"Captain's Log……….<RED ALERT!>"

Course Syllabus – February 2022 – We will be using the WebEx virtual link on this email! Stay tuned!

Round Table discussion:

Log4j/Log4shell

- What is it? How did it start?
- What have we learned?
- Mitigations and Remediation

Hands on Labs - Exploitation and Remediation

- Vulnerable Docker application
- HTB LogForge
- TryHackMe - Solar

Huddle Up – (10 min) (What did we learn? What would we like to see next time?)

⚠

Notes to Consider….

1. Code of Ethics – do not hack me, I will not hack you…hacking is illegal without permission!
2. Stay on the subnet! See rule #1
3. Environment for a 5–10-year-old…. growing learning environment
4. Change default password!
5. Learning Linux basics (some homework)
6. Chmod to make an executable, python basics, working with packages….
7. Contribute! Share your work, scripts, resources, etc.…. (Teamwork makes the dream work)
8. Taking notes is a must! Screenshots welcome!
9. Recordings…. ok, but remember rule #1
10. Ideas and suggestions welcome! Open forum!
11. Have fun!

Remote Notes:

- Add resources to cloud share/downloads….
- Demonstrate working environment/vulnerable devices
- WebEx, Zoom, any streaming application….

Quiz:

What vulnerability does log4shell exploit?

What is the CVE for log4shell?

Which protocol is mainly used in the attack?

Which company originally reported the vulnerability?

What are some of the log levels of Log4j?

What sandbox gaming platform was vulnerable to the Log4shell exploit?

What is the current version of Log4j, not vulnerable to log4shell?