FAQ

Have any questions?

Frequently asked questions related from the ICS Cybersecurity Virtual Training.

Session 1 - ICS Overview

Q 1. Does the exploit used in the vulnerability demonstration only pertain to machines running Windows XP?

Several exploits were used during the demonstration, and no they do not only pertain to Windows XP. Even if the exploits used did only pertain to Windows XP, there are other exploits that work for newer versions of Windows, including Windows 10.

Q 2. How do you evaluate the exposure of PLCs? Best Practices? Published Findings?

If your concern is exposure to the Internet, then use Shodan to search your IP range. If your concern is vulnerabilities or exploits, see Cybersecurity and Infrastructure Security Agency (CISA) ICS Advisory and Alerts: https://www.us-cert.gov/ncas

Q 3. Can someone explain or give a summary overview of what malware like Shamoon, BlackEnergy, Crashoverride, HAVEX, etc., do to disrupt a control system?

Each malware has different outcomes, targets, and results.

- The Shamoon attack literally erased the hard drive of each system it infected.
- Black Energy was a Trojan Horse used to conduct a DDoS (Distributed Denial of Service) attack, among others.
- Crashoverride is a platform specifically targeted to the electrical power grid.
- "Havex is a Remote Access Trojan (RAT) that communicates with a large network of compromised web sites used as Command and Control (C&C). The C&C servers deploy payloads that provide additional functionality for the intruder" -- us-cert.gov

Q 4. Can you provide feedback regarding if there is the same exposure on Linux as Windows? Is open-source software more secure or less secure than proprietary software?

Windows being more widely used has more recorded incidents, but all OS's have vulnerabilities. Open-source software tends to have more current input and updates, but are reliant on their developers and contributors to ensure valid cybersecurity coding. However, you need to apply the open-source patches. It does not matter what you use if you do not patch.

Q 5. How can attackers get a better understanding of a PLC they encounter during system profiling (i.e., figuring out what ports/fields control what)?

Understanding the data flows in/out. A netscan from an HMI can define these connections. Manufacturers have documentation to define ports and protocols.

Q 6. Would you say Python is a good language to learn for Ethical Hackers or Cybersecurity Engineers in general?

Sure. Understanding programming languages and techniques, compilers, and operating systems are all good foundational skills to help with those fields.

Q 7. Can MS Windows act as a real-time operating system, or are field devices likely to stick to proprietary Operating Systems/firmware for the foreseeable future?

Windows CE has been called a Soft RTOS, but generally it is not considered one, and Windows IoT is supposed to be an embedded OS. We do see more "mainstream" OS's being used. Keep in mind that Windows is also a proprietary OS.

Q 8. What types of measures could have prevented the infiltration of the system once the hacker got control of the corporate machine?

Measures such as a host-based firewall, Whitelisting, ACL on corporate machines, better firewall rules for ingress and egress (hacker should not be able to connect from DMZ and PCS networks to the internet), data traffic should be pushed from "Trust" to "Untrust" networks (PCS to DMZ; DMZ to Corp). An IDS system, updated and patched operating systems and services, could have helped prevent the attack simulated in the exploit demo.

Q 9. Would a similar exploit be possible on a network that uses a terminal server with remote clients to allow access to the SCADA network on the business network computers?

That would depend on how well the terminal server is maintained. Patching would need to be up to date, servers limited to terminal services ONLY, remote client devices used for remote access ONLY, remote client devices islanded while VPN'ed into the terminal server, and IDS and IPS rules that allow access from the terminal server to specific points ONLY, based to Role Based Access Control (RBAC).

Q 10. Please provide full elaboration on how the hack started and how to use Metasploit (MSF) command and scanning part of ICS?

The attack began when the attacker started a pseudo webserver that only served up malware. They then created a webpage that included a link to the malicious server. The victim clicked on the malicious link that requested the malware, which then exploited the victim’s browser and gave the attacker a Meterpreter shell into the victim host. No scanning was performed during the demo.

Q 11. How can we verify a contracted service company has changed default passwords on devices?

As part of your Statement of Work (SOW) or Service Level Agreement (SLA), you must require third-party contractors to list all devices that are their responsibility, list all default passwords, and list all changed passwords with documented proof.

Q 12. Is there a way to recreate the attack demo in a closed, safe environment to better understand how this works and what is being used?

It is advised to create a "sandbox" of your own. This will require the creation of a standalone network environment with segmentation that duplicates your production networks. You will need only one of each type of device/application/service/IP component. The demo environment used in the training is setup with VMs on desktop workstations. You can use whatever is available that will support your operational requirements. The cost to create this type of sandbox is more cost effective vs. an actual production environment.

Q 13. Please give an example of poor egress rules mentioned during the exploit demo.

The firewall rule that allowed the attacker to establish a connection from the PCS network all the way to the Internet was one. Egress should be from "Trust" to "Untrust" for one level ONLY. Firewall rules should also be point-to-point -- meaning IP or system to a particular system. Never allow the entire network to be allowed, even if it is a Trusted network.

Q 14. Can you discuss triage? If you inherit an antiquated system with security implemented in 1999, what is your first priority?

Your priority would be to map the environment and create an asset inventory. Include in the inventory – OS, hardware platform, applications, ports/services, patches, passwords, RBAC. If you accomplish that you can use it to make a priority list based on cybersecurity deficiencies. Once you have created your asset inventory, perform an evaluation of your environment with the DHS Cyber Security Evaluation Tool (CSET®). The CSET® reports will give you a priority list for you to implement.

Q 15. During the hack demonstration, are the commands the hacker used common commands among ICS users?

The attacker did not use any ICS commands during the attack. The attacker used Metasploit Framework to exploit systems and inject a payload (VNC) to capture the PCS HMI and manipulate the devices from there.

Q 16. Did the exploit elevate privileges on the CORP PC to do route add commands, or was the user running with admin permissions already?

The user on the CORP computer had administrator privileges. However, the attacker did not actually add a route on the victim host. The route was added within msfconsole to direct msfconsole where to send its packets. Once the packets where sent through the Meterpreter session, they were passed onto the victim’s network and used the victim’s normal network routing to reach their destination.

Q 17. Can you provide more details about possible threats during use of unidirectional communication (data-diodes, unidirectional gateways)?

Possible internal initial intrusion into ICS net with the following data transfer via unidirectional device outside? That is one benefit to unidirectional communication. That is, if the gateway is the only path for data to go from trust to untrust, then it becomes more secure. Also, a data diode is a physical connection, not a network connection -- which removes data diodes from network attacks.

Q 18. What are some of the vulnerabilities in legacy equipment? Are legacy OS really used in active ICS installations?

Because legacy equipment was built considering functionality and reliability first and security as an afterthought, we see many vulnerabilities, including:

- Plaintext protocols, ICS devices will do what they are asked/requested to do as long as it is valid commands
- Weak or default passwords
- Little or no patching of known vulnerabilities
- Systems running on end-of-life OSs
- No password check or verification on PLC programming downloads
- TRISYS, leaving a safety system PLC in remote program
- Trusted communications

When we poll our audience, we see old systems that are 30,40, even 50+ years that are still in use. That is one of the difficulties of the ICS environment, legacy systems, OS and equipment that may not be actively patched or updated.

Q 19. What are the dangers inherent in having unguarded equipment out in the field?

An attacker can connect to the device, perform MITM (man-in-the-middle) attack, replay attack, DDoS, and any number of things. The warning street signs are a good example. The default passwords were easy to obtain or crack. They were accessed and then used for a “joy ride.” Also, rogue wireless access points can be installed and used for access into the ICS network.

Q 20. What are some the most vulnerable protocols with known exploits in the Oil and Gas industry?

It is the same as all other industries. The oil and gas industry can use any protocol depending on what equipment they are using. The most common I have seen is Modbus and OPC, both which are subject to specific exploits.

Q 21. What are the most common tools for network asset inventories and auditing? Do these tools provide high fidelity results? What would be the best tool for mapping industrial networked assets?

There is a lot of different ones we talk about in this class. They can provide as high fidelity as you want, depending on your network. One of the best tools for mapping the network would be GrassMarlin, which is covered in the defense section. There also are many commercial tools available for doing network discovery on an OT network.