***A picture containing text, clock

Description automatically generated***

This project was supported by the Cybersecurity and IT Pathways grant from the Florida Department of Education through Cyber Florida, project number 291-1231C-2C001, funding authority 84.425C-D CRRSA ACT ESSER II 84.425D & GEER II 84.425C, FAIN#: S425C210052. More information at cyberflorida.org/pathways/

**Chapter Case**

Chapter 16 Cybersecurity

The Chapter Case was written for the Florida Public School System DIGITAL INFORMATION TECHNOLOGY (8207310) course. Funded by the Cyber/IT Pathways Program, Cyber Florida, and the Florida Department of Education.

# Chapter 16 Cybersecurity

## The Red Team Operators

NIST defines a “Red Team” as a group of people authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s security posture. The Red Team’s objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and what works for the defenders (i.e., the Blue Team) in an operational environment—also known as Cyber Red Team.[[1]](#footnote-1) In Figure 1 below, two Red Team operators are attempting to exploit any vulnerabilities by the Widget Inc. Human Resources (HR) department.

Damian Hatter, Red Team Operator 1, walked past the Widget Inc. HR department and looked through several of the windows to observe the general layout of the room prior to entering. He noticed that a single HR clerk was sitting behind a front desk, and there were several workstations positioned across the room that were shielded by cubicle walls. Hatter then walked in the HR department and approached the HR clerk behind the front desk. He asked the clerk if he could fill out an application for a job opening.

The clerk then directed him to sit down at a workstation and click the shortcut icon located on the PC desktop to begin the application process. Hatter then proceeded with sitting down at one of the workstations while the clerk remained sitting behind the front desk (see Figure 6).

Shortly after Hatter sat down at a workstation, he began to evaluate the PC for vulnerabilities. His primary goal was to implant a backdoor[[2]](#footnote-2) and maintain network persistence[[3]](#footnote-3) through a remote command and control server (C2)[[4]](#footnote-4) .

To accomplish this, he first started with verifying that he could use one of the open USB ports located on the PC. He reached into his pocket, pulled out his USB flash drive, and inserted it into an open USB port. The Windows Operating System immediately responded with a notification confirming that the USB port access was enabled. Upon confirmation, Hatter proceeded with opening his USB flash drive and executed a malicious program he had installed earlier prior to leaving his office desk.

The malicious program running on his USB flash drive then successfully communicated with his C2 instance running on a remote system located offsite from Widget Inc. Once he confirmed that his C2 instance could communicate with the malicious program executed from a networked PC located inside of the Widget Inc. network, his goal was complete. Hatter then ejected his USB flash drive, placed it in his pocket, and left the HR room.

As soon as Hatter left the HR room, Wanna Bee, Red Team Operator 2, walked in and went directly to a workstation without confronting the HR desk clerk. As soon as he sat down at the workstation, he immediately used a web browser to navigate to a website which he had previously setup on a remote webserver for the purpose of downloading malicious software. The user account setup on the PC had enough privileges to download and execute applications directly from the internet. Upon successfully downloading and executing the malicious software, Bee was able to communicate with the remote C2 system.

Hatter and Bee had successfully gained unauthorized persistent access to the Widget Inc. network. This was accomplished through exploiting unsecure physical and technical entry points.

Timeline

Description automatically generated

Figure illustrates a Red Team operation in a company’s Human Resources (HR) department.

## Case Questions

1. What vulnerabilities do you think exist in the HR department?
2. Identify as many cybersecurity controls as you can which you think should be added to the HR department based on this case scenario. Be sure to consider physical, procedural, or technical controls.

1. National Institute of Standards and Technology (NIST), Computer Security Resource Center, Red Team, Website accessed on 2/21/2023: <https://csrc.nist.gov/glossary/term/red_team> [↑](#footnote-ref-1)
2. Backdoor (computing), TechTarget, August 2017, Accessed from <https://searchsecurity.techtarget.com/definition/back-door> on 2/21/2023. [↑](#footnote-ref-2)
3. Maloney, Sarah, What is an advanced persistent threat (APT)?, Cybereason, 1/9/2018, Accessed from [https://www.cybereason.com/blog/advanced-persistent-threat-apt on 2/21/2023](https://www.cybereason.com/blog/advanced-persistent-threat-apt%20on%202/21/2023). [↑](#footnote-ref-3)
4. Command and Control Server, TechTarget, January 2017, Accessed from <https://whatis.techtarget.com/definition/command-and-control-server-CC-server> on 2/21/2023. [↑](#footnote-ref-4)