

01 WHAT IT IS

Safe methodologies for identifying vulnerabilities in fragile ICS environments without causing operational downtime or disruption.

WHY IT MATTERS

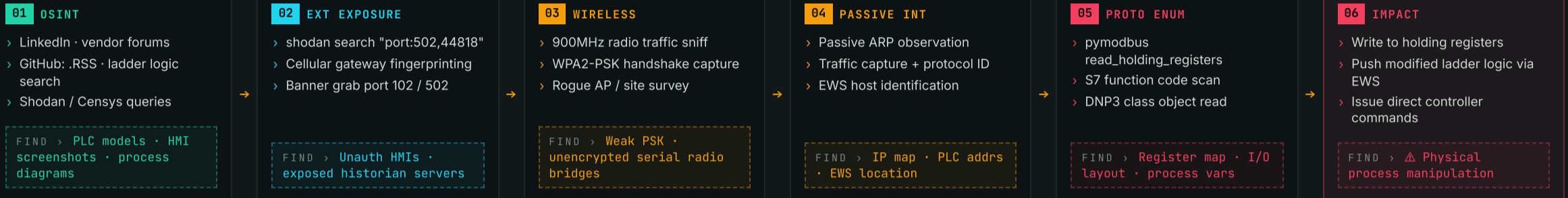
Traditional IT scanners (Nessus, Qualys) WILL knock PLCs offline — OT tolerates zero unexpected high-rate packets on the wire.

WHERE

Pre-engagement OSINT, wireless site surveys, and highly scoped, controlled internal network assessments.

§02 Recon Methodology & Protocol Map · 6-phase engagement · passive to active · ICS protocols that ship with zero auth

● **CROWN JEWEL** · The **Engineering Workstation (EWS)** is the ultimate prize — it holds the proprietary software needed to communicate with and reprogram every recon phases controller.

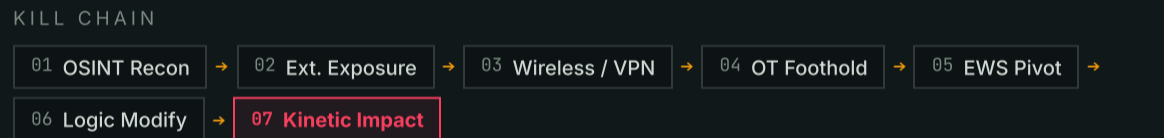


Modbus TCP L1-L3 Write any coil/register in one packet. Zero session, zero encryption required.	DNP3 L1-L2 SCADA ↔ RTU/IED. Supports unsolicited responses; replay attacks are trivial.	EtherNet/IP L1-L3 CIP over TCP for Allen-Bradley PLCs. Function code enum exposes CPU details.	S7 Comm L1-L3 Siemens S7-300/400. Rack/slot scanning silently maps all installed CPU modules.
--	--	---	--

■ OSINT · safe ■ External · passive ■ Wireless / Internal · low-impact ■ Active enum / Impact · auth required Passive phases always safe · active enum requires written authorization

§03 Attack Surface · where to look before touching anything

- Internet-Exposed** Cellular gateways and unauthenticated HMIs indexed on Shodan via misconfigured port forwarding rules.
- OSINT Leakage** Engineers posting HMI screenshots, specific PLC models, or network diagrams on LinkedIn and vendor forums.
- Wireless Bridges** 900MHz radios or WPA2-PSK Wi-Fi spanning remote substations to main facilities with weak shared keys.
- Dual-Homed EWS** Engineering workstations with both IT and OT NICs — the canonical lateral pivot point straight into OT.



§04 MITRE ATT&CK · ICS · techniques most-used in OT compromise

- T0817 Drive-by Compromise** Target engineers browsing the internet from dual-homed OT workstations via watering hole.
- T0843 Program Download** Reverse the engineering project file, modify ladder logic, push it back to the controller via EWS.
- T0806 Issue Command** Use pymodbus scripts to write values directly to holding registers, bypassing the HMI entirely.
- T0865 Spearphishing Attach.** Malicious vendor manual or fake software update targeting OT engineers with elevated system trust.

§05 Detection & Monitoring · signals · what logs actually matter in OT

- **EWS EDR Telemetry** Deploy EDR on Engineering Workstations and HMIs; catch LOLBins and unexpected process spawns early.
- **ARP / SYN Spike** Sudden ARP request storms or TCP SYN floods from within OT = lateral movement or active scanning.
- **Unauth Protocol Comms** Any device other than the designated EWS communicating on port 502, 102, or 44818 = immediate Sev-1.

§06 Mitigation & Hardening · what to actually deploy

- + **DPI Firewalls** OT-protocol-aware DPI — block Modbus "Write" function codes while permitting "Read" commands only.
- + **Physical Port Locks** Disable unused RJ45/USB on PLCs. "Run Mode" physical key prevents remote logic uploads entirely.
- + **Credential Rotation** Change ALL default creds on every OT device — they almost universally remain factory defaults.
- + **Network Segmentation** Strict Purdue Model zones. No direct IT→OT routing. Data Diodes for historian replication feeds.

§07 Red Team · offensive · what actually works

- 01** Default creds: OT devices ship with hardcoded factory credentials that operators almost never rotate.
- 02** GitHub OSINT: search "company + ladder logic" or ".RSS" to find leaked engineering project files.
- 03** pymodbus: write directly to holding registers from any OT-adjacent host, completely bypassing the HMI.
- 04** Dual-homed EWS: compromise the IT NIC via phish, then pivot across the NIC boundary into OT.

§08 Blue Team · defensive · what most teams miss

- 01** SIEM rule: Sev-1 alert the instant any device other than the designated EWS touches port 502, 102, or 44818.
- 02** OT-safe EDR (e.g. CrowdStrike) only on Level 3 + Level 2 Windows/Linux hosts — never directly on PLCs.
- 03** Alert on ARP storms or TCP SYN floods originating from inside the OT network segment.
- 04** Shodan monthly against your own IP space — see what attackers see before they do.

§09 Quick Commands · passive only on production OT · TCP connect · slow

```

> shodan search "port:502" → find globally exposed Modbus devices
> nmap -Pn -sT -p 502,102,44818 --max-rate 10 → TCP connect ONLY · no SYN · no -sC ever
> pymodbus read_holding_registers(0, 10) → passive read — safe on live OT
> msfconsole aux/scanner/scada/modbusclient → ICS-specific Metasploit module only
  
```

§10 Memory Hooks · commit these to muscle memory

Go Slow, TCP-Connect

Never SYN scan or run -sC scripts against live PLCs. TCP connect only, max-rate ≤ 10.

OSINT Is 80% of Work

Attackers map the physical process via manuals and social media before ever touching the network.

Connected = Vulnerable

OT protocols lack encryption. Packet injection is trivial once on the local OT segment.