Using Offensive Operations to Defend Industrial Operations

Bassem Hemida | bhemida.com

bhemida.com

Technical | Strategy Senior Manager

Bassem Hemida

Cyber Security Professional with strategic management experience for over a decade with corporates and multinational organizations throughout Europe and the Middle East.

Awarded Penetration Tester of the Year 2016 from EC-Council Foundation InfoSec Tech & Exec. Winner of SANS Core Netwars, CyberDefense Netwars, DFIR Netwars and GRID Netwars

Download CV | Contact

What I Do

Red Teaming and Cybersecurity Crisis Simulation

Build a Red Team program and leverage Red Team exercises and adversary emulations to obtain a holistic view of an organization's security posture to measure, train, and improve people, processes, and technology for the organization. Also, perform multiple penetration tests, and targeting network-level, client-side-level, and web application-level attack vectors.

ICS / SCADA Security

Design and audit ICS/SCADA network security architecture and align it with the internationally recognized security standard like ISA99 / IEC 62443 and NERC CIP. Moreover, perform in risk assessments of ICS related technologies and day-to-day cyber-related operations. Also, Perform ICS / SCADA security assessments to identify potential vulnerability malicious adversary scenarios that might significantly impact client operations.

IT / OT Cyber Strategy

Balance the requirements to be secure, vigilant, and resilient with strategic objectives and the risk appetite of the organization. Develop an actionable roadmap and governance model to support security priorities in an era where cyber is everywhere.

Incident Response

Manage security incidents by understanding common attack techniques, vectors, and tools as well as defending against and/or responding to such attacks when they occur. Concentrating on methods used to detect, respond, and resolve computer security incidents.

Certifications

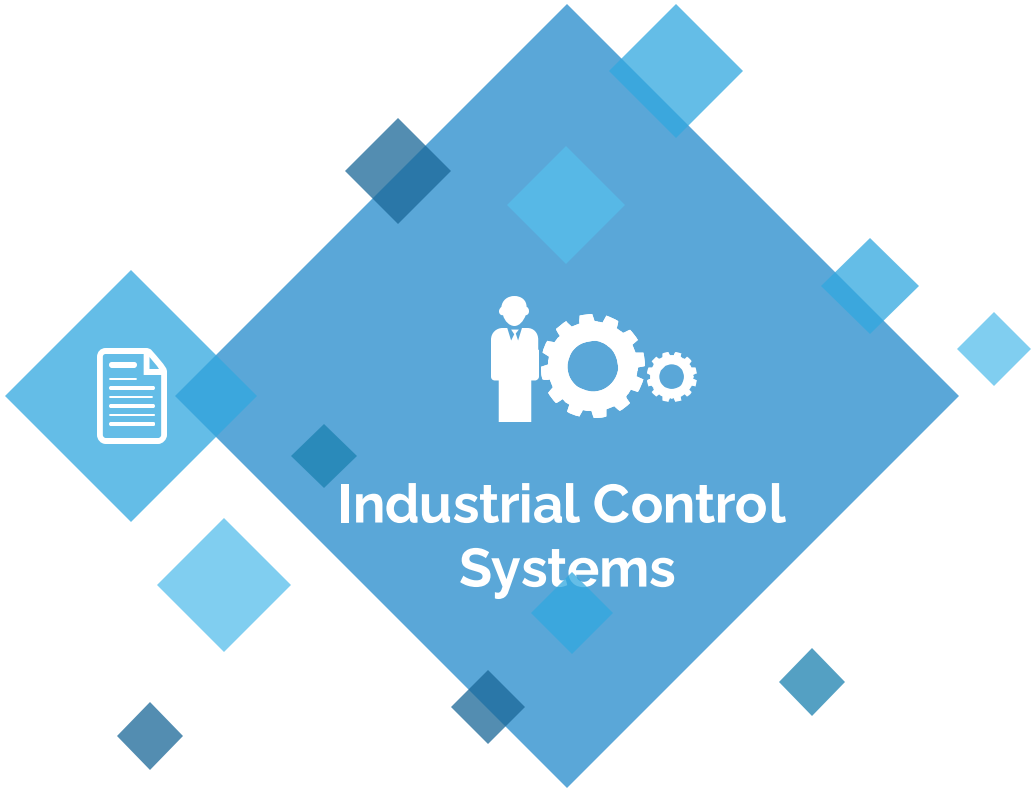
GXPN | GCIH | GCIA | GRID | OFFENSIVE OSCE | GICSP

Agenda

- What is Industrial Control Systems
- Why Industrial Operations
- Understanding the Attack Surface
- Understanding the Risk
- Offensive Operations
- ICS Most Common Vulnerabilities
- Demonstrate the Risk
- How to Defend?

We will explore how to demonstrate the threats in a vulnerable operational technology environment with minimal but effective interaction to understand the risk and introduce effective threat detection.

What is Industrial Control Systems



According to NIST

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

https://csrc.nist.gov/glossary/term/industrial_control_system

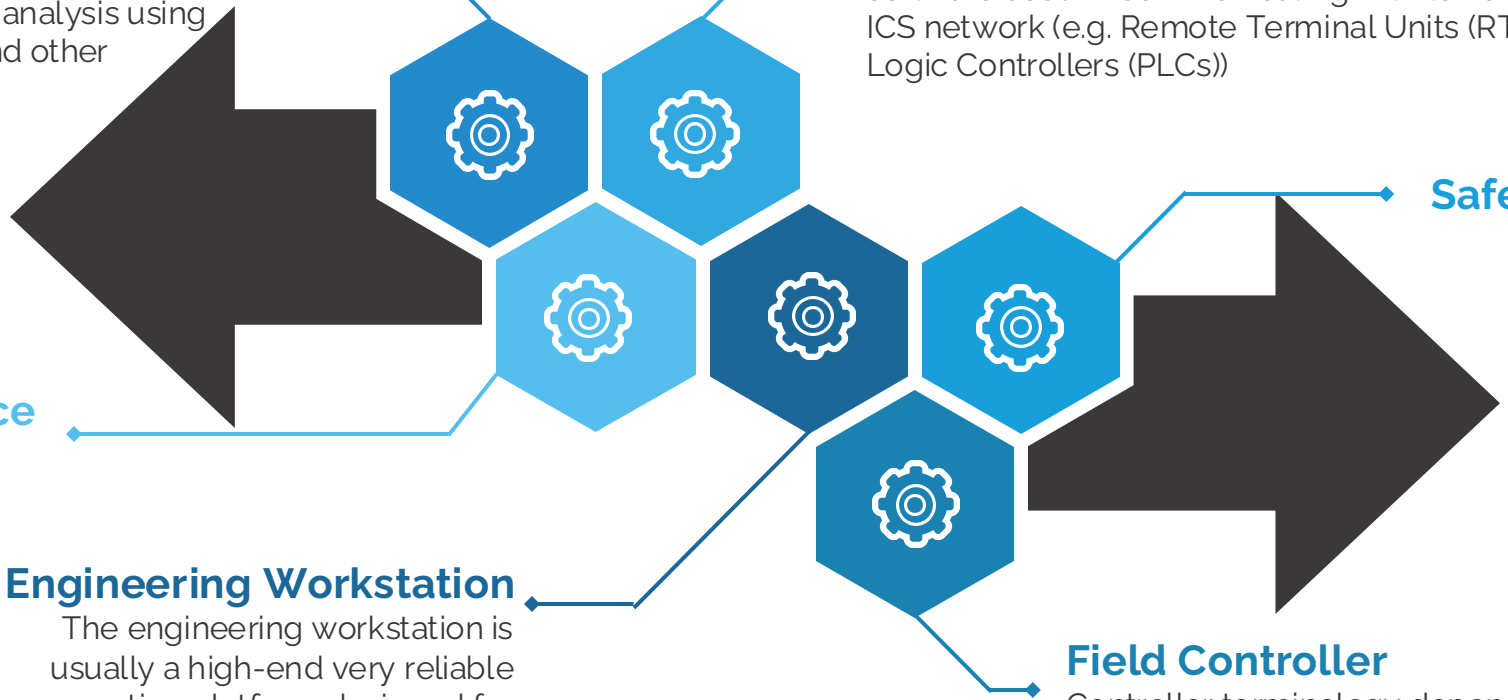
Assets in ICS Network

Data Historian

A centralized database located on a computer installed in the control system DMZ supporting external corporate user data access for archival and analysis using statistical process control and other techniques.

Control Server

A device which acts as both a server and controller, that hosts the control software used in communicating with lower-level control devices in an ICS network (e.g. Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs))

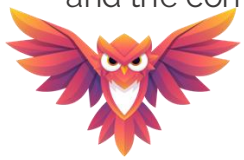


Safety Instrumented System

A safety instrumented system (SIS) takes automated action to keep a plant in a safe state, or to put it into a safe state, when abnormal conditions are present. The SIS may implement a single function or multiple functions to protect against various process hazards in your plant.

Human-Machine Interface

the Human-Machine Interface (HMI) refers to the graphical, textual and auditory information the program presents to the user (operator) using computer monitors and audio subsystems, and the control sequences



Engineering Workstation

The engineering workstation is usually a high-end very reliable computing platform designed for configuration, maintenance and diagnostics of the control system applications and other control system equipment

Field Controller

Controller terminology depends on the type of system they are associated with. They provide typical processing capabilities. Controllers, sometimes referred to as Remote Terminal Units (RTU) and Programmable Logic Controllers (PLC), are computerized control units that are typically rack or panel mounted with modular processing and interface cards.

Why Industrial Operations

A HISTORY OF STATE-SPONSORED ACTIVITY AGAINST OPERATIONAL TECHNOLOGY

2010 — IRANIAN NUCLEAR FACILITIES
Stuxnet first to target OT in Iranian nuclear enrichment facilities.

2012 — SAUDI ARAMCO & RASGAS
State-sponsored Iranian actors deploy Shamoon wiper malware to IT networks; OT unaffected.

2013 — BOWMAN DAM
State-sponsored Iranian actors infiltrate the control system and gain access to flood gates.

2014 — HAVEX CAMPAIGN
Russian-sponsored threat actor launches a global cyber- espionage operation against companies with OT assets.

2014 — GERMAN STEEL MILL
Unattributed state actors disrupt the control system, preventing a blast furnace from shutting down.

2015 — KYIV'S ELECTRICITY GRID (1 OF 2)
Russian Blackenergy malware used in unprecedented attack on CI: a portion of the city's grid loses power.

2016 — KYIV'S ELECTRICITY GRID (2 OF 2)
Russian state actors use CrashOverride malware to disrupt power supply.

2017 — ISTANBUL ELECTRICITY GRID
Energy Minster claims a severe state-sponsored cyberattack targeted the city's power grid.

2017 — UK ENERGY COMPANIES
State-sponsored actors penetrate the ICS of multiple UK energy companies.

2017 — OIL & GAS FACILITY
Russian-sponsored Triton OT malware triggers plant shutdown.

2018 — WESTERN CI SUPPLY CHAIN
Russian-sponsored Dragonfly 2.0 infiltrates the supply chain of CI OT asset owners.

2020 — ISRAEL AND IRAN TRADE CI ATTACKS
Iranian-sponsored threat actor targets two Israeli water pump stations. Israel disrupts operations at an Iranian port.

https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology

Understanding the Attack Surface

Business Context

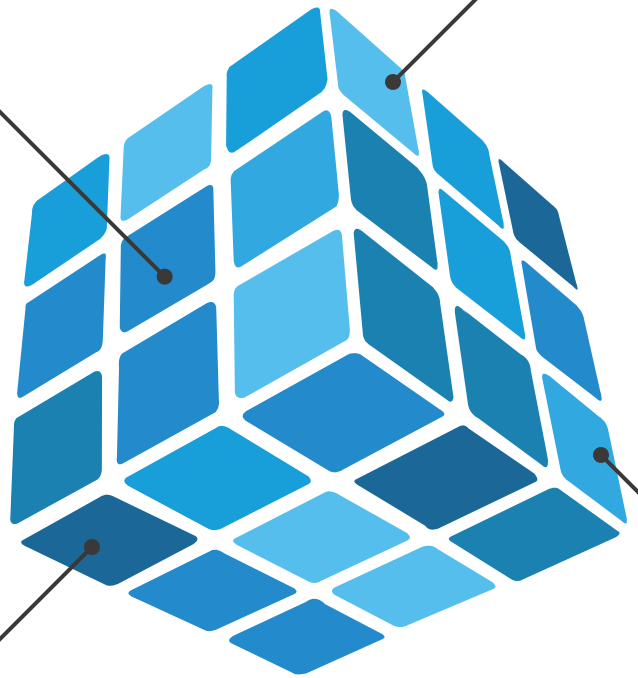
What are the business operation crown jewels?

- Mission critical services
- Mission critical information

Adversary Profiling

Who might attack your business?

- Cyber criminals
- Hactivists (agenda driven)
- Nation states
- Insiders/partners
- Competitors
- Skilled individual hackers



Adversary TTPs

What tactics and techniques might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise/supply chain
- Stolen credentials

Motivation

What are they after?

- Theft of PII, IP/strategic plans
- Financial fraud
- Reputation damage
- Business disruption
- Destruction of critical infrastructure

Understanding the Risk

Risk = Threat x Vulnerability

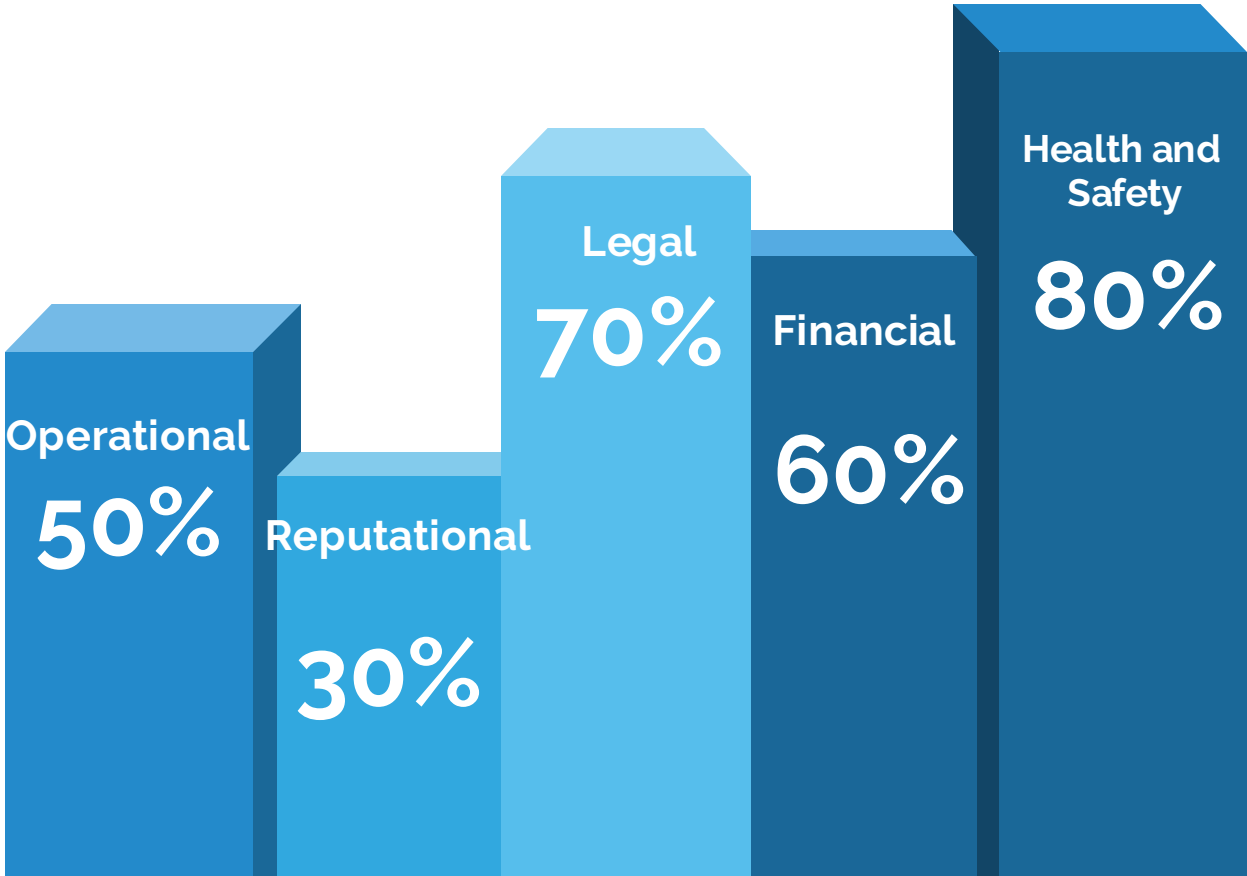
Risk is the exposure expressed by the gravity of the situation (impact).
Kye focus Safety, Availability, Integrity and Confidentiality.
Impact on HSE, Operational, Financial, Legal, and Reputational.

Threat

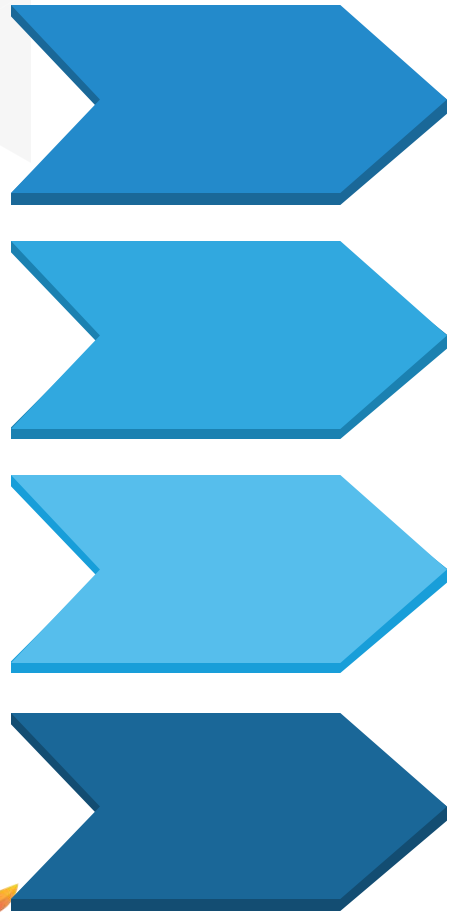
Using offensive operations to express the likelihood and demonstrate the possible danger

Vulnerability

Determine required defenses by identifying the weaknesses that can be used by adversary



Offensive Operations



Penetration Testing

Identify security vulnerabilities that could let an attacker either penetrate the network or computer system or steal data

Red Teaming

Using Adversary tactics, techniques and procedures to test detection and response capabilities

Purple Teaming

Cross-functional team consisting of Red and Blue Teamers with the objective of enhancing the identification, detection and response capabilities

Vulnerability Assessment

This process uses technical assessment tools to determine how threat actors may target and attack the organization and control network. It will produce technical listings of security weaknesses and related technical remediation steps.

ICS Most Common Vulnerabilities

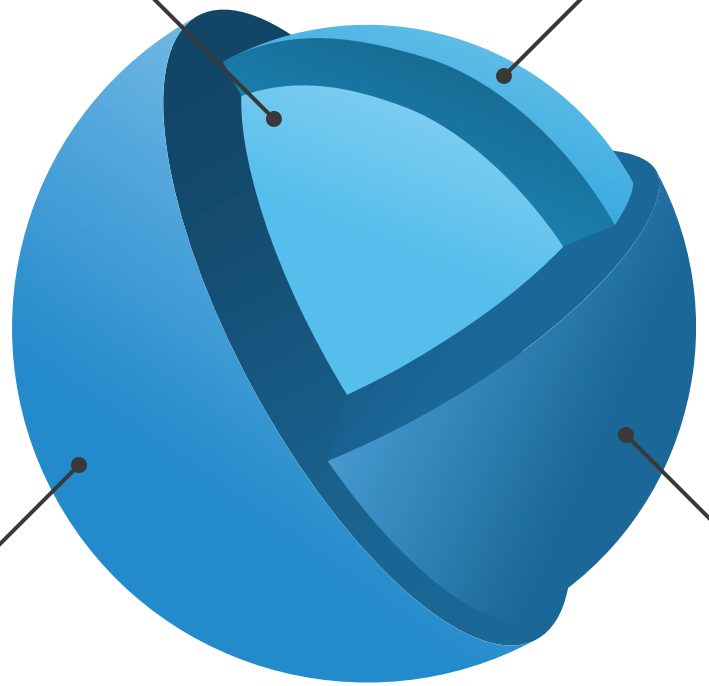
Weak /Default Passwords

Common passwords for

- OS administrator account
- Network administrator
- Vendor Application user

Absence of Patch Management

- Critical and High vulnerabilities in OS, NW or application not patched due to compatibility or business operating model.



Inadequate Architecture

- Same Domain or child domain
- Flat network 10.0.0.0/8
- Dual-homed network devices

Insufficient Security Controls

- Firewall rules ANY <-> ANY
- Endpoint Security missing update definition

AutoSave OFF — scadapass

Home Insert Draw Page Layout Formulas Data Review View Acrobat Table Tell me — Share Comments

Possible Data Loss Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. Save As...

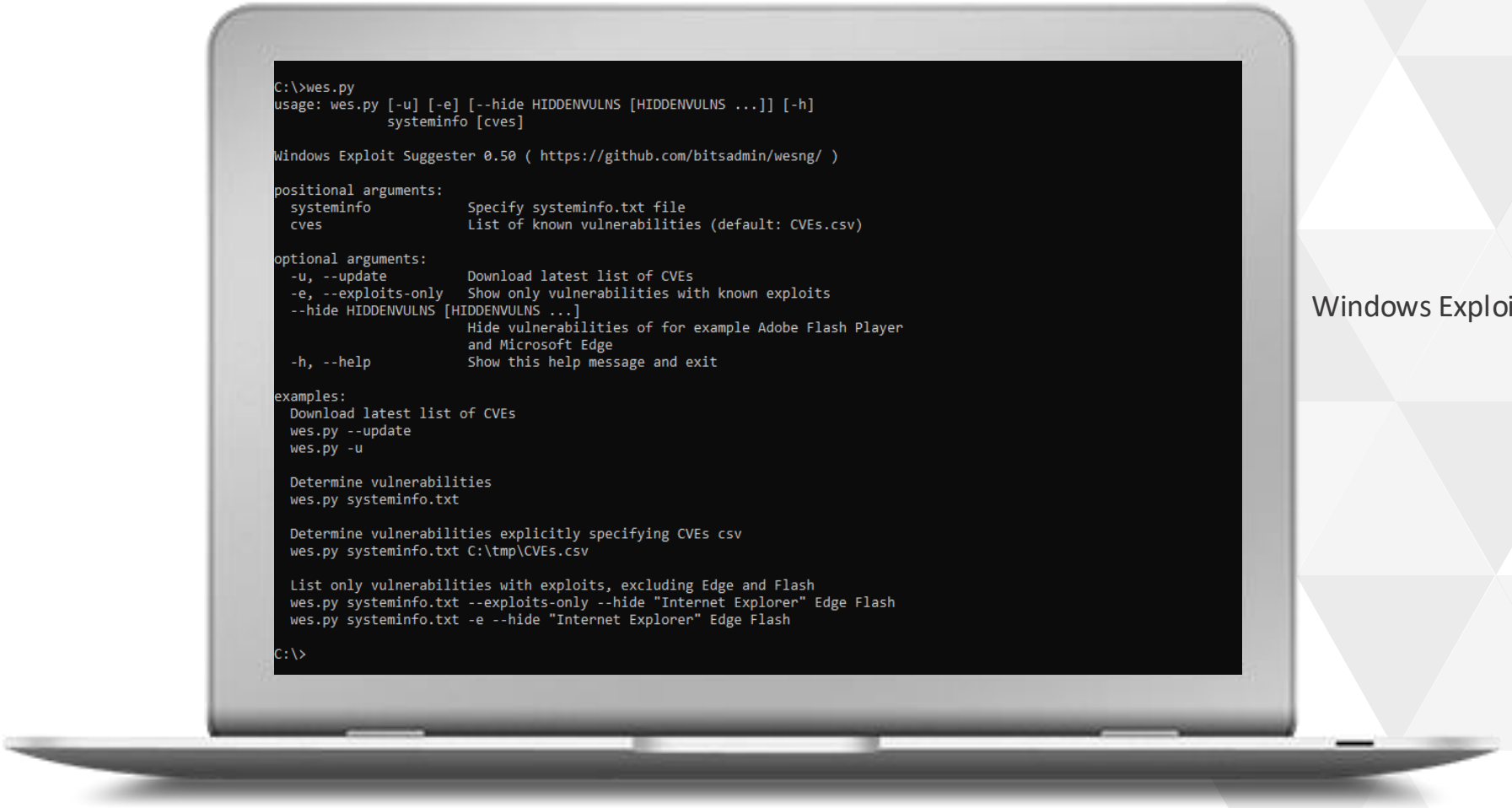
C24 — root:root

	A	B	C	D	E	F	G
1	Vendor	Device	Default password	Port	Device type	Protocol	Source
2	ABB	AC 800M	service:ABB800xA		Controller		https://library.e.abb.com/public/f355a67551218ae7c1257dc0003298c5/3BDS021515-600_-_en_AC_800M_6.0_PROFI
3	ABB	SREA-01	admin:admin	80/tcp	Ethernet Adapter Module	http	https://www.inverterdrive.com/file/ABB-SREA-01-Manual
4	Adcon Telemetry	Telemetry Gateway A840 and Wir	root:840sw	terminal program	Base Station		http://www.adcon.com/index.php?option=com_docman&task=doc_download&gid=41&Itemid=239&lang=de
5	Adcon Telemetry	addVANTAGE Pro 6.1, 6.5	root:root	8080/tcp	HMI	HTTP	http://adcon.com/index.php?option=com_docman&task=doc_download&gid=31&Itemid=239&lang=en, http://scient.s
6	Advantech	SNMP-1000, MIC-3924	advantech:admin	serial port	system management module, intelligent cha		http://support.elmark.com.pl/advantech/pdf/SNMP-1000man.pdf, https://ecauk.com/files/2011/08/Advantech-MIC-3
7	Advantech	Advantech WebAccess browser-ba	admin:blank	80/tcp	browser-based HMI and SC	HTTP	http://advantech.vo.llnwd.net/o35/www/webaccess/driver_manual/Advantech-WebAccess-Quick-Start-Guide.pdf
8	Advantech	EKI-7659C, EKI-7657C	admin:admin	80/tcp	industrial switch	HTTP	http://www.rts.ua/catalog/advantech/pdf/EKI-7659C_2_201316.pdf
9	Advantech	ADAM-6200 Series	root:00000000	80/tcp	Intelligent Ethernet I/O Mc	HTTP	http://www.bb-elec.com/Products/Manuals/ADAM-6200m-pdf.pdf
10	Advantech	ADAM-6050W	0		I/O module		http://datasheet.octopart.com/ADAM-6050W-AE-Advantech-datasheet-32780543.pdf
11	Advantech	ADAM-3600-A1F	Root:00000000, Admin:000000	80/tcp	Remote I/O Module	HTTP	https://www.proxis.ua/files/documents/UM-ADAM-3600-A1F-Ed1-EN.pdf
12	Alcatel-Lucent	OmniSwitch 6250	admin:switch	80/tcp, 23/tcp	switch	HTTP, Telnet	https://dariusfreamon.wordpress.com/tag/defaults/
13	Allied Telesis	IE200 Series: AT-IE200-6GT, AT-IE	manager:friend	terminal or termir	Industrial Ethernet Switches		http://www.alliedtelesis.com/userfiles/file/IE200_InstallGuide_RevC.pdf
14	Alstom	KVGC202/EN/M/E11, MiCOM P14	AAAA		Relays		https://www.gegridsolutions.com/alstomenergy/grid/Global/Grid/Resources/Documents/Automation/Technical%20
15	Argus	Argus Messenger	ArgusAdmin:masterkey		Messenger		https://dariusfreamon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/
16	Argus	Argus Address Manager	argus:argus		Address Manager Software		https://dariusfreamon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/
17	Astute Medical	ASTUTE140 Meter	1234:1234		analyzer		https://dariusfreamon.wordpress.com/2015/07/11/astute-medical-astute140-meter-default-user-credentials/
18	B&B ELECTRONICS	CR10 v2	root:root	80/tcp	Industrial router	http	http://tekniska.pl/downloadfile/1400014902-1208342584-pdf
19	B&B ELECTRONICS	Conel 4.0.1	root:root	80/tcp	Industrial router	http	http://conel.ru/shared/files/201502/9_411.pdf
20	B&B ELECTRONICS	SPECTRE Router	root:root	80/tcp	Router	http	b&b electronics SPECTRE Router.pdf
21	B&B ELECTRONICS	ER75i/ER 75i DUO/ER 75i SL/ER7!	root:root	80/tcp	Industrial router	http	http://ec-mobile.ru/user_files/File/Conel/ER75i_Manual_RUS.pdf
22	B&B ELECTRONICS	LR77 v2 Libratum/LR77 v2	root:root	80/tcp	Industrial router	http	http://www.induowireless.com/wp-content/uploads/2014/12/lr77-v2-libratum-manual.pdf, http://data.kommago.nl/
23	B&B ELECTRONICS	UR5i v2	root:root	80/tcp	Industrial router	http	http://www.cd.lucom.de/vpn-industrie-router/dokumentation/handbuch/ur5iv2-guide.pdf
24	B&B ELECTRONICS	UCR11-v2/UCR11 v2 SL	root:root	80/tcp	Industrial router	http	http://www.induowireless.com/wp-content/uploads/2014/03/ucr11-3g-router-hspa-cdma.pdf
25	B&B ELECTRONICS	XR5i v2E/XR5i v2/XR5i/XR5i SL	root:root	80/tcp	Industrial router	http	http://www.cd.lucom.de/vpn-industrie-router/dokumentation/handbuch/xr5iv2e-guide.pdf
26	B&B ELECTRONICS	ES1A	root:dbps	80/tcp	Converter	HTTP	http://www.bb-elec.com/Products/Manuals/pn-6909-rev003_ES1A-5012m.pdf
27	B&B ELECTRONICS	Vlinx VESR4x4	<blank>		SERIAL SERVER		http://www.bb-elec.com/Products/Manuals/VESP211-5012m.pdf
28	B&B ELECTRONICS	Vlinx MESR9xx Modbus Gateway	<blank>		Modbus Gateway		https://www.manualshelf.com/manual/b-b-electronics/vlinx-mesr9xx/modbus-gateway-brochure/page-31.html
29	Barco	MediCal QAWeb Agent	Advanced:advanced		client application		https://dariusfreamon.wordpress.com/2015/07/10/barco-medical-qaweb-agent-default-password/
30	Beckhoff Automation GmbH	CX5020	webguest:1	23/tcp	PLC	Telnet	https://www.researchgate.net/publication/272420507_ICSSCADA_Security_Analysis_of_a_Beckhoff_CX5020_PLC
31	Beckhoff Automation GmbH	TwinCAT	Administrator:1		Software for the Windows control and autor		https://infosys.beckhoff.com/english.php?content=../content/1033/sw_os/html/cx1000_os_xpe_geninfo.htm&id=
32	Beck IPC	¬†IPC@CHIP	PPPSERVER:, ppps:ppps		PLC	pap/chap	https://www.beck-ipc.com/files/api/scxxx/config.htm
33	BinTec Elmeg	BinTec X1200 II	admin:bintec,		Router		http://www.router-defaults.com/Router/BinTec--x1200-ip-password-username
34	BinTec Elmeg	any routers	(##unknown - means not known or any char):, ##		Router		http://www.router-defaults.com/Router/BinTec--x1200-ip-password-username
35	BinTec Elmeg	BinTec R230aw	admin:funkwerk		Router		http://www.tomshw.it/forum/banda-larga/154194-router-bintec.html
36	BinTec Elmeg	Bintec W2002T-n	admin:funkwerk, admin:admin		WLAN Access Point for applications in rolling		http://www.bintec-elmeg.com/download.php?src=portal/downloadcenter/dateien/w2002tn/documentation/Notes-d
37	BK Ultrasound	bk3000	administrator:superuser		Ultrasound System		https://dariusfreamon.wordpress.com/2015/07/12/bk-medical-aps-bk3000-ultrasound-system-default-credentials/
38	Carlo Gavazzi	PowerSoft	admin:admin, user:user		modular software		https://www.gavazzionline.com/pdf/PowerSoftIMENG.pdf
39	CAREL	easy/easy compact/easy split, PJ3	22 (access to the parameters)		electronic microprocessor controllers, plug-i		http://www.tempatron.co.uk/resources/product/manual_79.pdf, http://www.tempatron.co.uk/resources/product/ma
40	CAREL	pCOWeb	root:froot, carel:fcarel, guest:f	21/tcp, 80/tcp	communication card	FTP, HTTP	http://www.carel.com/documents/10191/0/%2B030220471/9619472f-f1c0-4ec9-a151-120aaa5e479a?version=1.0, h
41	CAREL	ir33 platform: ir33, ir33 power, ir3	22 (access to the parameters), 66 (download acti		integrated electronic microprocessor control		http://www.tempatron.co.uk/resources/product/manual_80.pdf
42	CAREL	Universal Infrared Series	22 (enter and modify parameters C0, C13, 15 and		pressure, humidity and temperature controll		http://www.tempatron.co.uk/resources/product/manual_76.pdf
43	CAREL	IR33-DN33 Universale series	77 (Setting type c, d, F parameters)		pressure, humidity and temperature controll		http://www.temperature-house.com/cms-files/Carel_IR33_Manual_for_Warming_Oven.pdf
44	CAREL	pRack PR100	user password: 0000, service password: 1234, m		compressor rack controller		http://www.carel-cz.cz/dokumentace/chlazeni/pRack/pRack_Quick%20guide.pdf
45	CAREL	humiSteam x-plus	77		humidifiers		http://www.airsystems.ro/assets/manual-humisteam-xplus--0300040en.pdf
46	CAREL	PlantVisorPRO Locale	admin:admin	443/tcp	Plant supervision	HTTPS	http://www.alltyperefrigeration.com.au/logos/monitoring/quick_guide.pdf
47	CAREL	PlantWatchPRO	PVRemote:PD35010 (from a re	80/tcp	supervisor for small-mediu	HTTP	http://www.carel.co.th/documents/10191/0/%2B040000021/4b549ef7-3d35-4454-bc04-91ba26aa945d?version=1.0
48	CAREL	Œ²C2SE	Direct level: <blank>, user level: 22, super user le		electronic controller		http://planetaklimata.com.ua/instr/Carel/Carel_mC2SE_User_Manual_Eng.pdf

scadapass +

Ready Accessibility: Unavailable 100%

https://github.com/scadastrangelove/SCADAPASS/blob/master/scadapass.csv



Project

Windows Exploit Suggester - Next Generation (WES-NG)

Link

https://github.com/bitsadmin/wesng

Brief

WES-NG is a tool based on the output of Windows' systeminfo utility which provides the list of vulnerabilities the OS is vulnerable to, including any exploits for these vulnerabilities. Every Windows OS between Windows XP and Windows 11, including their Windows Server counterparts, is supported.

Project

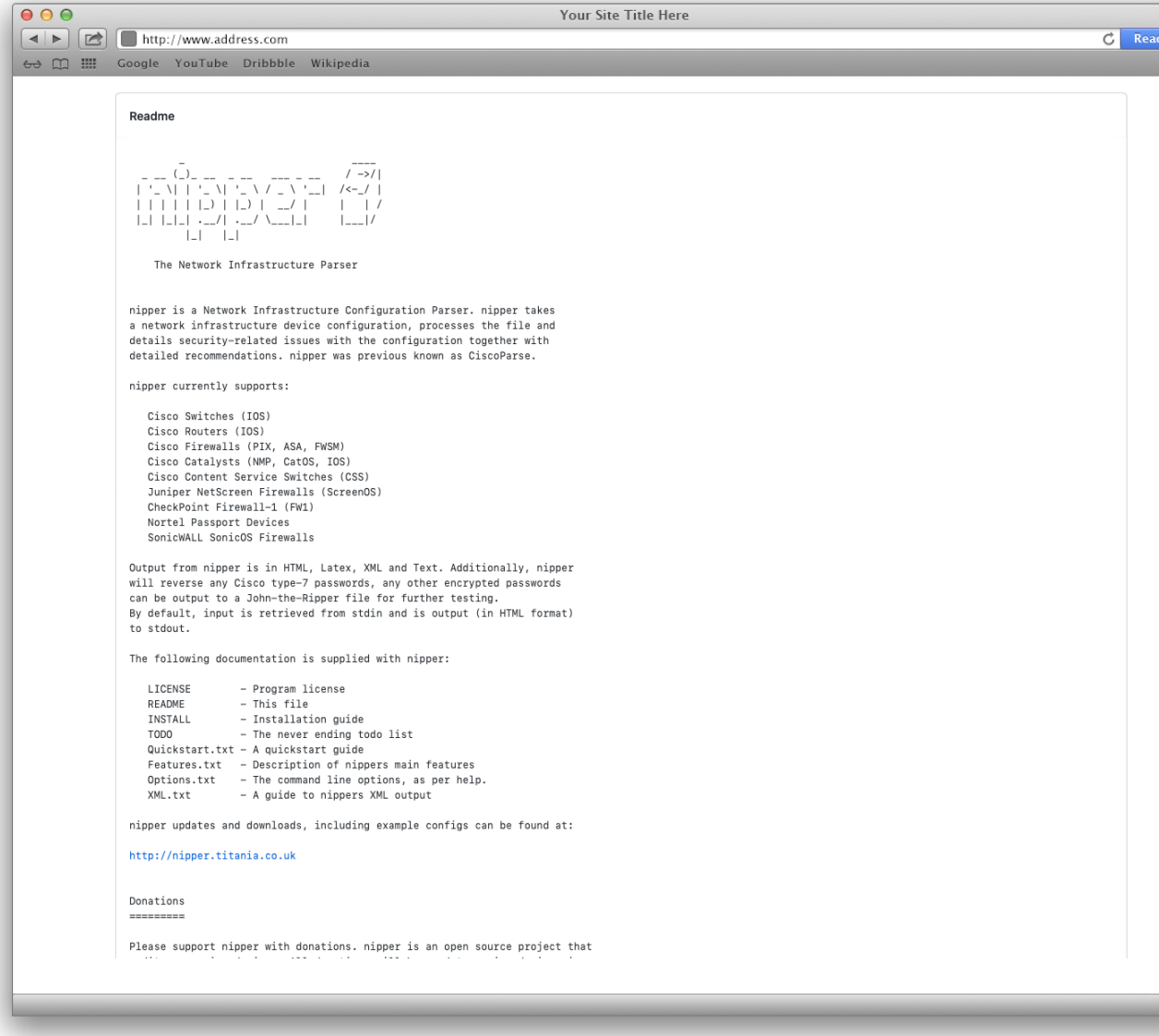
Nipper-ng

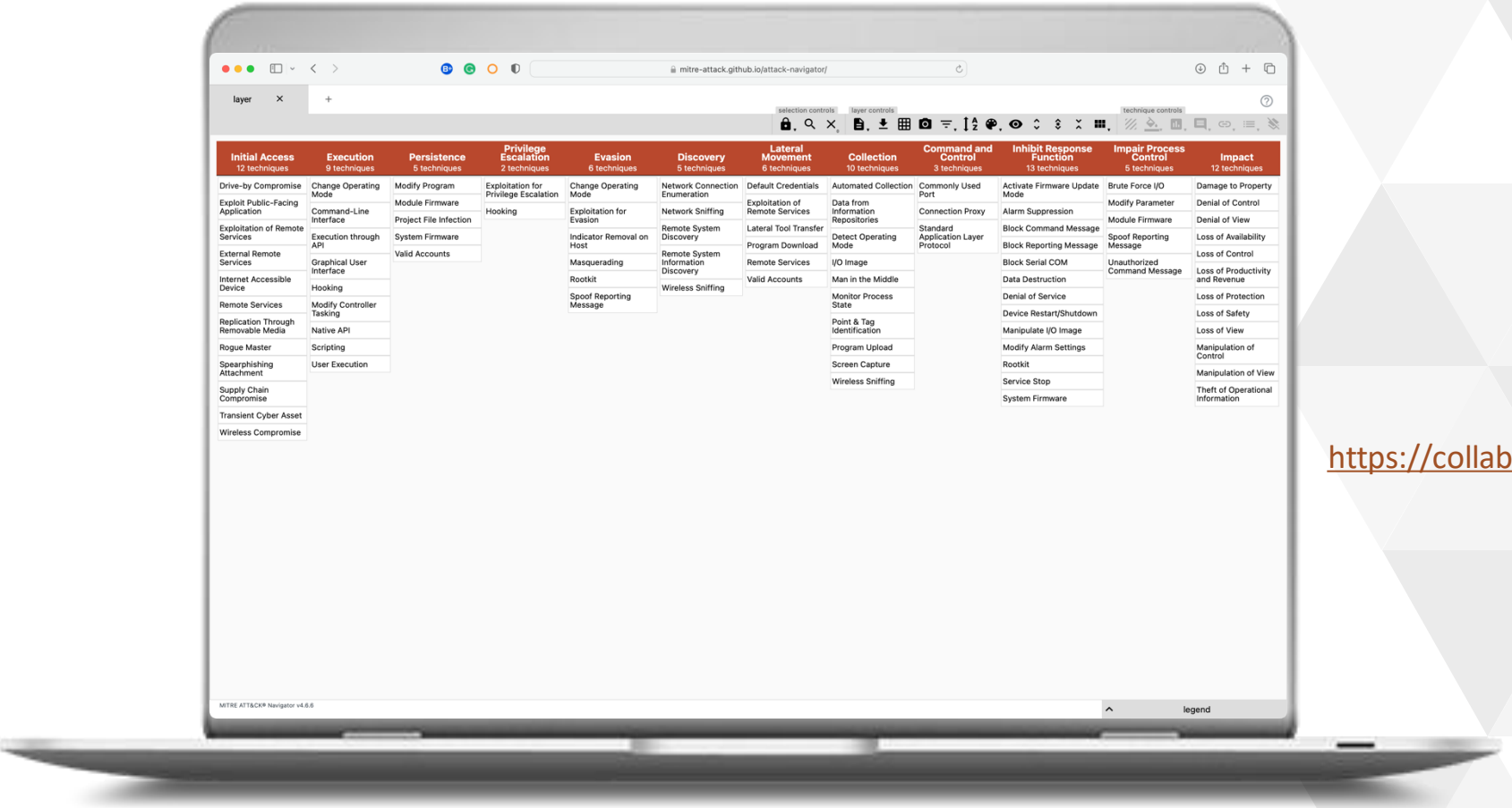
Link

https://github.com/arpitn30/nipper-ng

Brief

Nipper-ng is the next generation of nippper, and will always remain free and open source. This software will be used to make observations about the security configurations of many different device types such as routers, firewalls, and switches of a network infrastructure.





Project

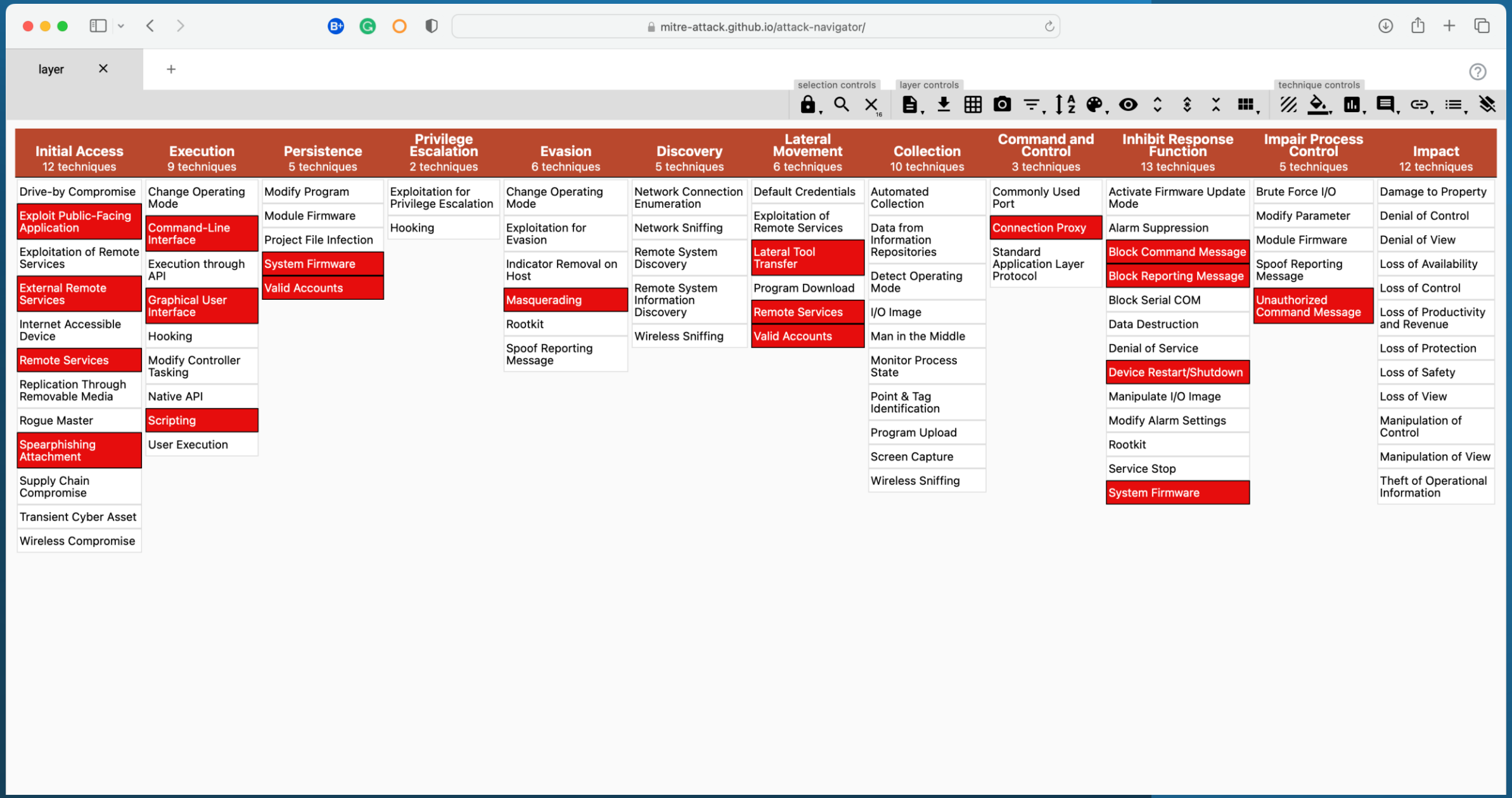
ATT&CK® for Industrial Control Systems

Link

https://collaborate.mitre.org/attackics/index.php/Main_Page

Brief

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.


mitre-attack.github.io/attack-navigator/
layer
selection controls
layer controls
technique controls
Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise
Execution
9 techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
5 techniques
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
6 techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
6 techniques
Default Credentials
Exploitation of Remote Services
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
10 techniques
Automated Collection
Data from Information Repositories
Detect Operating Mode
I/O Image
Man in the Middle
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
13 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Impact
12 techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information

Demonstrate the Risk

Ransomware

An adversary can gain initial access through compromising external remote service and exploit multiple critical system vulnerabilities to conduct lateral movement and privilege escalation till they reach the critical mission systems and deploy ransom

Be Creative

Use your offensive experience to explore realistic possible ways to leverage discovered weaknesses to create business impact.

Cyber Espionage

An adversary can gain access by compromising a software provider and gain highly privileged access to the mission critical information. The adversary can use this access to maintain a long-time network presence. Also, under certain circumstances, the adversary can use the access for sabotage.

How to Manage the Risk?

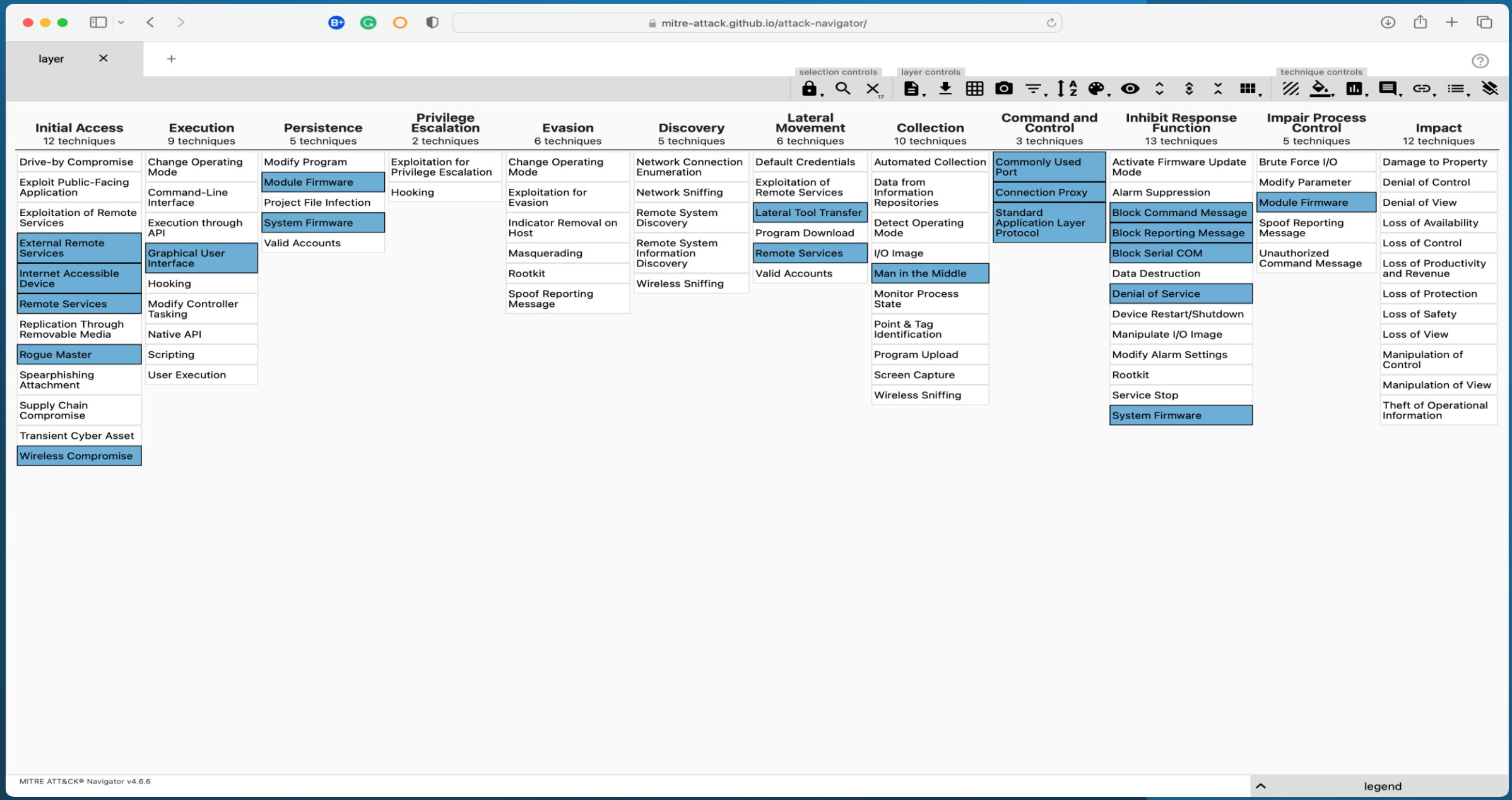
Start with Network Architecture

Network Segmentation and Segregation

Boundary Protection

Firewalls

Logically Separated Control Network


mitre-attack.github.io/attack-navigator/
layer
selection controls
layer controls
technique controls
Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise
Execution
9 techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
5 techniques
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
6 techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
6 techniques
Default Credentials
Exploitation of Remote Services
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
10 techniques
Automated Collection
Data from Information Repositories
Detect Operating Mode
I/O Image
Man in the Middle
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
13 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Impact
12 techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information
MITRE ATT&CK® Navigator v4.6.6
legend

Contact Me

Address
Netherlands, Amsterdam

E-mail
ping@cybersecowl.com

Website
https://bhemida.com

Thank You