

SZKOLENIE

INCIDENT RESPONSE W ZABEZPIECZENIACH CHECK POINT



CEL

Szkolenie ma na celu praktyczne przygotowanie osoby zarządzającej zabezpieczeniami Check Point w zakresie analizy rzeczywistych cyberataków, oceny sytuacji i reakcji na incydenty.

ODBIORCY

Osoby odpowiedzialne za zarządzanie cyberbezpieczeństwem w organizacji do skutecznego wykonywania swojej pracy powinny rozumieć sposoby działania cyberprzestępców oraz posiadać umiejętności wykorzystania dostępnych narzędzi i zabezpieczeń do analizy zdarzeń oraz podejmowania właściwych reakcji na incydenty.

ĆWICZENIA PRAKTYCZNE

Podstawą szkolenia są ćwiczenia, które odbywają się w sieci szkoleniowej wyposażonej w zabezpieczenia Check Point (NGFW, EDR) oraz indywidualne stacje uczestników zajęć wyposażone w odpowiednie narzędzia (stacje MS Windows i Kali Linux), a także różnego rodzaju serwery Web/SMB i środowisko Active Directory do wykonywania testów rzeczywistych cyberataków. Uczestnicy zajęć wykonują techniki stosowane w rzeczywistych cyberatakach wg MITRE ATT&CK (np. OS Credential Dumping: LSASS Memory/ Security Account Manager, Web Shell, Exploitation for Privilege Escalation, Lateral Tool Transfer, Pass the Hash, Exploitation of Remote Services - Eternal, Zerologon, Print Nightmare).

UNIKALNE KORZYŚCI DLA UCZESTNIKÓW SZKOLENIA

Uczestnicy zajęć wykonują realne techniki ataków, spotykane w rzeczywistych działaniach cyberprzestępców i przy tym posiadają dostęp do specjalistycznych systemów cyberbezpieczeństwa (m.in. Next-Generation Firewall z kompletem funkcji bezpieczeństwa, Endpoint Detection and Response z narzędziami Live Forensics i Threat Hunting), za pomocą których obserwują w jakim zakresie w rzeczywistości, możliwe jest wykrywanie poszczególnych technik cyberataków, za pomocą specjalistycznych narzędzi zabezpieczeń. Zdobyte w czasie szkolenia umiejętności w znacznym zakresie pomagają we wczesnym wykrywaniu i obsłudze rzeczywistych cyberataków.

Więcej informacji: audyt@clico.pl lub szkolenia@clico.pl

PLAN SZKOLENIA

DZIEŃ 1

WPROWADZENIE W TEMATYKĘ RED TEAM I ADVERSARY EMULATION:

- Jak przebiega rzeczywisty cyberatak?
- MITRE ATT&CK w realnych scenariuszach cyberataków.

ĆWICZENIA PRAKTYCZNE

Podstawowe umiejętności:

- Kopiowanie plików pomiędzy systemami Linux i Windows z linii komend.
- Zestawianie Bind Shell pomiędzy systemami Windows i Linux.
- Zestawianie Reverse Shell pomiędzy systemami Windows i Linux.
- Ćwiczenie dodatkowe: Tunelowanie komunikacji sieciowej w SSH.

Przykład włamania do serwera Web z użyciem Webshell, przejęcie poświadczeń z LSASS oraz administracyjny dostęp do kontrolera domeny metodą Pass-the-Hash:

- File and Directory Discovery, T1083 – Dirb.
- Network Share Discovery, T1135 - CrackMapExec, SmbClient.
- Lateral Tool Transfer, T1570 – SmbClient.
- Server Software Component: Web Shell, T1505.003 - aspx-reverse-shell.
- Exploitation for Privilege Escalation, T1068 - PrintSpoofer exploit.
- OS Credential Dumping: LSASS Memory T1003.001 - Procdump, Pypykatz.
- Pass the Hash T1550.002 - Impacket (Psexec.py).

Rekonesans i techniki popularne w rzeczywistych cyberatakach:

- File and Directory Discovery, T1083 - Dirb, Gobuster.
- System Information Discovery, T1082 - Net user, Adfind.
- Network Service Scanning, T1046 – Nmap.
- Network Share Discovery, T1135 - CrackMapExec, SmbClient, SmbMap.
- Malicious File, T1204.002 - Metasploit, Msfvenom, PowerShell.
- OS Credential Dumping: LSASS Memory, T1003.001 - CrackMapExec, Procdump, Pypykatz, Mimikatz.
- OS Credential Dumping: Security Account Manager, T1003.002 - Crackmapexec, PsExec, Reg Save, Impacket (Secretsdump.py).
- Pass the Hash, T1550.002 - Impacket (Wmiexec.py, Smbexec.py, Psexec.py), CrackMapExec, Evil-winrm.

DZIEŃ 2

Ataki exploit i cyberataki w środowisku Active Directory:

- Z czego składa się atak exploit?
- Narzędzia i zasady użycia Metasploit.
- Cyberataki w środowisku Active Directory.

Ćwiczenia praktyczne – Popularne techniki cyberataków w środowisku Active Directory

Scenariusz 1. Włamanie do serwera Windows z użyciem exploit na podatność, zebranie poświadczeń i przejęcie kontrolera domeny:

- Network Share Discovery, T1135 – CrackMapExec.
- Exploitation of Remote Services, T1210 – Metasploit.
- OS Credential Dumping: LSASS Memory, T1003.001 – CrackMapExec.
- OS Credential Dumping: Security Account Manager, T1003.002 – Crackmapexec.
- Pass the Hash, T1550.002 - Impacket (Psexec.py).
- OS Credential Dumping: NTDS, T1003.003 - Impacket (secretsdump.py).

Scenariusz 2. Włamanie do kontrolera domeny przez exploit na podatność, przejęcie poświadczeń i dostęp do innych serwerów w domenie:

- Exploit 1. Podatność MS17-010 Eternal (CVE-2017-0144).
- Exploit 2. Podatność Zerologon Vulnerability (CVE-2020-1472).
- Exploit 3. Podatność Print Nightmare (CVE-2021-1675).

DZIEŃ 3

Analiza śladów cyberataków z użyciem narzędzi dostępnych w zabezpieczeniach Next-Generation Firewall.

Analiza śladów cyberataków z użyciem narzędzi Live Forensics i Threat Hunting dostępnych w zabezpieczeniach Endpoint Detection and Response (EDR).

Techniki dodatkowe:

- Rejestrowanie i analiza ruchu sieciowego z użyciem Wireshark.
- OSINT w Red Team.