Red Teaming challenge: scenari di attacco dall'esterno

CODICE	**DT0111**
DURATA	**3 gg**
PREZZO	**2.800,00 €**
EXAM	

DESCRIZIONE

Approfondimento di tecniche come la scansione, l'enumerazione, l'abuso di condivisioni di file, il bypass di AMSI e Windows antivirus bypass, payload metasploit, enumerazione di domini, cattura e riutilizzo delle credenziali, estrazione di dati, elusione delle whitelist di applicazioni, abuso di SQL Server, pivoting, abuso di ACL, escalation dei privilegi di dominio e altro ancora!

Il laboratorio contiene una macchina basata su Linux per eseguire attacchi e una configurazione Active Directory di destinazione. L'AD di destinazione è un ambiente full patched con Windows Server 2022.
Il laboratorio ti consente di:

- Comprendere e mettere in pratica le basi per attaccare Active Directory utilizzando metasploit e altri strumenti.
- Comprendere come affrontare l'attacco su architetture Windows Server 2022.
- Imparare ad eseguire attacchi in memoria da Linux contro sistemi Windows.

TARGET

Security manager

PREREQUISTI

Nessuno

CONTENUTI

- Enumerazione di rete
- Bypassare AMSI e antivirus
- Generazione e utilizzo di payload in Metasploit
- Enumerazione di Active Directory
- Spraying attack e riutilizzo delle credenziali
- Escalation dei privilegi locali

- Estrazione di dati (SAM, LSASecrets, Lsaas process …)
- Nozioni di base sulla whitelist delle applicazioni ed elusione
- Abuso di server SQL
- Pivoting e Port Forwarding su Windows
- Abuso ACL di Active Directory
- Escalation a Domain Admin