FAQ

Have any questions?

Frequently asked questions related from the ICS Cybersecurity Virtual Training.

Session 5 - Network Attacks and Exploits

Q 1. The video mentioned storing salt and password in the user database. Did it mean both salt and hash, because the storing separately is no longer considered worthwhile?

If the salt is stored somewhere else other than right next to the password, there might be a gain of additional security, however it almost defeats the purpose of salting. Every time you want to validate a password, you need both the salt and the hashed password, so having them close can speed the validation process.

Q 2. Any suggestions on keeping wireless access points secure in large places such as refineries?

Verify the configuration and security settings. Several manufacturers have physical locking devices to secure the AP and the physical ports.

Q 3. Are there sandbox type environments where people test these techniques, or is it best practice to create your own environment?

There are several sandbox environments depending on your topic. By leveraging virtualization software, a sandbox can be created relatively inexpensively. OWASP.org, pentestmonkey, and hackthebox are a few quality outside resources, but always use caution.

Q 4. Regarding SQL injection defenses, is it possible for people (hackers/intruders) to get around properly parameterized queries?

There are no absolutes when it comes to cybersecurity, but properly parameterized queries are an effective solution to deterring SQL injection attacks.

Q 5. What are some wireless technologies used in ICS, and what are some recommended wireless techniques to practice beyond basic?

Wi-Fi, ZigBee, Bluetooth, Zwave and Software Defined Radios. Learning how to capture wireless traffic and analyze it.

Q 6. Any thoughts on 5G and how it will impact security in the wireless space?

5G security is more complex and complicated to manage (better encryption). Because there are more and more IoT devices, there are more vectors that can be leveraged by attackers. Any new technology brings new security challenges.

Q 7. The notes say to "Turn off SSID broadcasting." Isn't it relatively easy to determine hidden SSIDs these days?

Yes, it is. It can be part of your security plan. Every layer of protection can help.

Q 8. Is it possible to brute force hack a website/database that has a password limit? If so, how?

Yes, but it is tedious. However, an attacker can still run through the top 100 passwords relatively quickly. Hackers usually do not knock on the front door. They enter through the back window where nobody is watching. Brute-forcing usually means a hacker has already obtained the encrypted (hashed) passwords and has them in their possession. After the hacker gets the encrypted passwords on his computer, they can get as many additional computers as they want and run password crackers on them in parallel at their own convenience. The only thing that slows them down is the quality of the passwords and the quality of encryption.

Q 9. What are some of the other devices that use legacy Wi-Fi in ICS that will not be able to integrate WPA2 technology?

Inventory systems, sensors, older isolated segments of the network. According to this statistic: https://wigle.net/stats# about 7% of Wi-Fi networks still use WEP for encryption today. It is not a lot -- but at the same time, considering WEP was deprecated in 2004, it is. There are indeed systems and networks that continue to use WEP because the systems are too expensive or deemed unimportant to upgrade. The real danger of WEP is that it is trivial to obtain the encryption key.

Q 10. Is it best to protect databases with certificates?

SQL Injection has nothing to do with the security of the connection. Rather, it has to do with the security of how you handle user input. Using prepared statements helps prevent purposefully mis-formed input data from corrupting your SQL queries. If all of your users are trusted users who must log in, using SSL can provide some level of security against SQL injection, as you would be more confident that the users who get into your application would not be attempting to hack your system. However, SSL is no substitute for properly writing your database access code.

Q 11. Is Wi-Fi hacking protection is better built on a RADIUS server?

Yes. The user must provide their own unique, core set of credentials. Essentially, the same credentials users leverage to log in to their work system are the ones they will use to access to the network. With RADIUS in place, you no longer need to worry about bad actors stealing your network SSID and passphrase from a conference room whiteboard. The result is vastly improved network security. There are administrative costs to integrate it with several components and directory services.

Q 12. Please recommend some most persistent current wireless technologies, and some prospective ones.

WPA2, 900MHz, WEP too slowly being deprecated. Newer low-cost options ZigBee, Zwave, Bluetooth. More and more 5G IOT solutions, and of course, WPA3

Q 13. Can you discuss some of the challenges of monitoring wireless traffic?

Similar to the challenges of Network Monitoring, making the invisible visible, there are potentially multiple access points running different channels and frequencies at different strengths. Physical map of signal strengths. Sheer quantity of traffic.

Q 14. What if no password found in the Rainbow table?

If after all the iterations your password is not represented in the rainbow table, congratulations! Remember, the hacking community does not have every possible password hashed, so the key to not falling prey to a dictionary or Rainbow table attack is to ensure you do not use passwords that would be common enough or short enough (10 characters or less) to end up in a hackers' dictionary or Rainbow table."

General

Q 1. Can we get a copy of the full guide?

Currently we do not provide a full copy of the classroom trainee guide.

Q 2. Can we get a copy of the slide deck to keep for reference and share within my organization?

Slide decks are not available for distribution. However, feel free to download and share the participation guide.

Q 3. Do you have any advice on making a career transition from IT to OT (ICS)?

Take online OT training courses to get familiar with OT terminology, devices, services, servers, applications etc. There are online courses offered by DHS CISA available on this VLP website. Then work with your OT personnel and ask what types of ICS system(s) they are responsible for and where you can get information about it/them to study.

Q 4. How has working from home affected hacker’s ability to access our systems more easily?

It depends if you had to have outside access enabled on your Network Monitoring system. If nothing on your system has changed then your security is the same as before. It also depends on if more outside access to the ICS environment was required and how that access was enabled. If you had well defined and established remote access prior to teleworking, then the level of cybersecurity should be the same.