30 Bird–CompTIA Security+ (Exam SY0-701), Skill Labs

Course Specifications

Course Number: ACI76-014SL_rev1.0
Lab Length: Approximately 36 hours

30 Bird - Gathering Site Information (SY0-701)

Introduction
Overview

In this exercise, you'll perform simple probes on a website using browser-based OSINT tools. They show what the general public can learn about a website.

30 Bird - Footprinting a Website (SY0-701)

Introduction
Overview

In this exercise, you'll map a website using Maltego. To do so, you will need to register for a free Maltego account. The following instructions assume you're creating a new account using a student email address; alternatively, the instructor can create accounts for students before class.

30 Bird - Using Anti-Phishing Tools (SY0-701)

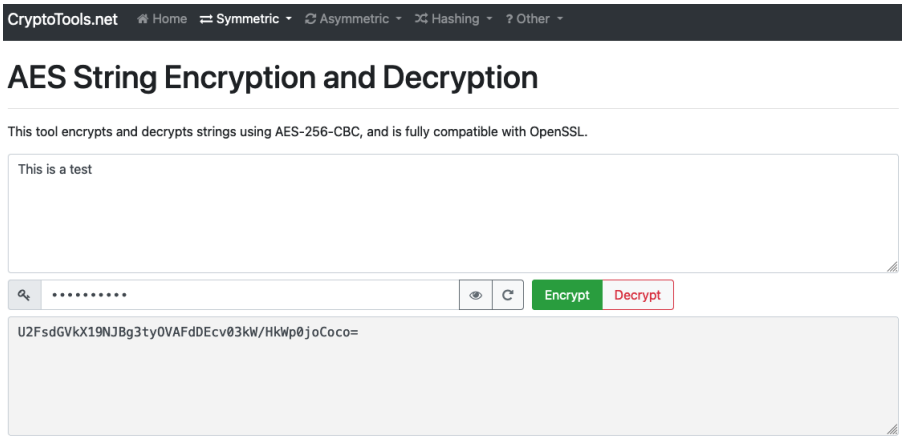
Introduction
Overview

In this exercise, you'll use a browser extension to detect phishing sites. The complete exercise may not work if your network has anti-phishing software or strict firewall rules. The Windows 10 VM must be running.

30 Bird - Using Symmetric Encryption (SY0-701)

Introduction
Overview

In this exercise, you'll examine AES encryption. You can perform it in any web browser.



30 Bird - Creating Asymmetric Key Pairs (SY0-701)

Introduction
Overview

In this exercise, you'll create RSA and ECC key pairs using the OpenSSL command-line tool.

30 Bird - Creating File Hashes (SY0-701)

Introduction
Overview

In this exercise, you'll use a hashing tool to demonstrate that slight data changes also alter the hash.

30 Bird - Examining PKI Certificates (SY0-701)

Introduction
Overview

For this exercise, you'll examine the Windows certificate store. The Windows 10 VM must be running.

30 Bird - Creating Certificates with OpenSSL (SY0-701)

Introduction
Overview

In this exercise, you'll create a self-signed certificate and a CSR using the OpenSSL command-line tool.

30 Bird - Launching a DoS Attack (SY0-701)

Introduction
Overview

In this exercise, you'll perform a SYN flood attack using the hping3 utility. Windows Server 2022 and Kali should both be open.

30 Bird - Capturing Credentials via Packet Sniffing (SY0-701)

Introduction
Overview

Many popular network protocols make it easy for eavesdroppers to scan for valuable information. In this exercise, you'll use a packet sniffer to capture a password.

30 Bird - Cracking Passwords (SY0-701)

Introduction
Overview

In this exercise, you'll use a password-cracking application to find your current Windows password.

30 Bird - Configuring a Network Firewall (SY0-701)

Introduction
Overview

In this exercise, you'll configure the network firewall built into the pfSense VM. pfSense serves as a router between your two Windows VMs and the Internet.

30 Bird - Installing Uncomplicated Firewall in Linux (SY0-701)

Introduction
Overview

In this exercise, you'll install and configure Uncomplicated Firewall in Kali. It's a simple front end for the nftables firewall built into Kali Linux.

30 Bird - Requesting a PKI Certificate in Windows (SY0-701)

Introduction
Overview

To use certificate-secured protocols, or authentication processes, you'll need to be issued a certificate by a CA. In this exercise, you'll request a user certificate from the domain's CA.

30 Bird - Securing a Wi-Fi Hotspot (SY0-701)

Introduction
Overview

Because this exercise uses a public web site, you can use it from any browser. However, the site may move or change. If the site is no longer available when you're taking this class, use a real WAP or a different emulator. In this exercise, you'll configure Wi-Fi security settings. The website is an online emulator of a popular WAP model, but most other models have similar available options.

30 Bird - Scanning the Network (SY0-701)

Introduction
Overview

In this exercise, you'll scan the local subnet for active hosts and services using the Nmap GUI.

30 Bird - Installing a RADIUS Server (SY0-701)

Introduction
Overview

In this exercise, you'll configure a Windows server to act as a network policy server for RADIUS authentication.

30 Bird - Examining Kerberos Settings (SY0-701)

Introduction
Overview

Windows Active Directory uses Kerberos as the SSO protocol to authorize access to all network resources.

30 Bird - Examining Active Directory Objects (SY0-701)

Introduction
Overview

Windows domains are controlled via Active Directory, Microsoft's directory service. AD uses LDAP, Kerberos, and DNS as its primary protocols. You'll examine some of AD's workings.

30 Bird - Delegating Control in Active Directory (SY0-701)

Introduction
Overview

In this exercise, you'll create an Active Directory group, then assign special permissions to it.

30 Bird - Enforcing Password Policies (SY0-701)

Introduction
Overview

In this exercise, you'll use group policy objects to enforce stronger Windows passwords.

30 Bird - Creating a Domain User (SY0-701)

Introduction
Overview

In this exercise, you'll add a new user to an Active Directory domain.

30 Bird - Creating Linux Users and Groups (SY0-701)

Introduction
Overview

In this exercise, you'll manage local users and groups on a Linux system.

30 Bird - Examining Spyware (SY0-701)

Introduction
Overview

In this activity, you'll use a keylogger which could be deployed as spyware.

30 Bird - Detecting Virtualization (SY0-701)

Introduction
Overview

In this exercise, you'll perform some simple commands to verify that your virtual environment is composed of VMs. If you were remotely accessing a similar network, it would take careful obfuscation by administrators to keep you from noticing the same.

30 Bird - Assigning NTFS Permissions (SY0-701)

Introduction
Overview

In this exercise, you'll explore how to view and assign permissions for an NTFS folder.

30 Bird - Creating a Security Template (SY0-701)

Introduction
Overview

NOTE: For this exercise, the Windows Server 2022 VM should be running.

30 Bird - Enforcing a Security Template (SY0-701)

Introduction
Overview

In this exercise, you'll enforce a security template.

30 Bird - Exploiting an Overflow Vulnerability (SY0-701)

Introduction
Overview

In this exercise, you'll exploit an overflow vulnerability. Although it's in a web application, similar vulnerabilities can exist in any software that accepts untrusted input.

30 Bird - Exploiting a TOCTOU Vulnerability (SY0-701)

Introduction
Overview

In this exercise, you'll exploit a race condition in a web application. Similar vulnerabilities can exist in any software.

30 Bird - Performing SQL injection in DVWA (SY0-701)

Introduction
Overview

In this exercise, you'll examine a command injection vulnerability in a web application.

30 Bird - Performing a Reflected XSS Attack (SY0-701)

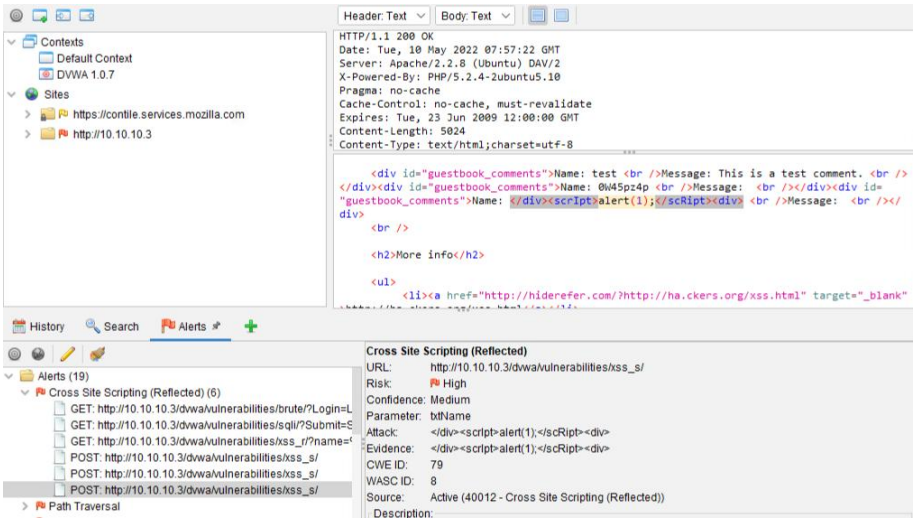
Introduction
Overview

In this exercise, you'll examine a command injection vulnerability in a web application.

30 Bird - Examining Web Application Vulnerabilities (SY0-701)

Introduction
Overview

In this exercise, you'll examine the results of a previously completed web application vulnerability scan.



30 Bird - Scheduling a Server Backup (SY0-701)

Introduction
Overview

Windows includes basic backup and recovery tools. You'll schedule a backup.

30 Bird - Viewing Windows Event Logs (SY0-701)

Introduction
Overview

In this exercise, you'll view event logs in Windows.

30 Bird - Viewing Linux Event Logs (SY0-701)

Introduction
Overview

In this exercise, you'll examine Linux system logs with journalctl, and view how they can be used to identify suspicious activity.