FAQ

Have any questions?

Frequently asked questions related from the ICS Cybersecurity Virtual Training.

Session 4 - Exploitation Process and Metasploit

Q 1. What are some good techniques (active and passive) for determining what vulnerabilities an ICS component may have?

Research is the best way to start, and the beginning of the research would be to have a complete inventory of each ICS field device and what version of software is running on those devices. From there you can query your vendor(s) for known vulnerabilities. The other place to go is the National Vulnerability Database where you can search for vulnerabilities.

Q 2. If the firewalls didn't allow direct egress back to the attacker, what other options does the attacker have to gain control of the PCS?

Firewall egress rules are a great way to stop attacks. However, in some cases it is possible to do a Bind connection instead of a Reverse connection where the attacked system does not call back out. Another way for an attacker to access the ICS network is via removable media, or perhaps wireless capabilities.

Q 3. Which of the analytical frameworks do you think is more effective to represent cyber attacks on ICS environments? (Cyber Kill Chain / Diamond Model / MITRE ATT&CK)

Any framework that addresses ICS environments would be good. Michael Assante and Robert Lee defined an ICS Kill Chain in 2015, and recently Mitre included an ICS matrix in their Att@ck framework. What is nice about Mitre's framework is that it is constantly being updated.

Q 4. Can we run tools other than Meterpreter commands (e.g., password cracking tools, scapy scripts, Nessus scanners) through Meterpreter routing?

Yes, it is possible to run other applications through a Meterpreter session by using the Metasploit socks proxy module within msfconsole. Meterpreter also has upload and download capabilities so a script could be uploaded and executed on a victim host.

Q 5. Would hackers use formal software such as Metasploit to illegally investigate vulnerabilities? Additionally, would firewalls or malware protection software be able to alert on traffic through known software packages like this? If so, how could a hacker avoid the obvious challenges that poses?

Hackers may use portions of Metasploit during an attack if there is a module that might help them. Yes well-known tools such as Metasploit are detectable; however attackers will have their own attack tools to try and avoid detection.

Q 6. What literature would you recommend for someone to gain more depth of knowledge with Metasploit?

https://www.offensive-security.com/metasploit-unleashed/ is a good place to start and installing and running Metasploit is always good. There are also training courses you can take.

Q 7. Can you use routing with Metasploit to send the outbound traffic through one of the compromised boxes?

Meterpreter routing is simply a way to route traffic from the attacker's host through the Meterpreter session to the victim host. Once the traffic goes through the Meterpreter session it uses the victim's normal network routing to get to the final destination.

Q 8. What are some Metasploit module examples for use against ICS systems?

A few of the modules are Schneider Modicon Quantum Password Recovery, Moxa Device Credential Retrieval, Yokogawa CENTUM CS 3000 Heap Buffer Overflow, Modbus Client Utility, Modbus Version Scanner, and CitectSCADA/CitectFacilities ODBC Buffer Overflow.

Q 9. I was most confused by the Meterpreter. How would this be used?

Meterpreter is like taking a part of Metasploit and sticking it onto the victim host to interact with the host, upload and download files, and use the victim as a pivot point into the victim's network. Through a Meterpreter session, post exploitation modules can be launched, and other applications can be run, including remote desktop sessions.

Q 10. What is the most common software and or other application used to monitor and notify of possible attacks?

It all depends on your network and ICS vendor. You can use an open-source IDS and install an open-source SIEM; but if it is not approved by your DCS (ICS) vendor, you probably should not (without lots of testing and understanding the programs).

Q 11. Is Metasploit available to government employees?

Most government systems are not allowed to install this type of "hacking" software. Also, some anti-virus software will flag Metasploit as bad and remove it. Check with your cybersecurity office for more information.

Q 12. Are you providing the information regarding Metasploit so we can (a) identify vulnerabilities within our ICS, (b) understand/recognize what Metasploit can do to a vulnerable environment or (c) both?

The most correct answer is ‘C’. Metasploit provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers.

Q 13. Is there a way search for Metasploit modules?

There are a couple ways to search for modules and keywords. In msfconsole there is the search command. There is also the Metasploit Exploit Database, which has search capabilities.

Q 14. How does the MITRE ATT&CK Framework assist attackers and defenders in threat analysis or attack planning?

The Mitre Att&ck framework is a 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. It tries to illustrate the actions and techniques an attacker may have taken during an attack. There is also the Mitre Att&ck framework for Industrial Control Systems that builds on the original framework that describes actions an attacker may take while operating within an ICS network. It focuses on adversaries who have a primary goal of disrupting industrial control processes, destroying property, or causing harm or death.

Q 15. Is Metasploit the only application utilized for malware delivery, or just the most common/useful?

For cybersecurity professionals, Metasploit Framework is the most common exploitation framework. There are also some exploitation frameworks that you can pay for, such as Metasploit Pro, Core Impact, Canvas, and Cobalt Strike.