linics-van-gogh

A to Z of LINICS

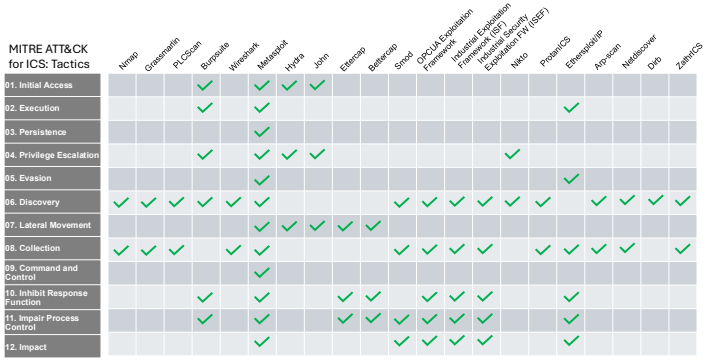
FOR LINICS 1.5

Hacktonics Ltd

A

ATT&CK

All the tools in LINICS are mapped to MITRE ATT&CK for ICS.



ARP Scan

Can be used to discover and fingerprint hosts on an OT network.

B

BesterICS

A tool we wrote specifically for LINICS, providing OT pentesters with a one-stop shop for managing and reporting on pentests. Like the Psi Cop in Babylon 5, BesterICS can help to sense and track threats.

BurpSuite Community Edition

Handy to identify vulnerabilities on web servers embedded in OT devices and test for exploitability.

Bettercap

Can be used for reconnaissance and attacks against WiFi, CAN-bus and IPv4/IPv6 networks as well as Bluetooth Low Energy devices and other wireless connected devices.

C

CAF, the Cyber Assessment Framework by NCSC

The tools in LINICS can be used to develop an understanding of an organisation's OT security with reference to the CAF.

D

DIRB

Can be used to look for existing or hidden web objects on hosts within an OT network.

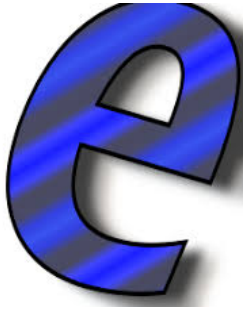
E

Ethersploit-IP

Can be used to exploit vulnerabilities in the EtherNet/IP protocol.

Ettercap

A person-in-the-middle attack framework, which is useful to probe vulnerabilities in industrial protocols as many of them are susceptible.



F

Fudge

What we say when we find bugs and Fudge is also what we buy with the money we put in the jar after shouting Fudge.

F

Grassmarlin

A passive asset discovery tool for OT networks to understand network topologies and extract information about OT devices.

H

Hydra and Hydra Graphical

Useful for online password cracking attacks against a number of protocols, including those used in OT.

I

ISF and ISEF

Two industrial security exploitation frameworks that offer a Metasploit like interface, with a number of modules for scanning and interacting with OT devices.

J

John the Ripper

John is a useful tool for password security audits.

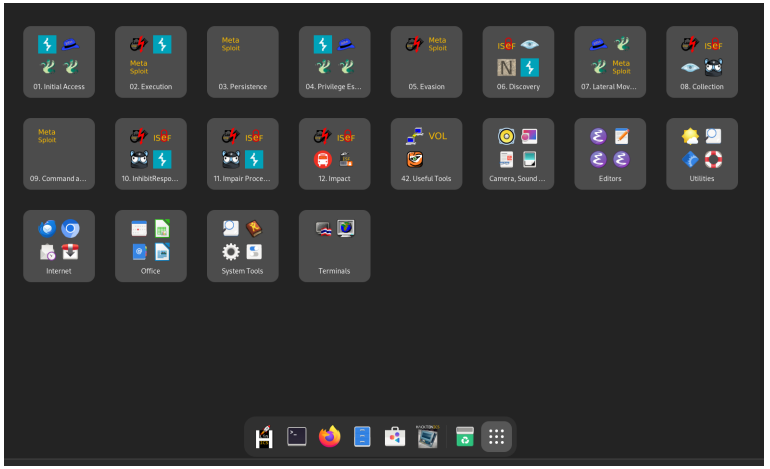
Jar Jar USBinks

The keeper of all the LINICS Live USBs. Get one of these from Jar Jar USBinks in person by attending one of our hands-on training workshops.

K

Kill Chain

One can follow the various steps of the MITRE ATT&CK Kill Chain using the tool mapping in LINICS.



L

linics-van-gogh

Our architect's alter ego . . . as LINICS is a thing of beauty!

M

Metasploit

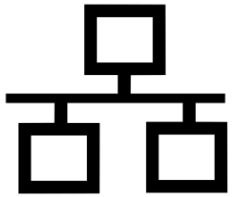
The framework has a number of modules for exploiting hosts and devices, including some OT specific ones. But we have added more OT specific modules too.

N

Nmap

One's got to have Nmap for mapping networks and fingerprinting hosts. But this is not any Nmap. This is Nmap in LINICS so we have souped it up with additional OT specific scripts.

Netdiscover



Can be used to identify accessible IP addresses using ARP requests.

Nikto

Handy for scanning webservers on OT devices, which are often used for remote connection, access and configuration.

O

OT

LINICS is packed with tools for OT security and we plan to add more.

OPC-UA Exploitation Framework

This includes tools for extraction of information and performing attacks against OPC-UA servers.

OVF (Open Virtualisation Format)

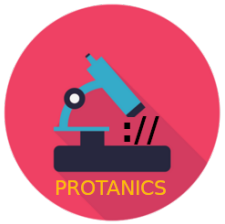
A pre-built LINICS VM can be downloaded in OVF and imported into a user's hypervisor of choice.

Operational Technology

P

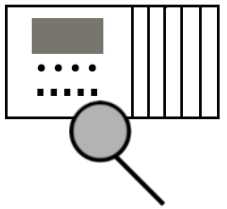
ProtanICS

A protocol analyser we wrote specifically for LINICS, which can be used to examine network captures.



PLCScan

A tool for scanning older Siemens S7 and Modbus devices.



Pink Fluffy Unicorn

Has a pride of place on the laptop where a lot of LINICS development work happens.

Q

qcow2

The VM format for KVM—a pre-built LINICS qcow2 image is available for download.

R

Ready

To get hands-on with LINICS? If so, download it from:
`https://linics.org`.

S

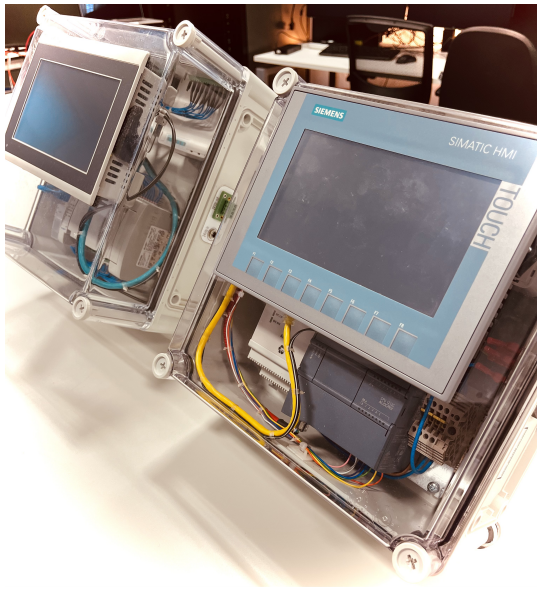
Smod

This tool includes a number of diagnostic and exploitation modules for the Modbus protocol.

T

Training Boxes

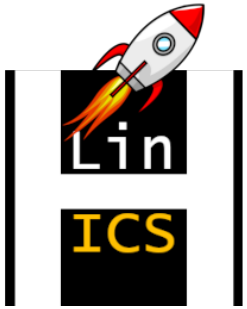
The Hacktonics training boxes are loved by everyone who attends our courses. They are nice, compact, support multiple vendors and, together with the tools in LINICS, give attendees a proper hands-on experience on OT security.



U

Users of LINICS

Join our Discord (`https://linics.org`) and tell us how you are using LINICS, share experience and give us feedback on any issues.

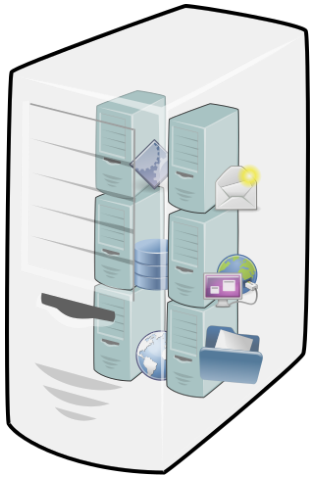


V

Volatility

A collection of tools for memory forensics, which can be used for OT devices too.

VOL



VirtualBox and VMWare

LINICS VMs are available to download for both VirtualBox and VMWare.

W

Watch this space

Well our website. We plan to update LINICS regularly so look out for news on the next release, with additional tools.

https://linics.org

X

Marks the spot. Because it does!

Y

You!

We want your contribution to LINICS. Know of an OT tool that you think should be in LINICS? Have written one? Want to write one? Drop us a note. We'd love to hear from you.

Z

ZathrICS

A tool we wrote specifically for LINICS, supporting an integrated approach for performing active scanning of OT networks. Like in Babylon 5, ZathrICS knows the secrets of the great ICS machine!