CEL

Osoby odpowiedzialne za zarządzanie cyber-bezpieczeństwem w organizacji, aby skutecznie wykonywać swoją pracą potrzebują rozumieć sposoby działania cyberprzestępców oraz posiadać umiejętności wykorzystania posiadanych narzędzi i zabezpieczeń do analizy zdarzeń oraz podejmowania właściwych reakcji na incydenty. Szkolenie ma na celu praktyczne przygotowanie osoby zarządzające zabezpieczeniami Palo Alto Networks w zakresie analizy rzeczywistych cyber-ataków, oceny sytuacji i reakcji na incydenty.

ĆWICZENIE PRAKTYCZNE

Podstawą szkolenia są ćwiczenia, które odbywają się w sieci szkoleniowej wyposażonej w zabezpieczenia Palo Alto Networks (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 cyber-ataków. Uczestnicy zajęć wykonują techniki stosowane w rzeczywistych cyber-atakach 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 w wczesnym wykrywaniu i obsłudze rzeczywistych cyberataków.

CENA SZKOLENIA: 3900 PLN OD OSOBY
(terminy szkoleń ustalane są indywidualnie dla grup min. 4 osób)

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

PLAN SZKOLENIA

DZIEŃ 1

WPROWADZENIE W TEMATYKĘ RED TEAM I ADVERSARY EMULATION:

- Jak przebiega rzeczywisty cyber-atak?
- MITRE ATT&CK w realnych scenariuszach cyber-ataków

ĆWICZENIE 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)

ĆWICZENIE PRAKTYCZNE

Rekonesans i techniki popularne w rzeczywistych cyber-atakach:

- File and Directory Discoverym, 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 cyber-ataki w środowisku Active Directory

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

ĆWICZENIE PRAKTYCZNE – Popularne techniki cyber-ataków 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 cyber-ataków z użyciem narzędzi dostępnych w zabezpieczeniach Next-Generation Firewall

Analiza śladów cyber-ataków 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