Applied Purple Teaming – C0200 Course Lab Infrastructure
Technology Overview
Design Considerations
Connection and Account Information

Applied Purple Teaming Lab

- We built environment specifically for this course.
- You can build this this same lab your environment with modifications to ensure that your network specifics are similar.
- Consequently, Lifecycles will be tailored specifically to your environment.

Development is not done in Production

- You can destroy things.
- That would be bad.
- Really bad.
- For all of us.

- So… APT Development Lab

Lifecycles Start In Development

Lifecycles:

- First tested in lab environment
- Define necessary changes in lab environment
- Deploy changes in lab environment
- Regression Testing? Have there been adverse effects in the lab environment?
- Pilot test changes in production (Change Management)
- Deploy changes to production (Change Management)
- Retest as Fidelity Check: In lab environment and production

Lifecycles End in Production

Lifecycles:

- Lifecycle output is a Change Control application that lists the necessary changes to deploy changes (or no-changes) in production environment.
- Dependency Review
- UAT testing, etc.

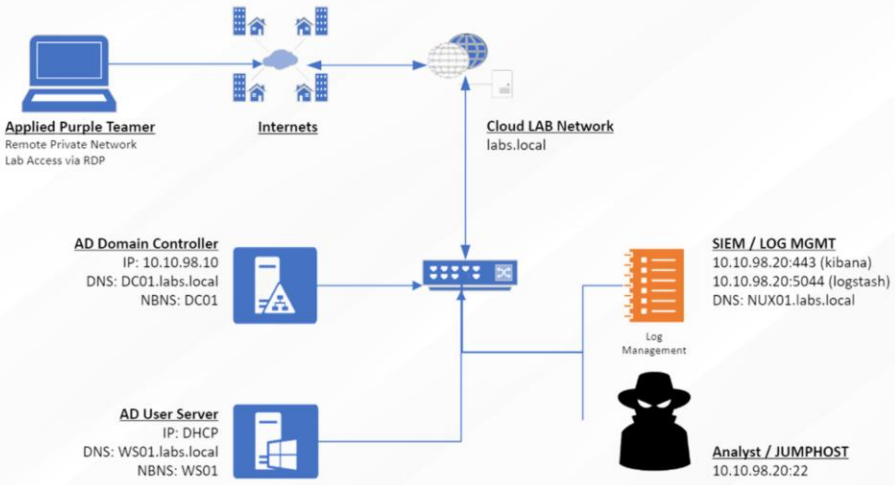
APT Lab Infrastructure

- A smaller network/infrastructure designed similar in nature to your production enterprise networks.
- The environment should use similar network infrastructure, operating system, programming, etc.

Class APT Lab Infrastructure

- Windows 2016 Member Server (WS01) - 10.10.98.14
- Windows 2016 Domain Controller (DC01) - 10.10.98.10
- Ubuntu Linux Host (nux01) - 10.10.98.20
  - HELK SIEM – Kibana, Kafka, Elastic Stack
  - CrackMapExec
  - John the Ripper binaries
  - Impacket toolkit
  - Responder
  - SilentTrinity C2 Framework

APT Lab Infrastructure



defensiveorigins.com