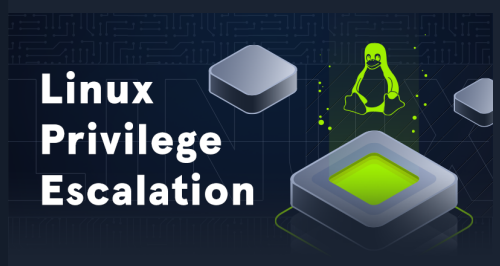
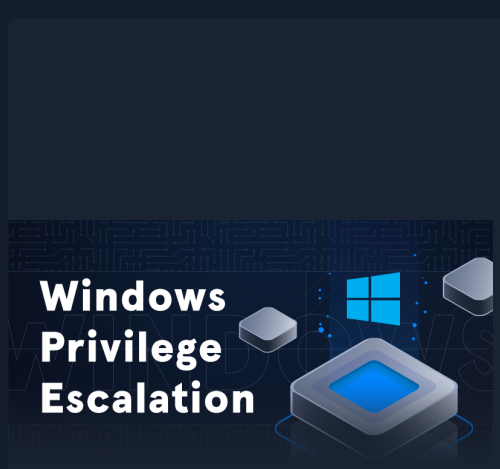
Student Transcript

19-06-2024

HTB ACADEMY

Brian Sivieri
#1186634

Targets compromised: 45
Ranking: Top 20%

MODULE	PROGRESS
 Intro to Academy 8 Sections Fundamental General Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.	50% Completed
 File Transfers 10 Sections Medium Offensive During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.	100% Completed
 File Inclusion 11 Sections Medium Offensive File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.	100% Completed
 Linux Privilege Escalation 28 Sections Easy Offensive Privilege escalation is a crucial phase during any security assessment. During this phase, we attempt to gain access to additional users, hosts, and resources to move closer to the assessment's overall goal. There are many ways to escalate privileges. This module aims to cover the most common methods emphasizing real-world misconfigurations and flaws that we may encounter in a client environment. The techniques covered in this module are not an exhaustive list of all possibilities and aim to avoid extreme "edge-case" tactics that may be seen in a Capture the Flag (CTF) exercise.	100% Completed
 Windows Privilege Escalation 33 Sections Medium Offensive After gaining a foothold, elevating our privileges will provide more options for persistence and may reveal information stored locally that can further our access in the environment. Enumeration is the key to privilege escalation. When you gain initial shell access to the host, it is important to gain situational awareness and uncover details relating to the OS version, patch level, any installed software, our current privileges, group memberships, and more. Windows presents an enormous attack surface and, being that most companies run Windows hosts in some way, we will more often than not find ourselves gaining access to Windows machines during our assessments. This covers common methods while emphasizing real-world misconfigurations and flaws that we may encounter during an assessment. There are many additional "edge-case" possibilities not covered in this module. We will cover both modern and legacy Windows Server and Desktop versions that may be present in a client environment.	21.21% Completed
 Introduction to Active Directory 16 Sections Fundamental General Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.	100% Completed