Authorized Training Center

CLICO

paloalto NETWORKS

INCIDENT RESPONSE

IN PALO ALTO NETWORKS SECURITY

TRAINING OBJECTIVE:

Those responsible for managing cybersecurity in organizations, in order to do their jobs effectively, need to understand the ways in which cybercriminals operate and be able to use the available tools and security solutions to analyze incidents and adequately respond to them. The training is designed to provide Palo Alto Networks security managers with hands-on experience to enable them analyze real-world cyber attacks, assess the situation and respond to incidents.

PRACTICAL EXERCISES:

The training is based on exercises performed in a training network equipped with Palo Alto Networks security (NGFW, EDR) and individual workstations of the participants equipped with appropriate tools (MS Windows and Kali Linux workstations), as well as various types of Web/SMB servers and Active Directory environment to perform tests of real-world cyber attacks. Participants use the techniques used in actual cyber attacks according to MITRE ATT&CK (e.g. 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).

UNIQUE BENEFITS FOR TRAINING PARTICIPANTS:

Participants use real-world attack techniques encountered in actual cybercriminal activities and, in the process, have access to specialized cybersecurity systems (including Next-Generation Firewall with complete security features, Endpoint Detection and Response with Live Forensics and Threat Hunting), with which they observe to what extent it is actually possible to detect particular cyber attack techniques using specialized security tools. The skills acquired during the training significantly help in the early detection and handling of real-world cyber attacks.

DAY 1

INTRODUCTION TO RED TEAM AND ADVERSARY EMULATION

- How does an actual cyber attack work?
- MITRE ATT&CK in real-world cyber attack scenarios

PRACTICAL EXERCISES

#1 Basic skills

- Copying files between Linux and Windows from the command line
- Setting up Bind Shell between Windows and Linux systems
- Setting up Reverse Shell between Windows and Linux systems
- Additional exercise: tunneling of network communication in SSH

#2 Example of hacking a Web server using Webshell, capturing credentials from LSASS and getting administrative access to a domain controller using Pass-the-Hash method

- 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)

#3 Practical exercises – reconnaissance and techniques popular in actual cyber attacks

- 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

DAY 2

#1 Exploits and cyber attacks in an Active Directory environment

- What does an exploit attack consist of?
- Tools and rules for using Metasploit
- Cyber attacks in an Active Directory environment

#2 Practical exercises – popular cyber attack techniques in an Active Directory environment

Scenario 1. Hacking a Windows server using a vulnerability exploit, collecting credentials and taking over a domain controller

- 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)

Scenario 2. Hacking a domain controller using a vulnerability exploit, capturing credentials and getting access to other servers in the domain

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

DAY 3

#1 Analyzing traces of cyber attacks using Live Forensics and Threat Hunting tools available in Endpoint Detection and Response (EDR) security

#2 Optionally, analyzing traces of cyber attacks using tools available in Next-Generation Firewall security

#3 Additional techniques:

- Logging and analysis of network traffic with Wireshark
- OSINT in Red Team

Training Price: 840 Euro net per person
(training dates are set individually for groups of min. 4 people)

Authorized Training Center
CLICO

More information:
assessments@clico.pl or trainings@clico.pl
www.clico.pl »