Hybrid and Full Live Cyber Defence Exercise Scenarios

Table of Contents

Hybrid Exercise – 1

Initial Scenario: The attackers compromise the on-premise network using compromised credentials of an employee

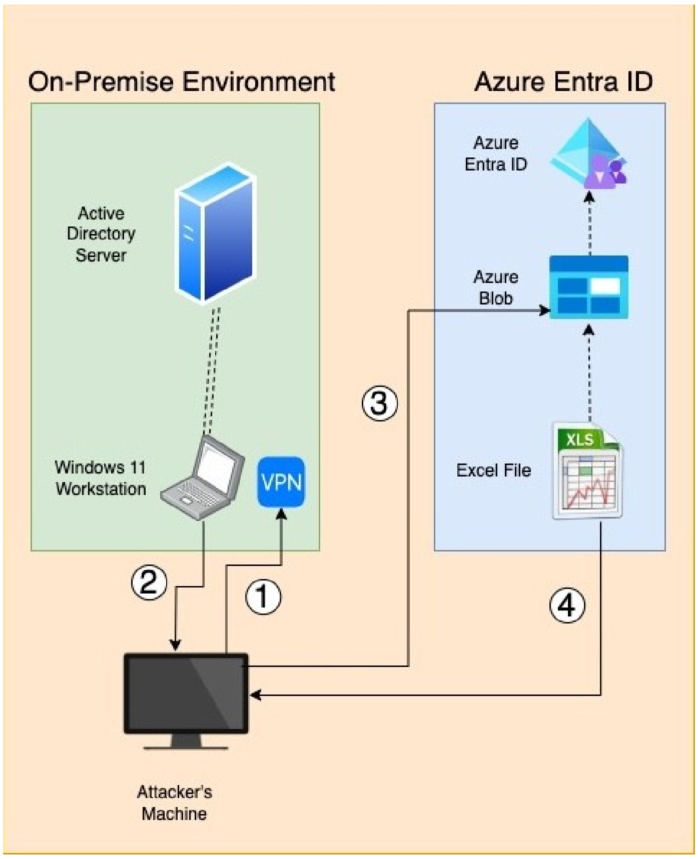
Red Team Objective: Exfiltrate an excel file containing employee personal information present in Azure Blobs

Blue Team Tools:

1. OpenEDR
2. Wazuh
3. Velociraptor
4. Zeek + Rita
5. Cyber Deception

Note: Workstation is Domain joined, but not Azure Entra ID joined.

Attack Scenario:



1. Adversary gets initial access via a compromised VPN credential into an employee's workstation
2. Escalation of privileges are done using two ways:

   1. Privilege escalation is done by dumping logged on credentials and persistence is established using Schedule Tasks running as the new user who is a domain administrator
   2. Password stored in Firefox is dumped, where Azure Entra ID credentials of this user is found

3. Adversary logs in to Azure Entra ID using these credentials. This user has an Azure built-in role of “Storage Blob Data Owner”.
4. Using this account, the excel file containing employee personal information is downloaded by the adversary

Reference:

1. https://www.inversecos.com/2022/01/how-to-detect-and-compromise-azure.html

Hybrid Exercise – 2

Initial Scenario: The attackers send out-of-band phishing emails to employees prompting them to enter Entra ID credentials

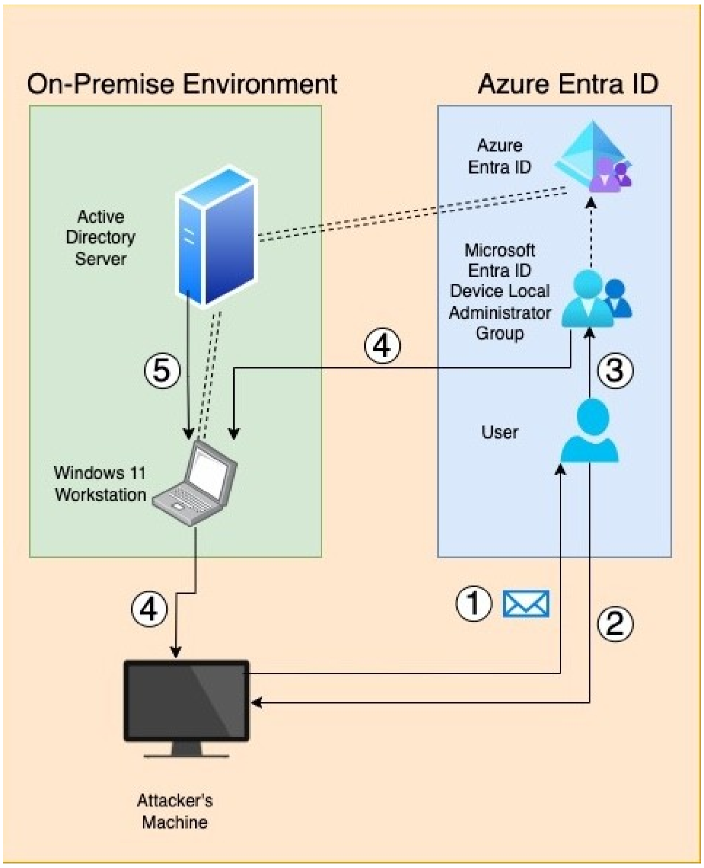
Red Team Objective: Create new Domain Administrator user

Blue Team Tools:

1. OpenEDR
2. Wazuh
3. Velociraptor
4. Zeek + Rita
5. Cyber Deception

Note: Workstation is Domain joined and Azure Entra ID joined.

Attack Scenario:



1. Adversary sends an out-of-band phishing email
2. The active session received belongs to a User Administrator role
3. By abusing dynamic group rules on “Microsoft Entra Joined Device Local Administrator”, a new user is created in this group

4. Using the new user, the adversary gets initial access into a machine on on-premise environment
5. Using LLMNR poisoning attack on the on-premise attack, the adversary impersonates Domain Administrator using the NTLM hash of this user, and a new Domain Administrator user is added to this Active Directory environment

Reference:

1. https://www.mnemonic.io/resources/blog/abusing-dynamic-groups-in-azure-ad-for-privilege-escalation/
2. https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d

Hybrid Exercise – 3

Initial Scenario: The attackers tricks user into inputting a user code into a Microsoft owned verification link.

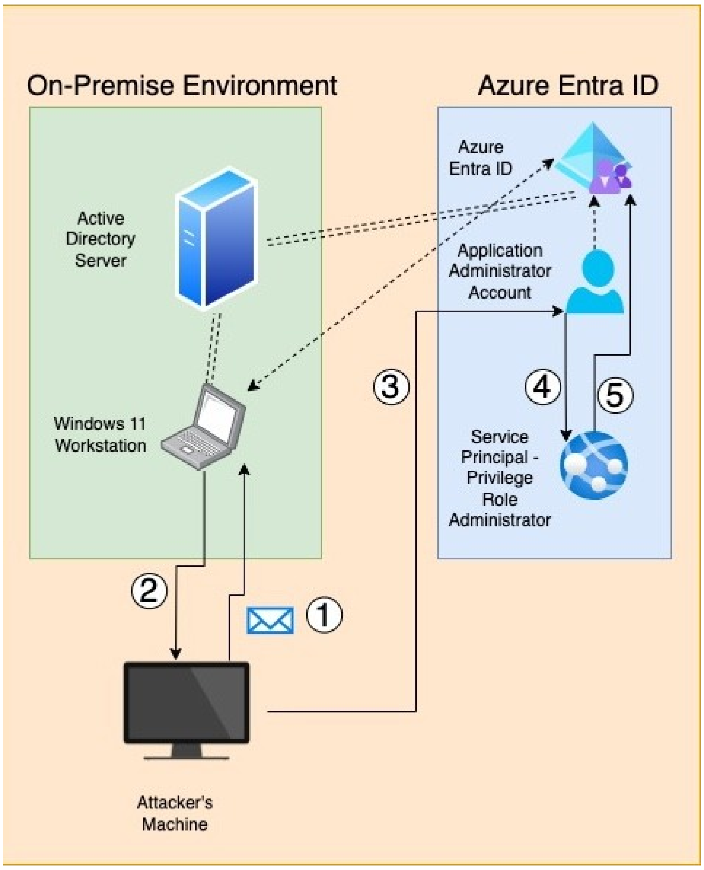
Red Team Objective: Add a Global Administrator user in Azure Entra ID

Blue Team Tools:

1. OpenEDR
2. Wazuh
3. Velociraptor
4. Zeek + Rita
5. Cyber Deception

Note: Workstation is Domain joined and Azure Entra ID joined.

Attack Scenario:



1. Adversary sends an OAuth Device Code Phishing email to an employee having Application Administrator account where the employee adds in the device code sent by the adversary and logs into their account
2. Adversary retrieves refresh and access tokens to access Azure Entra ID of the target organisation

3. Using the refresh and access token, adversary logins in using Graph API with Application Administrator role
4. As the Application Administrator account, the adversary changes the password of a service principal that has Privilege Role Administrator role
5. Using the service principal account, adversary gives the Application Administrator account, Global Administrator right

Reference:

1. https://www.inversecos.com/2022/12/how-to-detect-malicious-oauth-device.html
2. https://redfoxsec.com/blog/azure-privilege-escalation-via-service-principal/

Full Live Exercise

Initial Scenario: The attackers send phishing emails to employees prompting them to run a PowerShell Command impersonating HelpDesk

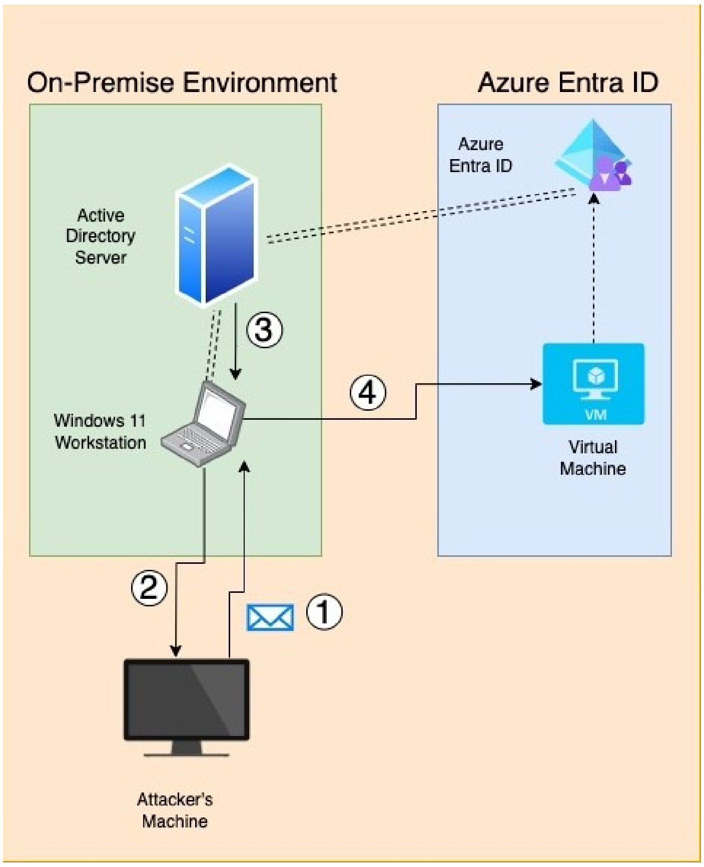
Red Team Objective: Run a script in a VM hosted on Azure Entra ID to simulate crypto mining

Blue Team Tools:

1. OpenEDR
2. Wazuh
3. Velociraptor
4. Zeek + Rita
5. Cyber Deception

Note: Workstation is Domain joined and Azure Entra ID joined.

Attack Scenario:



1. Adversary sends a phishing email prompting user to run a PowerShell command
2. Target user runs the command giving a beacon to the adversary
3. Using kerberoasting, the adversary impersonates a service account

4. Using this service account, the adversary is able to laterally move into a VM on Azure Entra ID and gets a shell access, where this user has owner rights and runs their own script in the background simulating a crypto mining activity

Reference:

1. https://github.com/LarryRuane/minesim