

Detecting Active Directory Attacks using Elastic

DISCLAIMER

whoami

- Rahul R - @Rahul_R95
- Security Consultant @ Activbytes
- CTF player
- SOC N00B

Agenda

- What is Elastic /ELK stack ?
- Creating our own Test Environment
- Analysing different attacks
- Creating Custom Alarms on Elastic SIEM

What is Elastic ?

Popularly known as ELK stack (Elastic Logstash Kibana)



Configuring your Test Environment.

Things you will be needing

- Windows Server (Victim)
- Attacker Machine (Any preference)
- Elastic Cloud Instance (14 days Free Trial)
- Winlogbeat (Log Collection)
- Sysmon
- Vulnerable AD (<https://github.com/WazeHell/vulnerable-AD>)

Configuring your Elastic Instance

Attack Map



Initial Access and Execution

IIS Executing System Commands

- Default Accounts for IIS DefaultAppPool, IUSR, IIS_IUSRS
- Logged by Elastic Endpoint Process Monitor

```
f process.name cmd.exe
④ process.parent {
  "name": "php-cgi.exe",
  "pid": 3932,
  "entity_id": "NWU4NmFhMGUtM2E0Ny00Zjc1LT1lNWUtZjZmNzRjYzdkOTZlLTM5MzItMTMyNDkxNDkxNjcuNDAYNDMwMA==",
  "executable": "C:\\Program Files (x86)\\PHP\\v7.0\\php-cgi.exe"
}
f process.pe.original_file_name Cmd.Exe
# process.pid 4052
f user.domain IIS APPPOOL
f user.name DefaultAppPool
```

Discovery and Credential Access

Detecting Credential Spraying

- Event ID :- 4625
- Event Type :- Security

† event.action	logon-failed
† event.category	authentication
† event.code	4625
📅 event.created	Nov 6, 2020 @ 19:31:52.960
† event.kind	event
† event.module	security
† event.outcome	failure
† event.provider	Microsoft-Windows-Security-Auditing

Discovery and Credential Access

Kerbroasting

- Event ID :- 4769
- Ticket Encryption :- 0x17
- Event Type : Security

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	brynn.marita
Supplied Realm Name:	VICTIMCORP.ORG
User ID:	victimcorp/brynn.marita

Service Information:

Service Name:	krbtgt
Service ID:	victimcorp/krbtgt

Network Information:

Client Address:	10.0.2.15
Client Port:	41194

Additional Information:

Ticket Options:	0x50800000
Result Code:	0x0
Ticket Encryption Type:	0x17
Pre-Authentication Type:	0

Certificate Information:

Log Name: Security

Source: Microsoft Windows security

Event ID: 4769

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 11/6/2020 8:28:54 AM

Task Category: Kerberos Authentication Service

Keywords: Audit Success

Computer: WIN-NFUUDOUCTEA.victimcorp.org

Lateral Movement

Explicit Login

- Event ID :- 4648
- Event Type : Security

Subject:

Security ID:	victimcorp\brynn.marita
Account Name:	brynn.marita
Account Domain:	victimcorp
Logon ID:	0x5D6A0
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:

Account Name:	barry.alice
Account Domain:	
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Target Server:

Target Server Name:	WIN-NFUUDOUCTEA.victimcorp.org
Additional Information:	WIN-NFUUDOUCTEA.victimcorp.org

Process Information:

Process ID:	0x270
Process Name:	C:\Windows\System32\wsmpmhvhost.exe

Log Name: Security

Source: Microsoft Windows security

Event ID: 4648

Level: Information

User: N/A

OpCode: info

More Information: [Event Log Online Help](#)

Logged: 11/14/2020 1:01:32 AM

Task Category: Logon

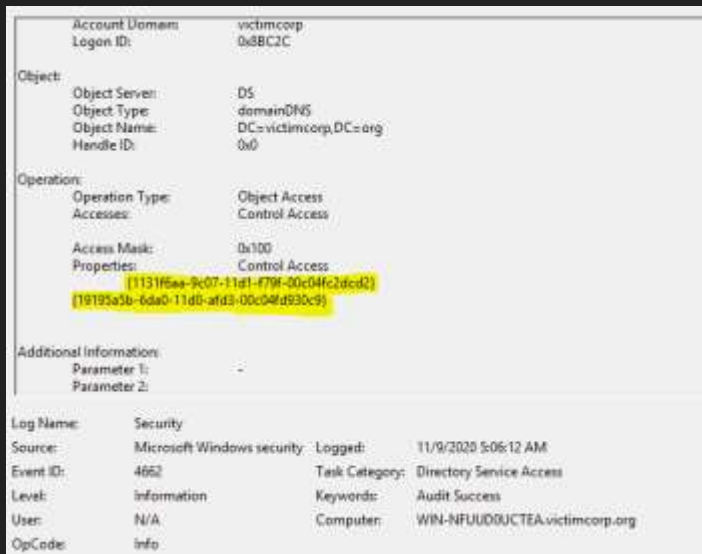
Keywords: Audit Success

Computer: WIN-NFUUDOUCTEA.victimcorp.org

Privilege Escalation

DCSync / DCReplication

- Event ID : 4662
- Event Type : Security
- Triggered By : Replication GUID ({1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} {19195a5b-6da0-11d0-afd3-00c04fd930c9})



The screenshot displays the details of a Windows Security event (ID 4662) related to DCSync. The event is categorized as 'Directory Service Access' and 'Audit Success'. It occurred on 11/9/2020 at 5:06:12 AM on the computer WIN-NFUUD0UCTEA.victimcorp.org, initiated by user N/A. The event details include the account domain (victimcorp), login ID (0x8BC2C), and the object being accessed (DC=victimcorp,DC=org). The operation type is 'Object Access' with 'Control Access' permissions. The access mask is 0x100, and the properties list the Replication GUIDs: {1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} and {19195a5b-6da0-11d0-afd3-00c04fd930c9}. The log name is 'Security' and the source is 'Microsoft Windows security'.

Account Domain	victimcorp
Login ID:	0x8BC2C
Object:	
Object Server:	DS
Object Type:	domainDNS
Object Name:	DC=victimcorp,DC=org
Handle ID:	0x0
Operation:	
Operation Type:	Object Access
Accesses:	Control Access
Access Mask:	0x100
Properties:	Control Access
	{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}
	{19195a5b-6da0-11d0-afd3-00c04fd930c9}
Additional Information:	
Parameter 1:	-
Parameter 2:	-
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4662
Level:	Information
User:	N/A
OpCode:	Info
Task Category:	Directory Service Access
Keywords:	Audit Success
Computer:	WIN-NFUUD0UCTEA.victimcorp.org
Logged:	11/9/2020 5:06:12 AM

Persistence

PSEXec as Administrator

- Event ID : 7045
- Event Type : Security



Defence Evasion

Log Clearance

- Event ID : 1102,104
- Event Type : Security
- Event Action Log Clear



Q&A

Join our discord channel: <https://dc0471.org/discord>

Thank You

Reach me

@RahulR_95

jamoski