#

CIP Penetration Testing

## Table of contents



---

## Revision History

| Revision No | Date | Change description | Author | Reviewed by |
|---|---|---|---|---|
| 001 | 2021-03-31 | Draft CIP penetration test investigation document | Shivanand | TBD |

---

## Objective

The primary objective of this document is to identify suitable penetration testing tool and document the process how this can be re-used by CIP end users for their specific use cases.

Currently this document captures generic use cases of CIP and in future it can be further enhanced to capture specific use cases of CIP based end products.

## Penetration testing

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in either virtually or for real and reporting back the findings.

The main objective of penetration testing is to identify security weaknesses.

### Purpose of penetration testing

The primary goal of a pen test is to identify weak spots in an organization's security posture, as well as measure the compliance of its security policy, test the staff's awareness of security issues and determine whether and how the organization would be subject to security disasters.

### Penetration testing DO'S & DONT'S

- Make sure you do everything as discussed and set out within the agreed scope.
- Make sure you do get authorization signed off to perform the penetration test.
- Do not ever perform a penetration test without prior approval.
- Do not perform testing outside of the agreed scope of the test.

**Benefits of performing a penetration testing**

- Identifying Network Security Flaws
- Understanding Risk Levels
- Mapping Out the Organization's Overall Security Posture
- Fixing Information Security

## CIP Penetration Testing

CIP is used in the programmable Logic controllers(PLC) at industrial control system(ICS). It is one of the most important components of ICS.

Industrial control systems are one of the most favorite targets of the hackers because of many points,

- Easy targets: Lack of security training = Easy social engineering
- No security measures
- Out-dated OS
- No security policy
- Default passwords
- Default configuration
- No patch management policy

In network, the primary aim is to identify exploitable vulnerabilities in networks, systems, hosts, and network devices (i.e., routers and switches) before hackers discover them and wreak damage.

Thorough network penetration testing:

- Reveals real-world opportunities for hackers to compromise systems and networks for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.
- Simulates an attack to understand the level of risk for your organization
- Helps address and fix identified network security flaws.

The idea is to view the systems through the eyes of both a hacker and experienced network security professional to discover where the security posture can improve.

**Use case to consider for penetration testing**

- CIP in programmable Logic controllers
- CIP in networking switch

**Suitable tools for penetration testing**

The penetration testing tools mentioned below are widely used in the industrial control systems(ICS) and network testing. This list will be updated based on the further investigation.

- NMAP
- Metasploit
- Shodan
- PLCSCAN
- Wireshark
- Nipper
- Nexpose

**How to capture the output of penetration testing**

```
yet to update
```

## Post Penetration Testing

```
yet to update
```

## Next Step

```
yet to update
```

## References

- https://resources.infosecinstitute.com/topic/pentesting-ics-systems/
- https://www.redteamsecure.com/penetration-testing/network-penetration-testing
- https://github.com/enaqx/awesome-pentest#industrial-control-and-scada-systems