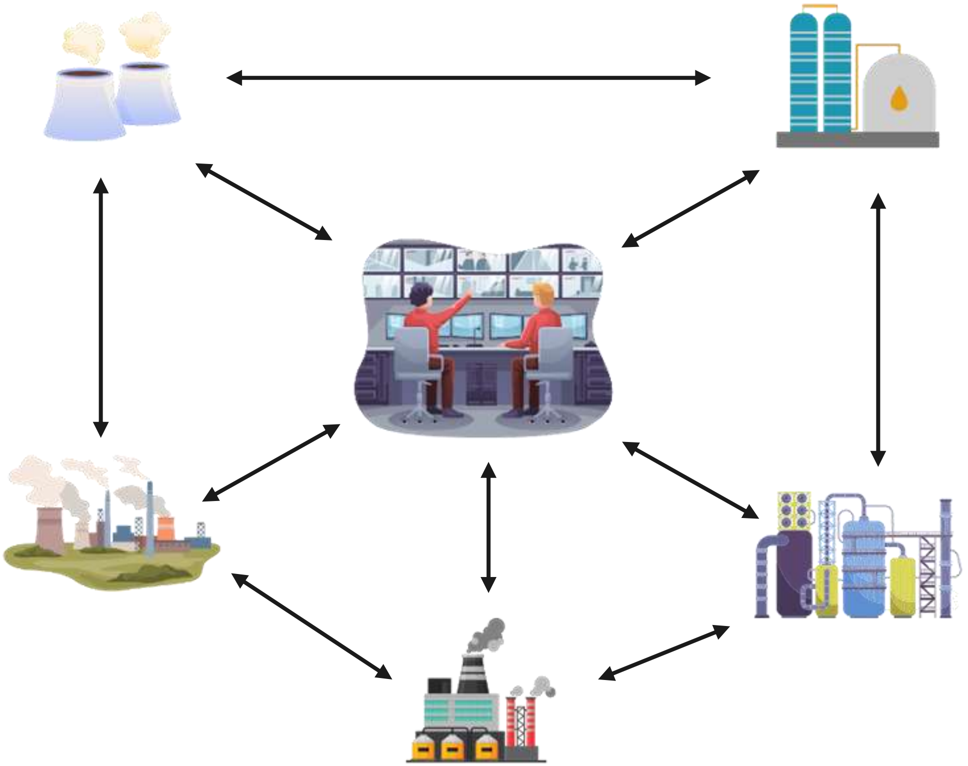
```
huxley — root@kali: ~ — ssh root@23.92.21.49 — 144x71

                        Metasploit

       =[ metasploit v6.3.1-dev                          ]
+ -- --=[ 2295 exploits - 1202 auxiliary - 409 post      ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use hardware/remote/38964.rb
msf6 auxiliary(hardware/remote/38964) > info

       Name: Simatic S7-1200 CPU START/STOP Module
     Module: auxiliary/hardware/remote/38964
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2023-04-11

Provided by:
  Nguyen Manh Hung <tdh.mhung@gmail.com>

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  FUNC     1                yes       func
  MODE     SCAN             yes       Mode select:
                                        START -- start PLC
                                        STOP  -- stop PLC
                                        SCAN  -- PLC scanner
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT    102              yes       The target port (TCP)
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Update 2015 The Siemens Simatic S7-1200 S7 CPU start and stop
  functions over ISO-TSAP.


View the full module info with the info -d command.

msf6 auxiliary(hardware/remote/38964) > 
```

Passively failing defensive scanning

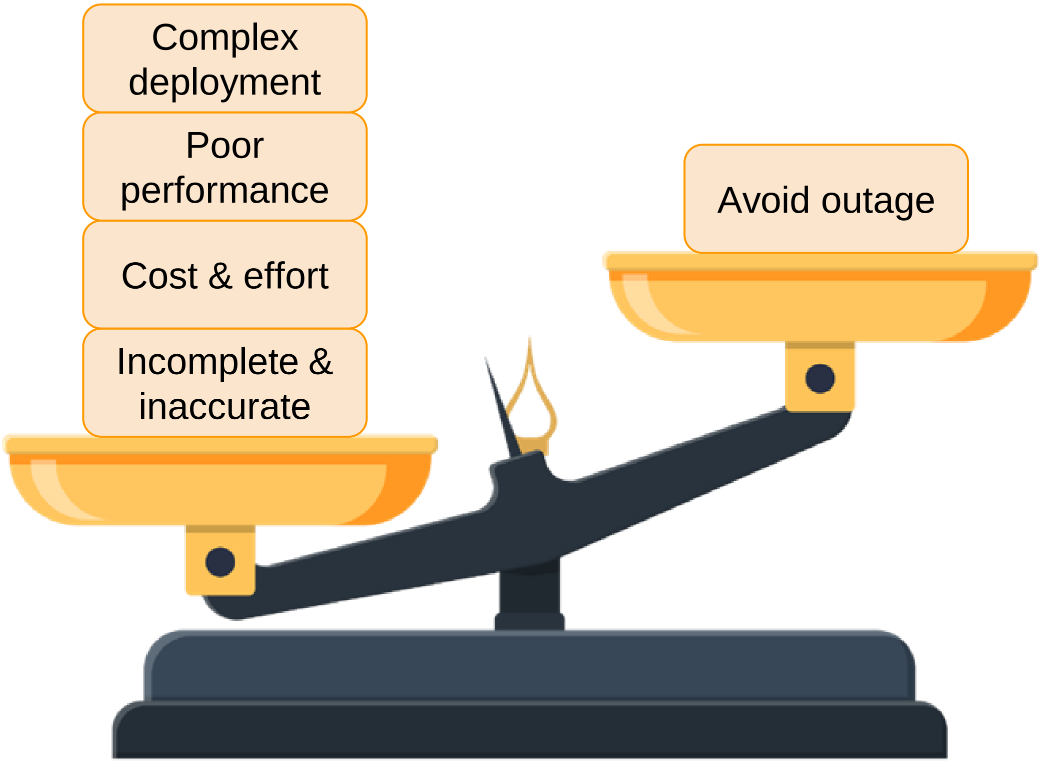
Finding chokepoints



Finding chokepoints



Good and bad of passive network monitor



Complex deployment

Poor performance

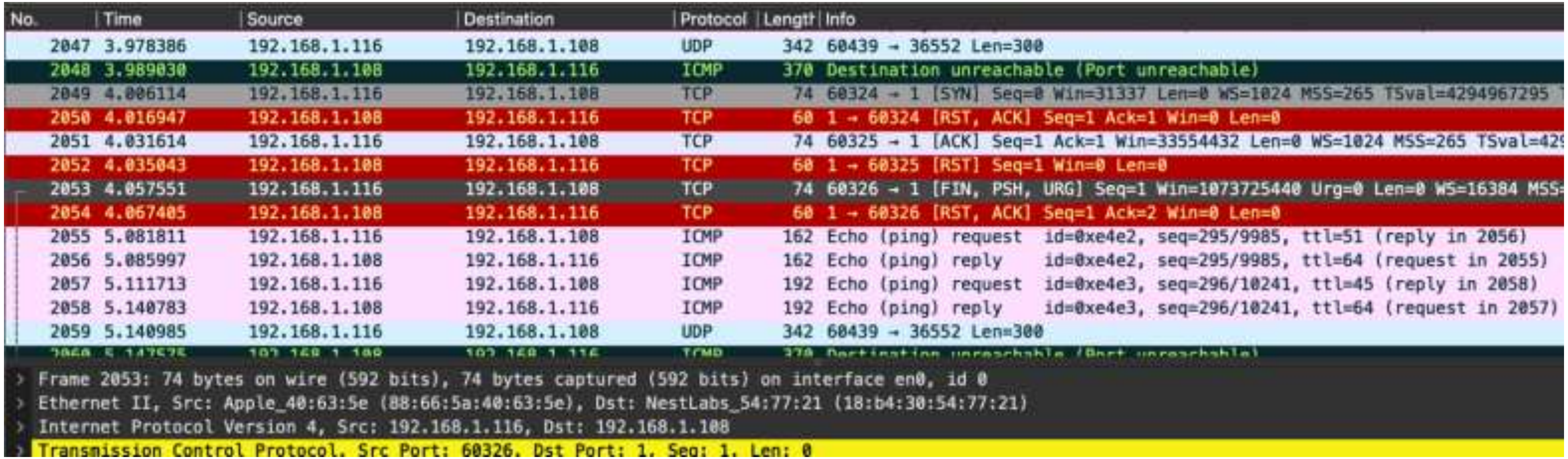
Cost & effort

Incomplete & inaccurate

Avoid outage

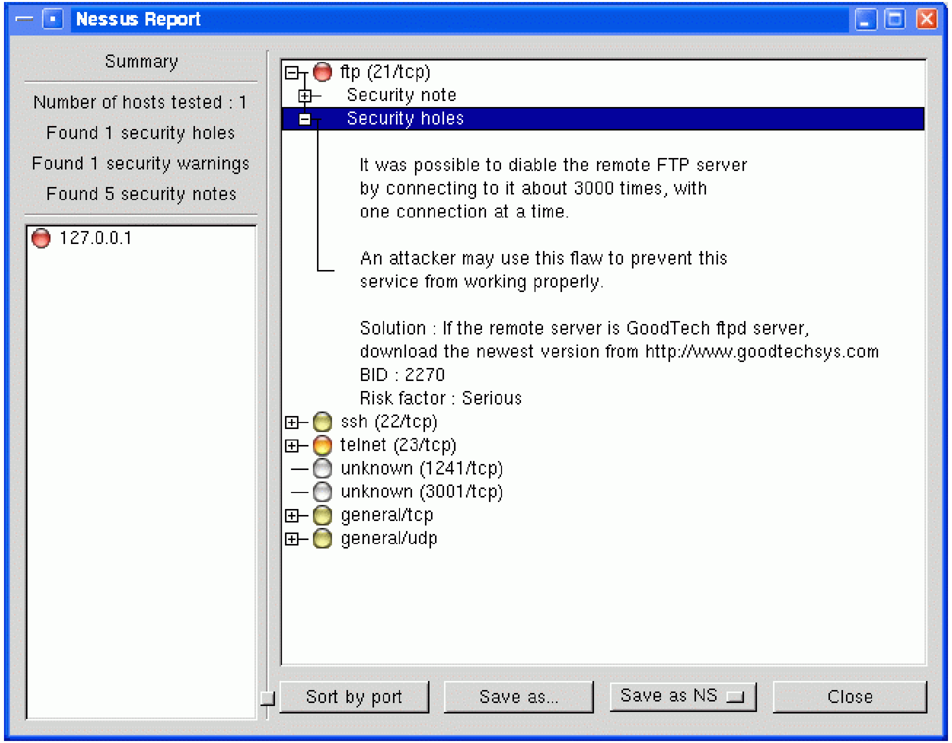
Five Principles of Active OT Scanning

1/5: Send standard packets and expected payloads



```
No.     Time        Source          Destination     Protocol  Length Info
  2047 3.978386    192.168.1.116   192.168.1.108   UDP       342  60439 → 36552 Len=300
  2048 3.989030    192.168.1.108   192.168.1.116   ICMP      370  Destination unreachable (Port unreachable)
  2049 4.006114    192.168.1.116   192.168.1.108   TCP        74  60324 → 1 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS=265 TSval=4294967295 T
  2050 4.016947    192.168.1.108   192.168.1.116   TCP        60  1 → 60324 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  2051 4.031614    192.168.1.116   192.168.1.108   TCP        74  60325 → 1 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS=1024 MSS=265 TSval=429
  2052 4.035043    192.168.1.108   192.168.1.116   TCP        60  1 → 60325 [RST] Seq=1 Win=0 Len=0
  2053 4.057551    192.168.1.116   192.168.1.108   TCP        74  60326 → 1 [FIN, PSH, URG] Seq=1 Win=1073725440 Urg=0 Len=0 WS=16384 MSS=
  2054 4.067405    192.168.1.108   192.168.1.116   TCP        60  1 → 60326 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
  2055 5.081811    192.168.1.116   192.168.1.108   ICMP      162  Echo (ping) request  id=0xe4e2, seq=295/9985, ttl=51 (reply in 2056)
  2056 5.085997    192.168.1.108   192.168.1.116   ICMP      162  Echo (ping) reply    id=0xe4e2, seq=295/9985, ttl=64 (request in 2055)
  2057 5.111713    192.168.1.116   192.168.1.108   ICMP      192  Echo (ping) request  id=0xe4e3, seq=296/10241, ttl=45 (reply in 2058)
  2058 5.140783    192.168.1.108   192.168.1.116   ICMP      192  Echo (ping) reply    id=0xe4e3, seq=296/10241, ttl=64 (request in 2057)
  2059 5.140985    192.168.1.116   192.168.1.108   UDP       342  60439 → 36552 Len=300
  2060 5.147575    192.168.1.108   192.168.1.116   ICMP      370  Destination unreachable (Port unreachable)

> Frame 2053: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface en0, id 0
> Ethernet II, Src: Apple_40:63:5e (88:66:5a:40:63:5e), Dst: NestLabs_54:77:21 (18:b4:30:54:77:21)
> Internet Protocol Version 4, Src: 192.168.1.116, Dst: 192.168.1.108
> Transmission Control Protocol, Src Port: 60326, Dst Port: 1, Seq: 1, Len: 0
```

2/5: Avoid security probes



Number of hosts tested : 1
Found 1 security holes
Found 1 security warnings
Found 5 security notes

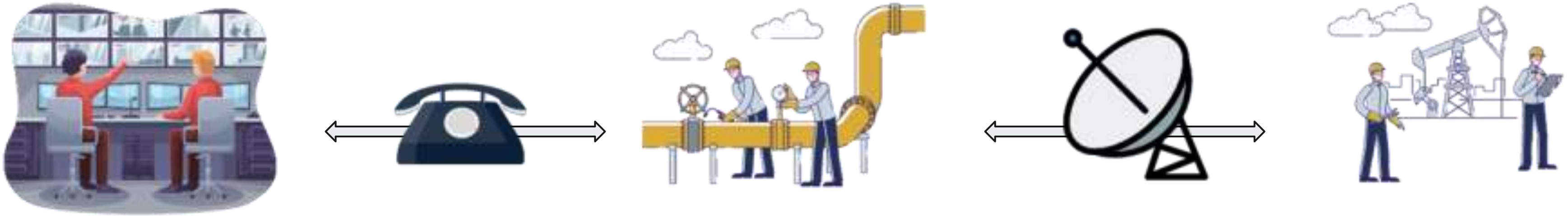
● 127.0.0.1

● ftp (21/tcp)
Security note
Security holes

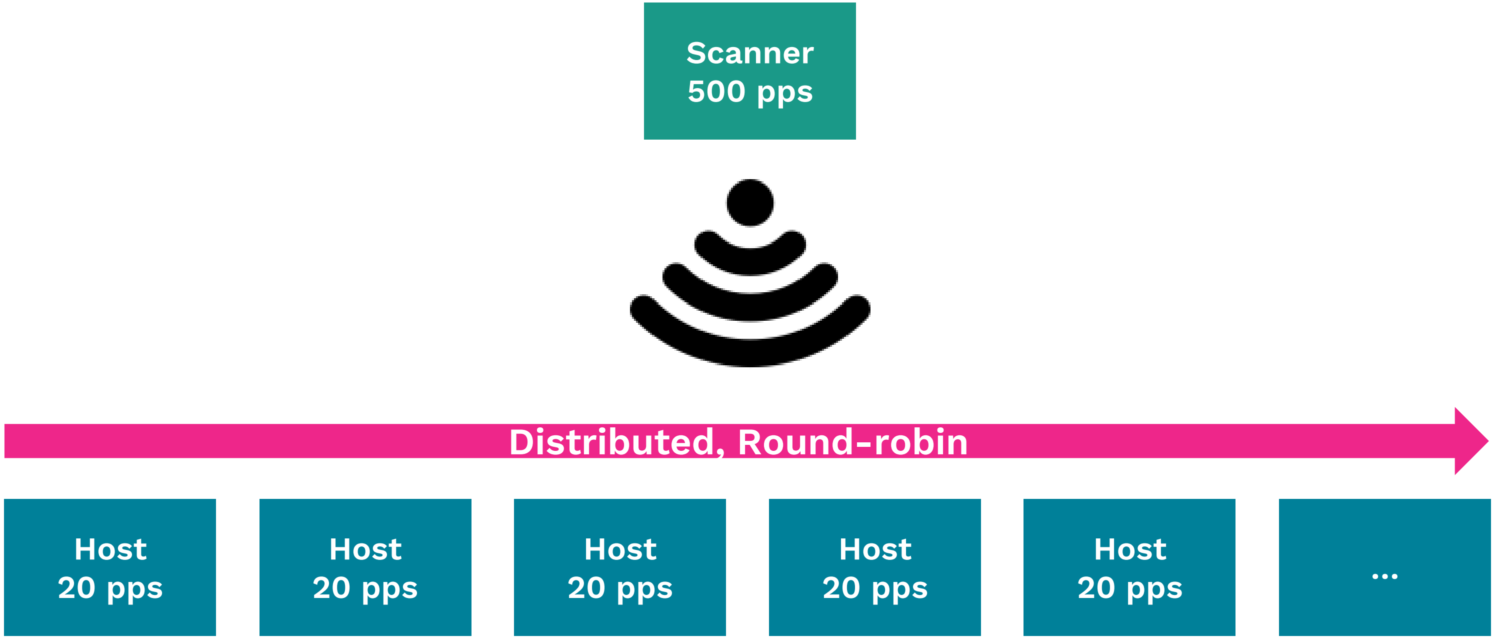
```
It was possible to diable the remote FTP server
by connecting to it about 3000 times, with
one connection at a time.

An attacker may use this flaw to prevent this
service from working properly.

Solution : If the remote server is GoodTech ftpd server,
download the newest version from http://www.goodtechsys.com
BID : 2270
Risk factor : Serious
```

● ssh (22/tcp)
● telnet (23/tcp)
○ unknown (1241/tcp)
○ unknown (3001/tcp)
● general/tcp
● general/udp

3/5: Manage overall and per host packet count to avoid heavy traffic



3/5: Manage overall and per host packet count to avoid heavy traffic



Scanner
500 pps

Distributed, Round-robin

Host
20 pps

Host
20 pps

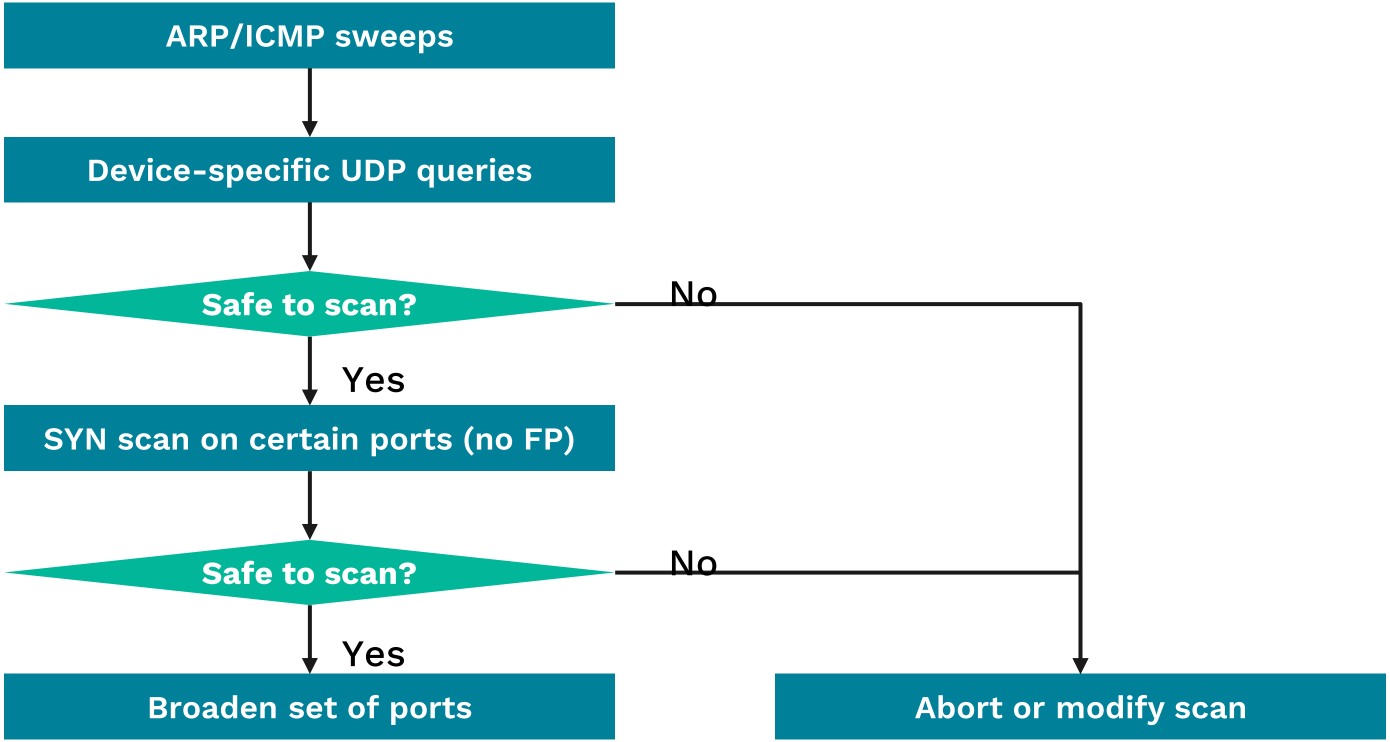
Host
20 pps

Host
20 pps

Host
20 pps

...

4/5: Fingerprint incrementally

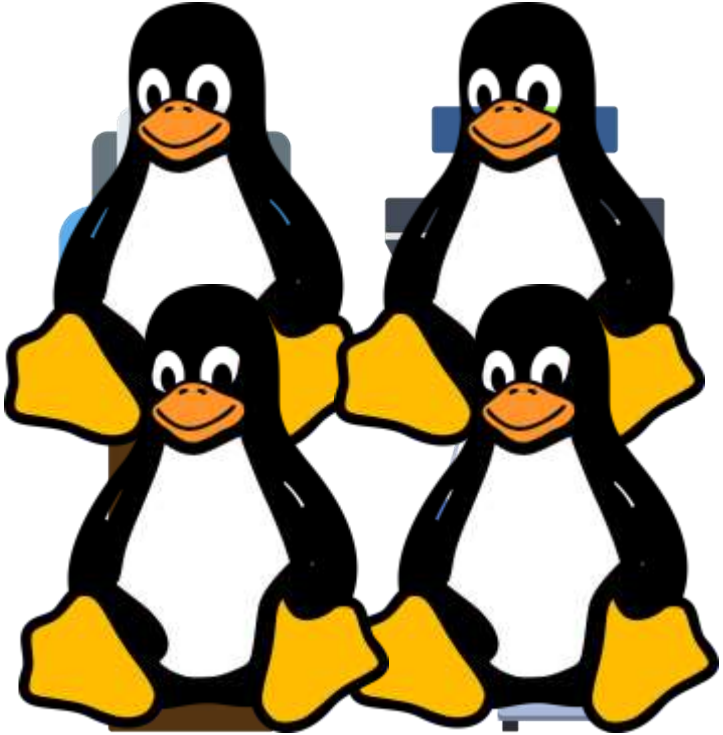


Five Principles

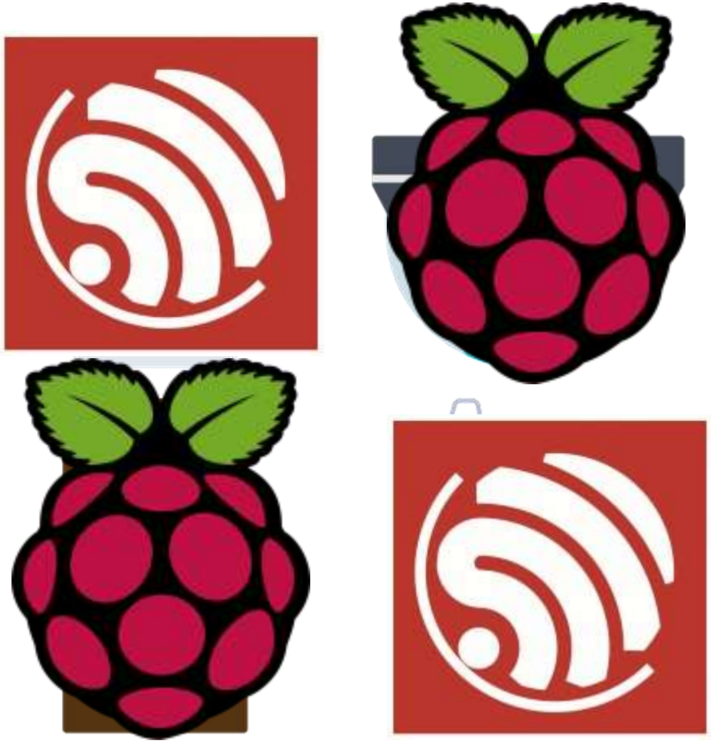
- Send standard packets and expected payloads
- Avoid security probes
- Distribute scan traffic sensibly
- Fingerprint/scan incrementally
- Test and scan over time

IoT: everywhere, anywhere, and right here

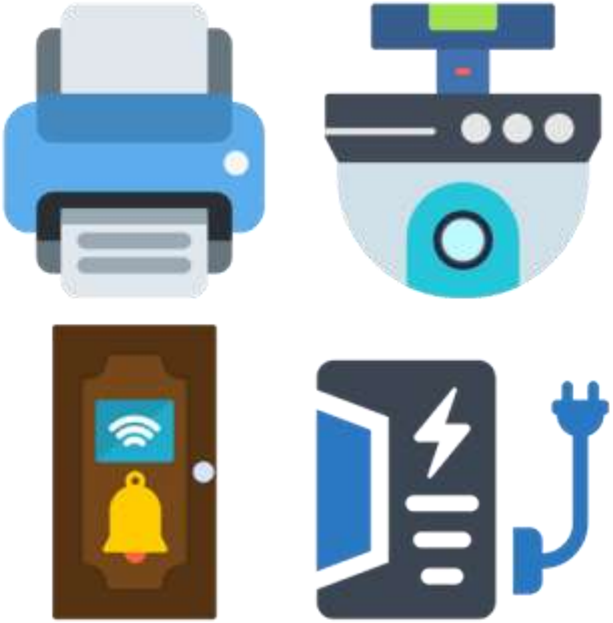
Fingerprinting IoT sucks



Fingerprinting IoT sucks



Fingerprinting IoT sucks



IoT may be disrupted too

Five Principles – They work for IoT too

- Send standard packets and expected payloads
- Avoid security probes
- Distribute scan traffic sensibly
- Fingerprint/scan incrementally
- Test and scan over time

Questions?

Parting thought

Don't get into a stranger's car.

Don't take your hands off the wheel.

Only governments can issue currency.

Work in an office so you make a good salary.

Don’t actively scan OT networks.

Connect with me

runZero

huxley@runzero.com

runZero

Thank you.