Project 2: Red Team Virtualized Data Communication Networks

Company Description

During our 35-year history, FTI has steadily developed a sterling reputation in the government support space, leveraging our proven military-tested technologies to provide customized decision-making software to the DoD. We help our customers to make the best, most informed decisions using data they trust. FTI continually invests in developing new technology, tools, and techniques enabling more sophisticated capabilities around augmenting data analysis and exploitation- they are purpose build and are highly scalable and extensible. At FTI, we have an opportunity to make a big difference, solving some of the most complex problems our nation has to offer. For this project, students will be supporting FTI's cyber team..

Team Size

- Red Team 3 – 5 people

Location

- The network will be based in the FTI's Chesapeake Virginia office, but the students will work and participate remotely through virtual Team's meetings.
- Willing to accommodate with class schedule as needed.

Project Description

This proposal is for two virtualized data communication networks. These networks will be built with two specific purposes.

- The first network, ACME, will be a typical Microsoft Windows Active Directory (AD) virtualized environment consisting of VMware, Windows AD servers Virtual Machines (VMs), Database server, Windows 10/11 and Red Hat Linux client. VMs. This network will serve as an administrative network for day-to-day operations ACME Business Solutions.
- The second network, Hackers-R-Us, will also be a typical Microsoft Windows AD virtualized environment consisting of VMware, Windows AD servers, Windows 10/11 and Red Hat Linux client and Kali Linux client VMs. The Kali Linux VMs will be running penetration test tools for Red Team operations against the ACME network.

These networks will be used to test different security postures to aid in the overall cyber survivability impact of each network in a cyber contested environment.

Objectives of the Networks

The network is designed to achieve several specific business/operational objectives:

- Secure Service: The main objective of the ACME network is to provide secure administrative computing service to the business. It is designed to be functionally and physically isolated from access by people not employed by the ACME Business Solutions system to minimize the risk of unauthorized use.
- Versatile Information Processing: The network will enable users to retrieve, process, and store ASCII and non-ASCII text, still graphics, audio, and video from any connected computer or VM.
- Collaboration: The network will combine the power and capabilities of diverse equipment to provide a collaborative medium that helps users combine their skills regardless of their physical location.
- Scalability: The design is scalable so that more VMs can be added as needed.

Intended Users

- The primary users of the ACME network will be members of human resources, accounting, administration, and the information technology department to include system administrators, information assurance engineers, and network engineers.
- The primary users of the Hackers-R-Us network will be system administrators, information assurance engineers, network engineers, and Red Team penetration testers.

Project Goals

- Networks are secure from adversarial threats.
- If/when threats are detected, and systems compromised networks operations are able to continue to accomplish business objectives.
- Threats are detected and neutralized within a specific timeframe.
- Create scripts to automate some of the security hardening and log scraping.
- Create/modify exploits to use during Red Team operations using Bash, Python, etc.

Design Assumptions

This design assumes the following:

- Both networks have a firewall that protects all information coming and going.
- Internet service is provided by a local ISP.
- VPN access will be utilized to build the network infrastructure.

Technologies

- VMware
- Firewalls/IDS
- Routers
- Switches

- MySQL database

Student Outcomes

- Work with real-world Enterprise software and hardware.
- Learn how to function as part of a Red Team and what test tools are utilized by each team.
- Learn to manage and secure computer systems, networks, and IT infrastructure from unauthorized access, attacks, misuse, or damage by implementing various security processes, technologies, and best practices.

Work Details

- Work will be between the hours of 9:00 – 5:00, Monday – Friday as schedules allow.
- Students that meet or exceed project expectations may be offered internship opportunities which can extend into a full-time position.