2022 NSA CODEBREAKER CHALLENGE

CODEBREAKER CHALLENGE 101

- Annual technical NSA outreach effort
- Open to schools based in U.S. or territories
- Runs throughout the fall semester
  - August – December

TECHNICAL FORMAT

- Challenge is a series of technical tasks
  - Follow a realistic story line
  - Varied difficulty (starts easy, ends hard)

- Goal: Complete tasks and
  - Learn a bit about NSA's mission and technical work
  - Sharpen your crypt / cybersecurity skills

2022 SCENARIO

- A company's internal network has been taken over by ransomware. They called FBI, who asked us for technical assistance.

MISSION

- **Find** the attacker's identity
- **Identify** the tools that they used to carry out their attack
- **Investigate** a Ransomware-as-a-Service website used by the attacker
  - **Find** and **Exploit** vulnerabilities to recover the victim's files

TASKS

- Tasks A1-A2: Investigate the Victim's Network
  - Task A1: Which user account was compromised? (Log Analysis)
  - Task A2: Recover the attacker's tools and discover their identity (Network and File Forensics)

TASKS

- Tasks B1 – B2: Investigate the Ransomware Site
  - Task B1: Locate ransomware-as-a-service website (Web reverse engineering)
  - Tasks B2: Find more information about the RaaS site (Web analysis & exploitation)

TASKS

- Tasks 5-6: Gain access to the RaaS Site
  - Task 5: Recover information from the attacker's computer (Reverse Engineering, Cryptanalysis)
  - Task 6: Access the RaaS site as the attacker (Web Hacking)

TASKS

- Tasks 7-9: Recover the victim's keys
  - Task 7: Escalate privileges to an administrator account (Web Hacking)
  - Task 8: Find the key-encrypting-key used to protect the keys that encrypt victim's files (Web Hacking, Reverse Engineering)
  - Task 9: Recover the victim's files (Cryptanalysis, Software Development)

SKILLS LEARNED

- Forensics (network, host)
- Binary Reverse Engineering
- Web Analysis and Exploitation
- Cryptanalysis
- Software Development

TECHNICAL BACKGROUND

- Host Forensics
- Network Traffic Analysis
- OpenSSH ssh-agent
- Web Exploitation
- Binary Reverse Engineering

HOST FORENSICS

- Log Analysis
  - Unsure about format? Look for documentation!
  - Parsing manually is painful. Use scripts.

- Look for things that stick out:
  - Unusual errors?
  - Unlikely combinations of events?

NETWORK TRAFFIC ANALYSIS

- Wireshark is excellent for analyzing network packet captures
- If you happen to have a server's private key, Wireshark can even decrypt SSL traffic

OPENSSH SSH-AGENT

- Used to hold private keys in memory for SSH authentication
- Core dump: contains contents of volatile regions of memory, typically used for debugging
- Your challenge for Task 5: extract a private key from an ssh-agent core dump
  - Some reverse engineering skill is necessary, but remember that OpenSSH is open-source

- Recommended tools: Ghidra, GDB

WEB EXPLOITATION

- Web sites often have common classes of vulnerabilities
- OWASP (Open Web Application Security Project) Top 10 (2021):
  - Broken Access Control
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring Failure
  - Server-Side Request Forgery

BINARY REVERSE ENGINEERING

- Recommended Tool: Ghidra
- Reverse Engineering Tips
  - Interesting strings?
  - System calls? (Network sockets, file I/O)
  - Linked libraries
  - Exported symbols
  - Debug symbols, if you're lucky

- Best way to get better is to practice!
  - Lots of resources / tutorials online.
  - Codebreaker "Resources" page; Ghidra tutorials

GET STARTED

- Visit `nsa-codebreaker.org`
- Sign up with your school email address
- Learn and have fun!
- Challenge open until late December

THANKS!

nsa-codebreaker.org

codebreaker@uwe.nsa.gov

www.intelligencecareers.gov/nsa

- Summer Programs: Sep 1 – Oct 31