



SİBER GÜVENLİK EĞİTİMİ DERS NOTLARI

5.GÜN

Eğitim İçeriği
<ul style="list-style-type: none">❖ Cybrer kill chain❖ MITRE ATT&CK❖ Strings❖ Ltrace (Library Tracking)❖ Strace (Systemcall Tracking)

❖ CYBER KILL CHAIN

Cyber kill chain; Siber saldırıları analiz edebilmek amacıyla geliştirilmiş modellerden biridir. Lockheed Martin firması tarafından geliştirilmiştir. Keşif aşamasından saldırı aşamasına kadar olan işlem adımlarını içerir. Bu model 7 aşamadan oluşmuştur ve saldırıyı gerçekleştirmek veya önlemek amacıyla kullanılabilir. Cyber kill chain; kısaca özetlemek gerekirse bir kuruma siber saldırı yaparken veya savunurken uygulanan kurallar bütünüdür.



- Reconnaissance (keşif)
- Weaponization (silahlanma)
- Delivery (iletme)
- Exploitation (sömürme)
- Installation (yükleme)
- Command and control,c2 (komuta kontrol)
- Actions on objectives (eylem)

MITRE ATT&CK

MITRE ATT&CK, cyber kill chain 'in 14 maddelik halidir. MITRE ATT&CK, Günümüze kadar yaşanmış olan siber olayların kayıtları incelenerek, bir saldırının nasıl oluştuğunu hangi açıklıklardan yararlanıp saldırdığını, hangi teknikleri kullandığını gösteren bir kaynaktır. Bu kaynak kullanılarak saldırganların önceden hangi yolları kullandığını görülüp bir sonraki hamlelerini tahmin edebiliriz.

Web sitesine bu linkten ulaşabilirsiniz; <https://attack.mitre.org/>

MITRE ATT&CK Matrisi temel olarak saldırganlarının kullanmış oldukları teknikleri barındırır. Bu kullanılan teknikler ayrı ayrı kategorize edilmiş biçimde bulunur. Firma tarafından 3 bölüme ayrılmıştır. Bunlar;

- Enterprise ATT&CK
- Mobile ATT&CK
- ICS ATT&CK

Enterprise ATT&CK

Enterprise ATT&CK matrisi Windows, Linux veya MacOS sistemlerinde çalıştırılan teknik ve taktiklerden oluşur.

Mobile ATT&CK

Mobil cihazlara uygulanan taktikleri ve teknikleri içerir.

ICS ATT&CK

ICS endüstriyel kontrol sistemlerinin (SCADA, DCS, PLC gibi) kısaltmasıdır. Endüstriyel olarak yapılan saldırıların teknik ve taktikleri bu matris içinde bulunur.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Exploit Public-Facing Application	Command and Scripting Interpreter (6)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Execution (14)	BITS Jobs	BITS Jobs	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Encrypted Through Removable Media	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (3)	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)			Browser Extensions	Debugger Evasion	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Replicate Through Removable Media	Browser Session Hijacking (2)	Data Obfuscation (3)	Exfiltration Over Physical Medium (1)	Defacement (2)
Phishing for Information (3)	Establish Accounts (3)	Phishing (3)	Exploitation for Client Execution	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replicate Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Other Network Service (3)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Inter-Process Communication (3)	Domain Policy Modification (2)	Deploy Container	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Encrypted Channel (2)	Fallback Channels	Scheduled Service (3)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Modify Authentication Process (6)	Container and Resource Discovery	Taint Shared Content	Data from Cloud Storage	Ingress Tool Transfer	Exfiltration Over Web Service (3)	Firmware Corruption
Search Open Websites/Domains (3)		Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Escape to Host	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Configuration Repository (2)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Event Triggered Execution (16)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Information Repositories (3)	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
			Shared Modules	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Shifting	Domain Trust Discovery		Data from Local System	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
			Software Deployment Tools	External Remote Services	Hide Artifacts (10)	Hide Artifacts (10)	OS Credential Dumping (8)	File and Directory Discovery		Data from Network Shared Drive	Protocol Tunneling	Service Stop	System Shutdown/Reboot
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Steal Application Access Token	Group Policy Discovery		Data from Removable Media	Proxy (4)		
			User Execution (3)	Process Injection (12)	Impair Defenses (10)	Impair Defenses (10)	Steal or Forge Authentication Certificates	Network Service Discovery		Data from Staged (2)	Remote Access Software		
			Windows Management Instrumentation	Scheduled Task/Job (5)	Indicator Removal (6)	Indicator Removal (6)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Traffic Signaling (2)		
				Valid Accounts (4)	Indirect Command Execution	Indirect Command Execution	Steal or Forge Authentication Certificates	Network Sniffing		Input Capture (4)	Web Service (3)		
				Modify Authentication Process (8)	Masquerading (8)	Masquerading (8)	Steal or Forge Authentication Certificates	Password Policy Discovery		Screen Capture			
				Office Application Startup (6)	Modify Authentication Process (8)	Modify Authentication Process (8)	Steal or Forge Authentication Certificates	Peripheral Device Discovery		Video Capture			
				Pre-OS Boot (5)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Steal or Forge Authentication Certificates	Permission Groups (Discovery (3))					
				Scheduled			Steal or Forge Authentication Certificates						

STRINGS KOMUTU

Derlenmiş olan kodun içerisindeki stringlerin bir kısmını görüntülemek için kullanılır. Örnek bir c kodu yazalım.

main.c uzantılı bir dosyanın içerisine şu basit kodları yazıyoruz.

```
#include<stdio.h>
int main( )
{
    int val= 100;
    int val2;
    printf("Sayı giriniz /n ");
    scanf("%d",&val2);
    if (val== val2)
        printf("TRUE /n ");
    else
        printf("FALSE /n ");

    return 0;
}
```

Terminal ekranına " gcc main.c" yazarak kodu derliyoruz. Derlenmiş c kodu "a.out " ismiyle kayıt ediliyor. Terminal ekranından " strings ./a.out " komutu çalıştırıldığında aşağıdaki çıktıyı alırız.

```
(kali@kali) [~/Desktop]
$ strings a.out
/lib64/ld-linux-x86-64.so.2
puts
__libc_start_main
__cxa_finalize
__isoc99_scanf
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
__ITM_deregisterTMCloneTable
__gmon_start__
__ITM_registerTMCloneTable
PTE1
u+UH
sayi giriniz
TRUE
FALSE
;*3$"
GCC: (Debian 13.2.0-2) 13.2.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
main.c
__FRAME_END__
_DYNAMIC
GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_start_main@GLIBC_2.34
__ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
__edata
__fini
```

Ltrace (Library Tracking):

Program içerisinde çalışan tüm kütüphaneleri listeler.

Strace (Systemcall Tracking):

Programın kullandığı tüm sistem komutlarını listelemeye yarar