Building an Effective IT Team for CCDC

Team 6

Recruiting Processes

- Interested students applied to the team, expressing interest in up to four of the team's specialized roles
    - Made up of club members and individual applicants
- Applicants were scheduled for interviews to showcase technical skills, research and learning ability, and passion for cybersecurity
- Based on interviews and observations, team members were chosen for Linux, Networking, Windows, and Liaison roles

Assignments and Job Roles

Position Details:

- Windows: Manages AD, DNS, and GPOs. Utilizes PowerShell and SysInternals heavily.
- Linux: Focused on a variety of services across Debian, RHEL, Arch, and Alpine based systems. There is a lot of focus on Bash and systemd.
- Liaisons: Handles injects, research, and team support. Helps keep the team organized and on-track.
- Networking: Configures Palo Alto firewall scripts, ACLs, and defends against unwanted traffic. Also must learn a little bit of Linux.

Training Regimen

General Focuses:

- Research on vulnerabilities, threat-hunting, troubleshooting, and recognizing IoCs.
- Script development for automation and custom tooling.
- Hands-on practice in virtual machine environments with our Cyber Range.

Additional Training and Resources:

- 3 WRCCDC Invitationals
- Self-hosted skirmish with another team and a red team
- Frequent “fun” inject slam days
- CCDC and WinterKnight Discord servers
    a. Interacting with the wider CCDC community has been extremely educational

Organizational Procedures and Tools

- GitHub
  1. Scripts, templates, and tools
- Google Drive
  1. Research, guides, docs, etc
- Discord:
  1. General communication, announcements, online practices
- Sub-roles
  1. Beyond the simple title of Linux, Windows, Networking, or Liaison
- Defined processes
  1. Procedures for performing technical injects
  2. Incident Reports
  3. Threat hunting

Team Collaboration and Practices

- Communication and collaboration have major focuses this year

- Discord
  a. Main communication hub
  b. Updates, joint-work, and group research

- Scripting
  a. A new, huge focus for the team
  b. We spent half of our practices working on building, testing, and breaking our scripts

- Practices - (Up to) 10 hours a week
  a. Two 3-hour in person sessions Friday and Sunday
  b. Two 2-hour online sessions Monday and Wednesday (open)

Conclusion and Future Outlook

Summary: Our team excels due to:

- Organized roles, expectations, and procedures.
- Frequent, varied training.
- Extra competitions.
- Practiced and refined communication.
- Pure passion.

Next Steps: Taking the base we've built this year and expanding it and our training even further. Continue competing as much as possible as well as grow and improve our skirmish.

Any Questions?