Lab Module 19 Cloud Computing

Lab 1: Perform Reconnaissance on Azure

As an ethical hacker, you need to know how to utilize PowerShell command-based scripting tools for conducting reconnaissance and gathering information. This information can then be used to assess the security posture of other systems within the network.

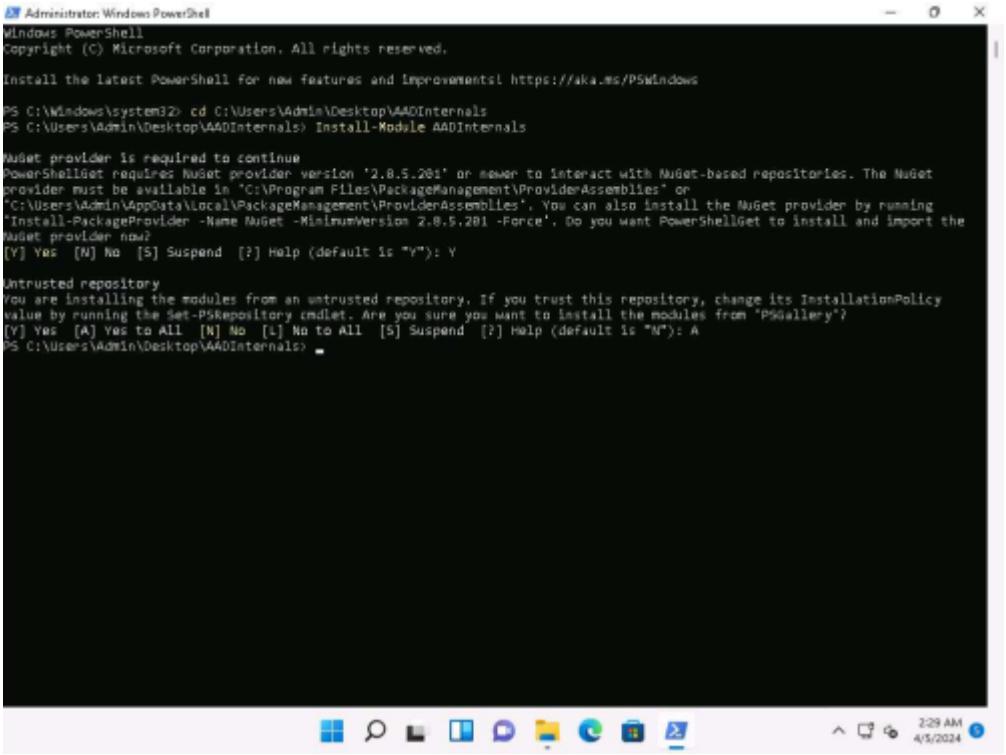
Reconnaissance tools serve as indispensable assets for attackers in cloud hacking, providing them with the essential information and insights needed to orchestrate successful attacks against cloud environments.

Task 1: Azure Reconnaissance with AADInternals

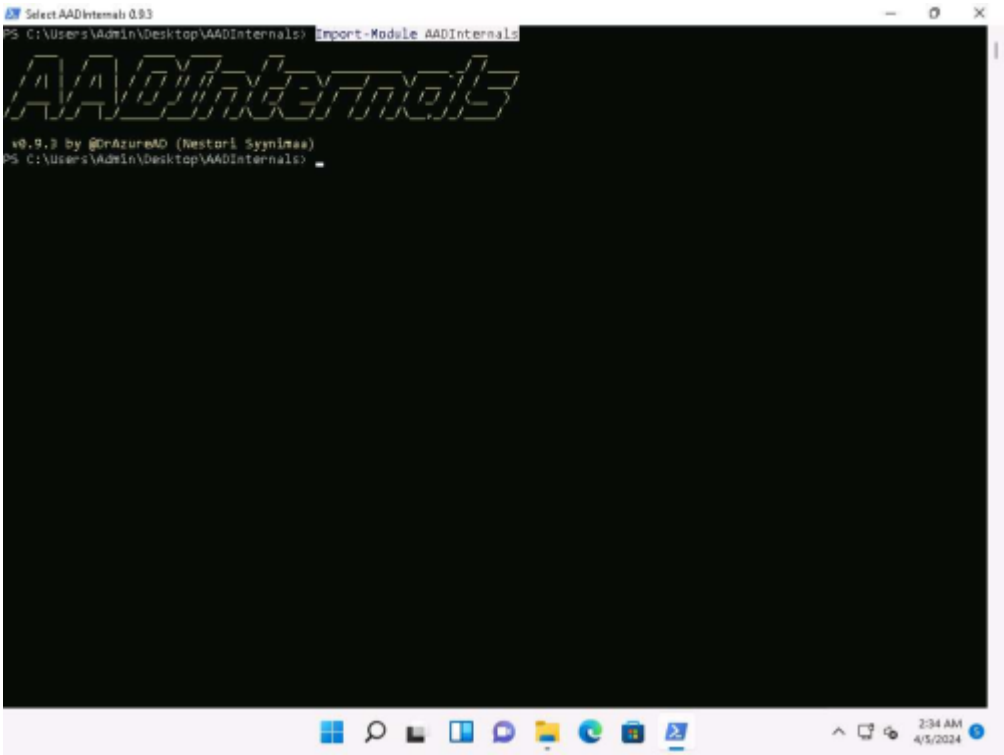
AADInternals is primarily focused on auditing and attacking Azure Active Directory (AAD) environments, it can still be utilized as part of a broader cloud reconnaissance effort. This tool has several features such as user enumeration, credential extraction, token extraction and manipulation, privilege escalation, etc.

In this lab we will perform Azure Active Directory reconnaissance as an outsider.

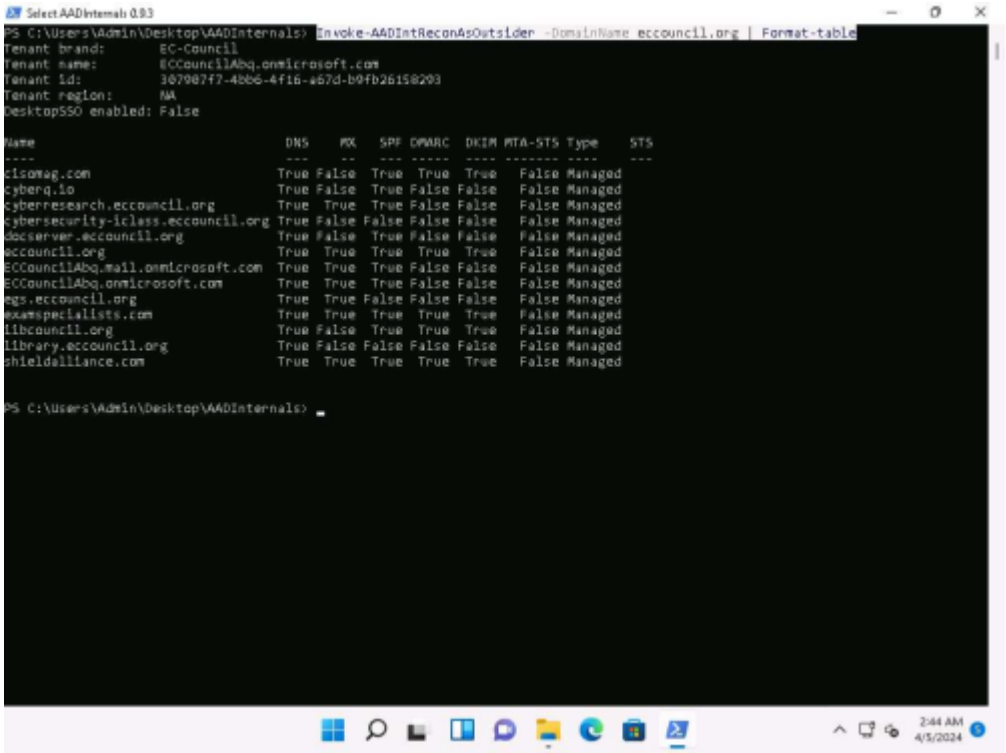
1. In the Windows search type powershell and under PowerShell click on Run as Administrator to open an administrator PowerShell window.
2. In the PowerShell window run Install-Module AADInternals command to install AADInternals module.



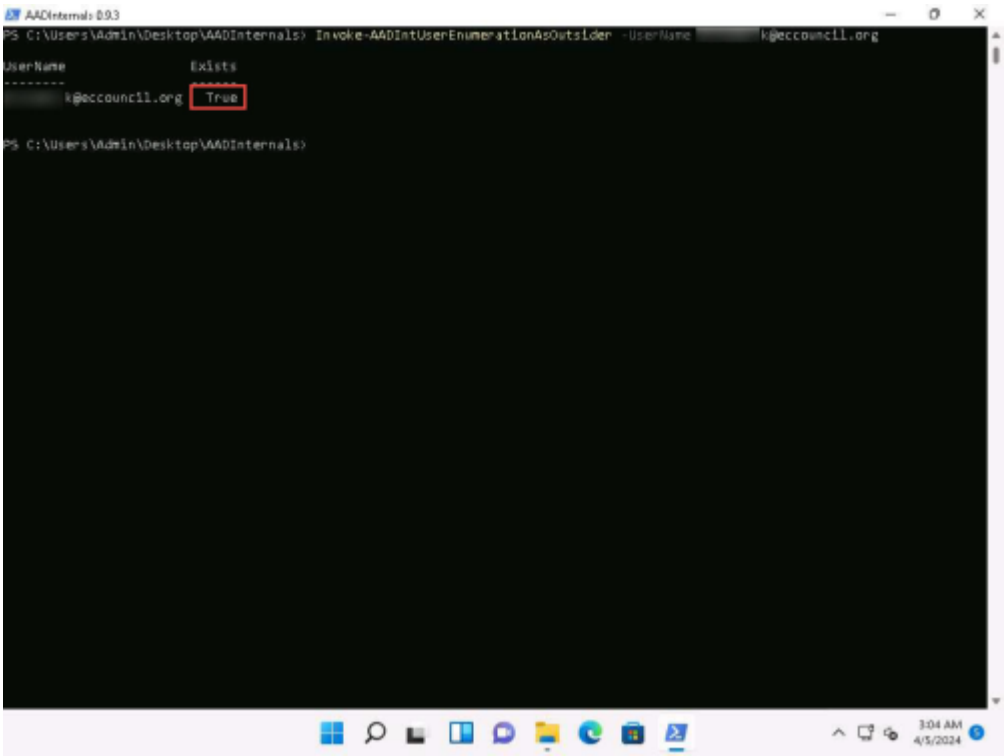
3. Now, run Import-Module AADInternals command, to import AADInternals module.



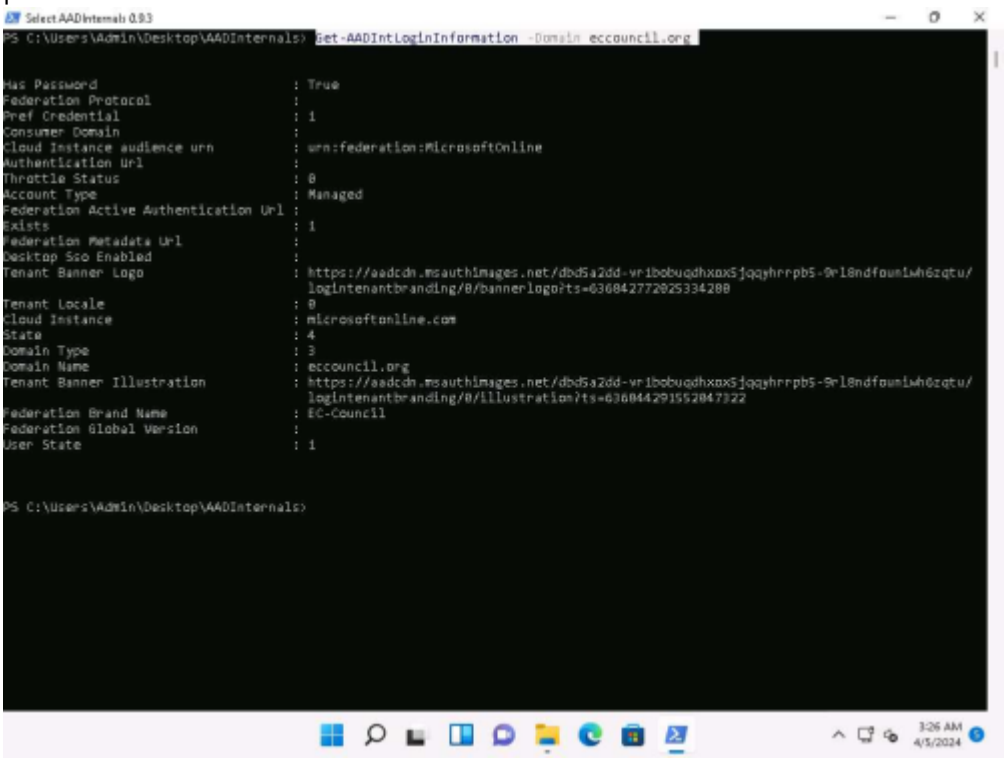
4. Now, we will gather the publicly available information of a target Azure AD such as Tenant brand, Tenant name, Tenant ID along with the names of the verified domains.
5. In the PowerShell window run Invoke-AADIntReconAsOutsider -DomainName company.com | Format-table command.
    1. In the above command replace the company.com with the target company's domain (here, we are using eccouncil.org).



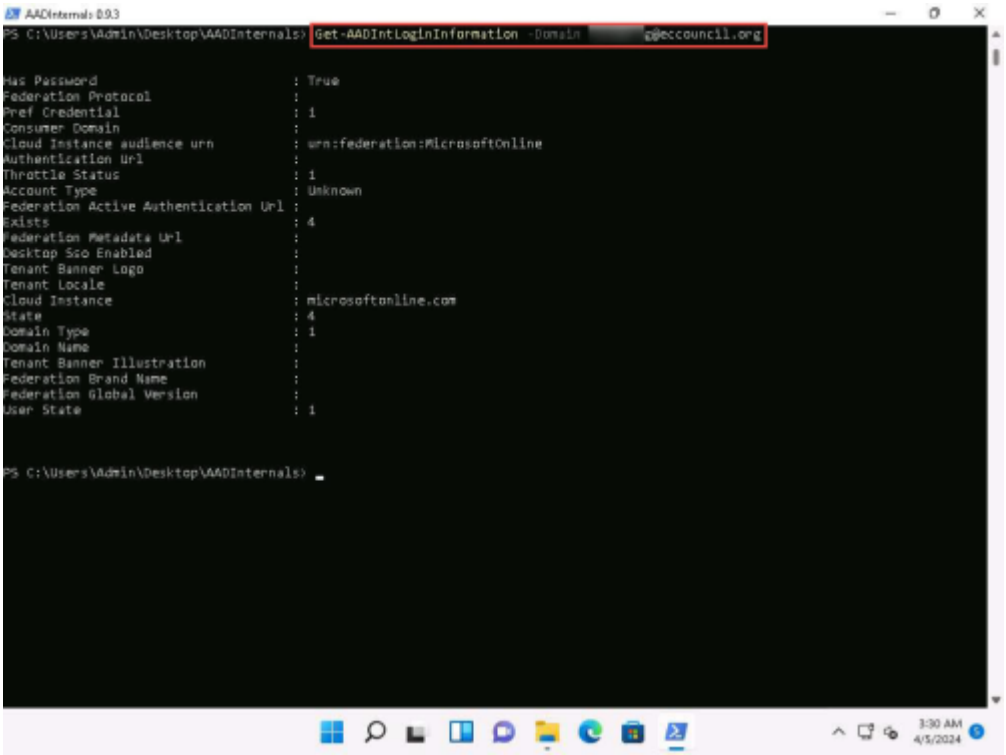
6. From the above screenshot we can gather information such as DNS, MX, SPF, DMARC, DKIM etc.
7. Now, we will perform user enumeration in Azure AD, in the PowerShell window type Invoke-AADIntUserEnumerationAsOutsider -UserName user@company.com and press Enter.



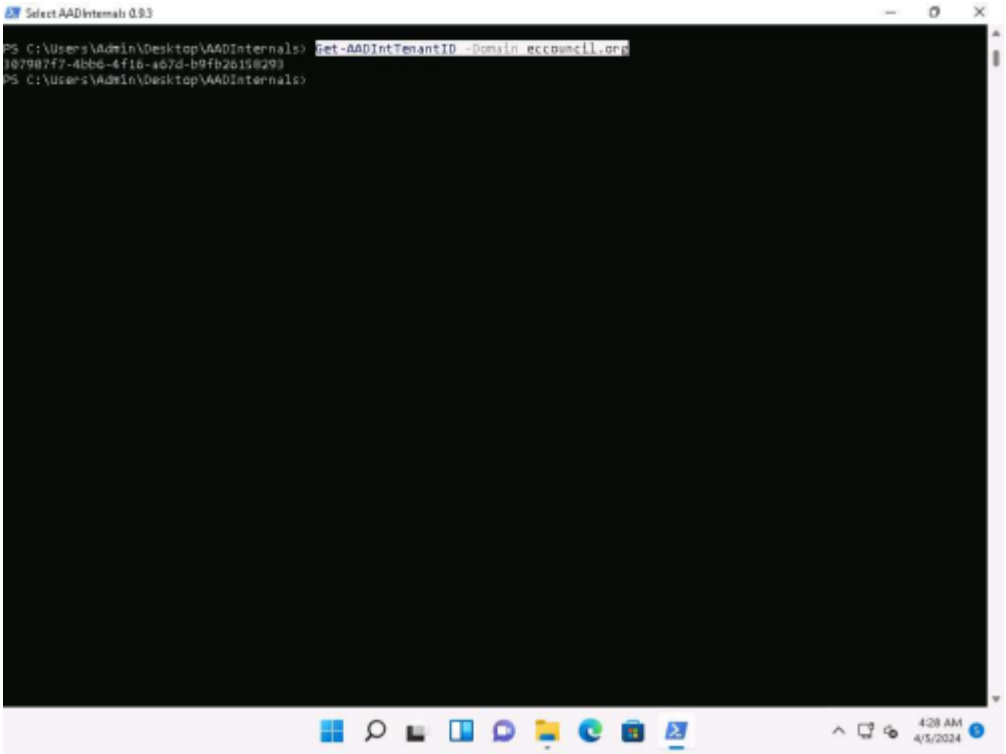
8. We can see that the result appears, True under Exists field which implies that the Azure account with the given username exists and the attacker can perform further attacks.
9. We can also perform the user enumeration by placing the usernames in a text file, by running Get-Content .\users.txt | Invoke-AADIntUserEnumerationAsOutsider -Method Normal. Where the users.txt file contains the target email addresses.
10. Now, to get login information for a domain type Get-AADIntLoginInformation -Domain company.com and press Enter.



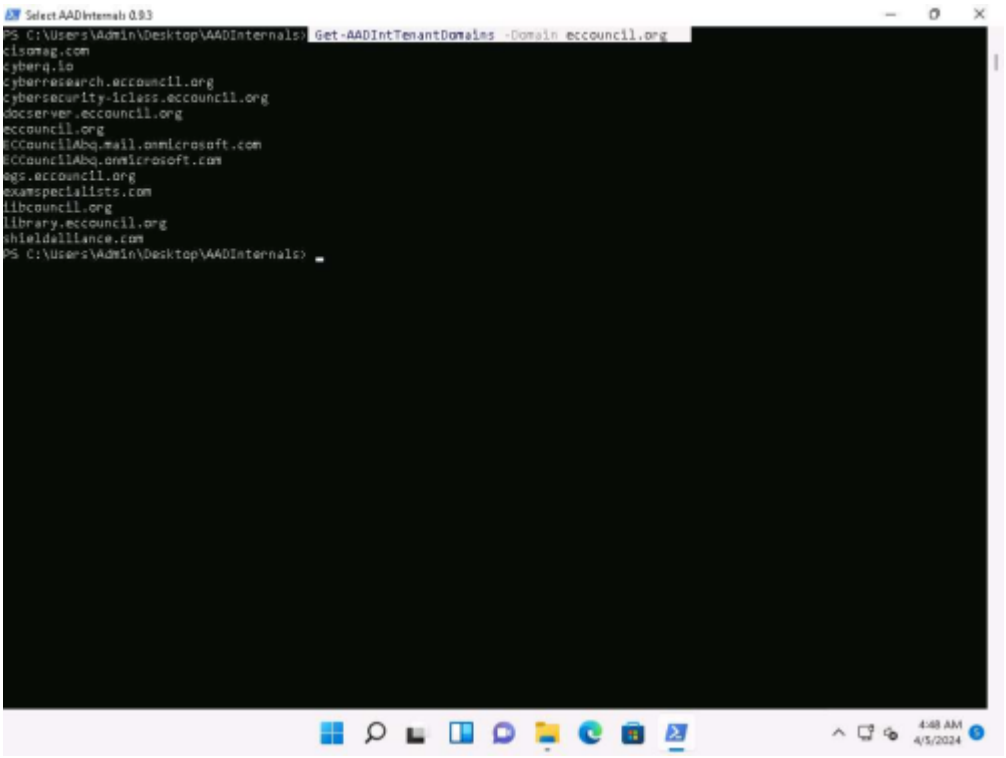
11. Now, to get login information for a user type Get-AADIntLoginInformation -Domain user@company and press Enter.



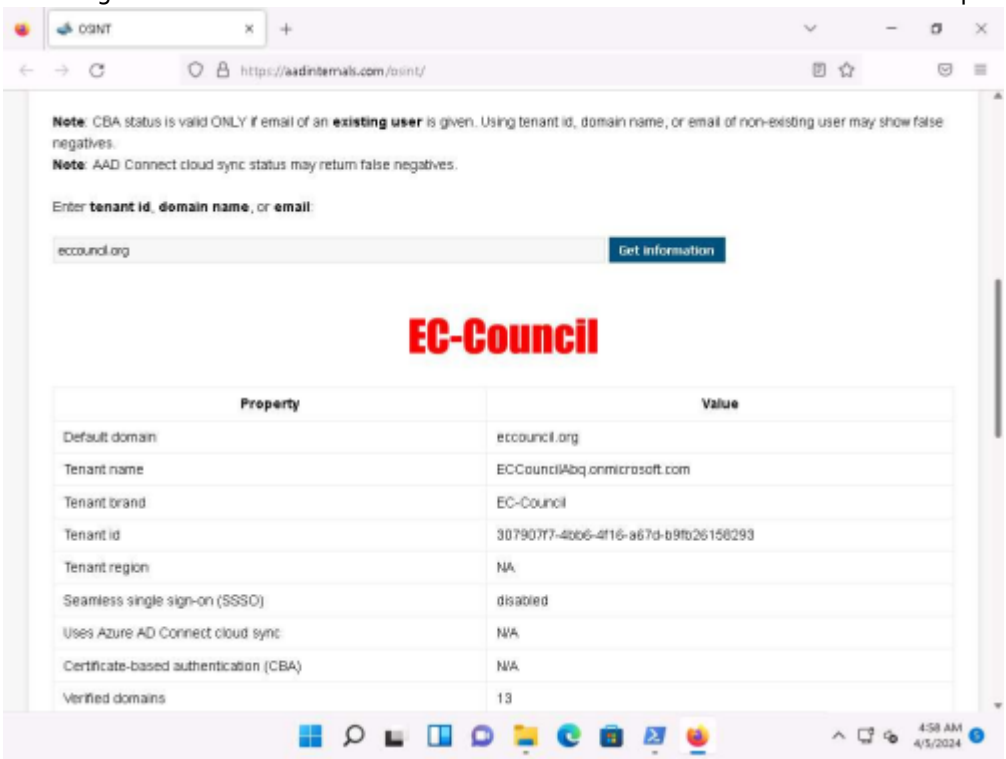
12. To get the tenant ID for the given user, domain, or Access Token, type Get-AADIntTenantID -Domain company.com.

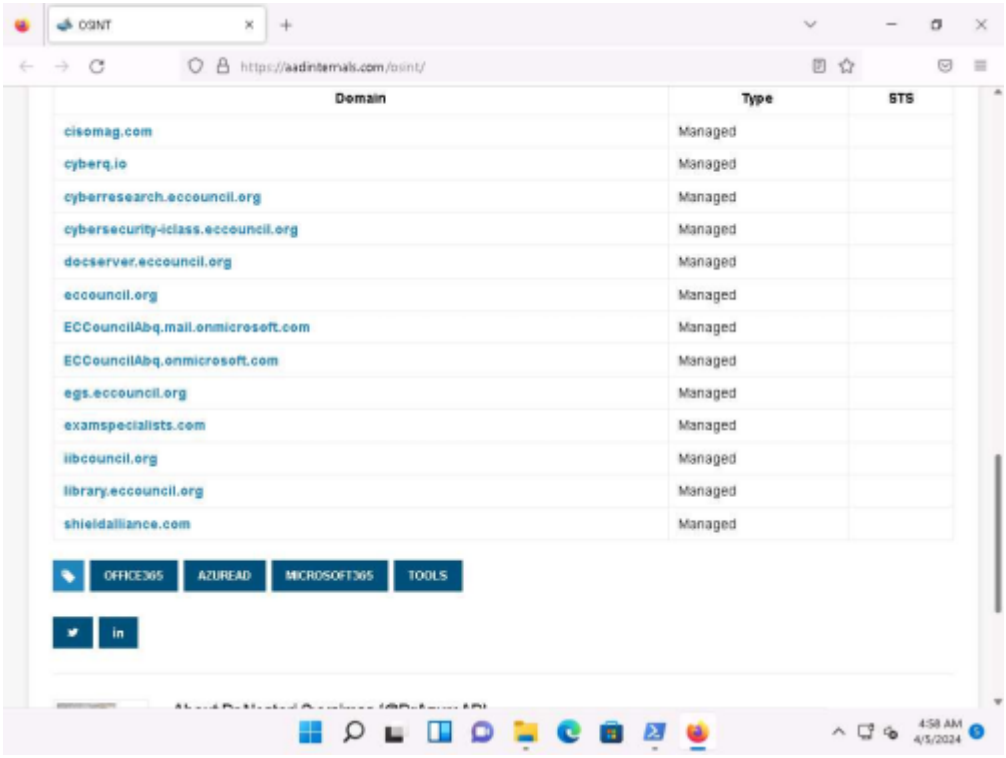


13. To get registered domains from the tenant of the given domain Get-AADIntTenantDomains -Domain company.com



14. We can see that all the domains associated with the tenant will be listed.
15. Alternatively you can visit https://aadinternals.com/osint/ site and type the tenant ID, domain name, or email to get the openly available information for the given tenant.
16. Launch Firefox browser and go to https://aadinternals.com/osint/ and type the domain name in the search box and click on Get information button.
17. We will get the Domain information and the list of domains connected with the provided domain name.





18. In similar way you can enter the tenant ID and email in the search field to view the information regarding the tenant and the user.

Lab 2: Exploit S3 Buckets

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- Inspecting HTML: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- Brute-Forcing URL: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- Finding subdomains: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- Reverse IP Search: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- Advanced Google hacking: Use advanced Google search operators such as "inurl" to search for URLs related to the target S3 buckets

Task 1: Exploit Open S3 Buckets using AWS CLI

Lab 3: Perform Privilege Escalation to Gain Higher Privileges

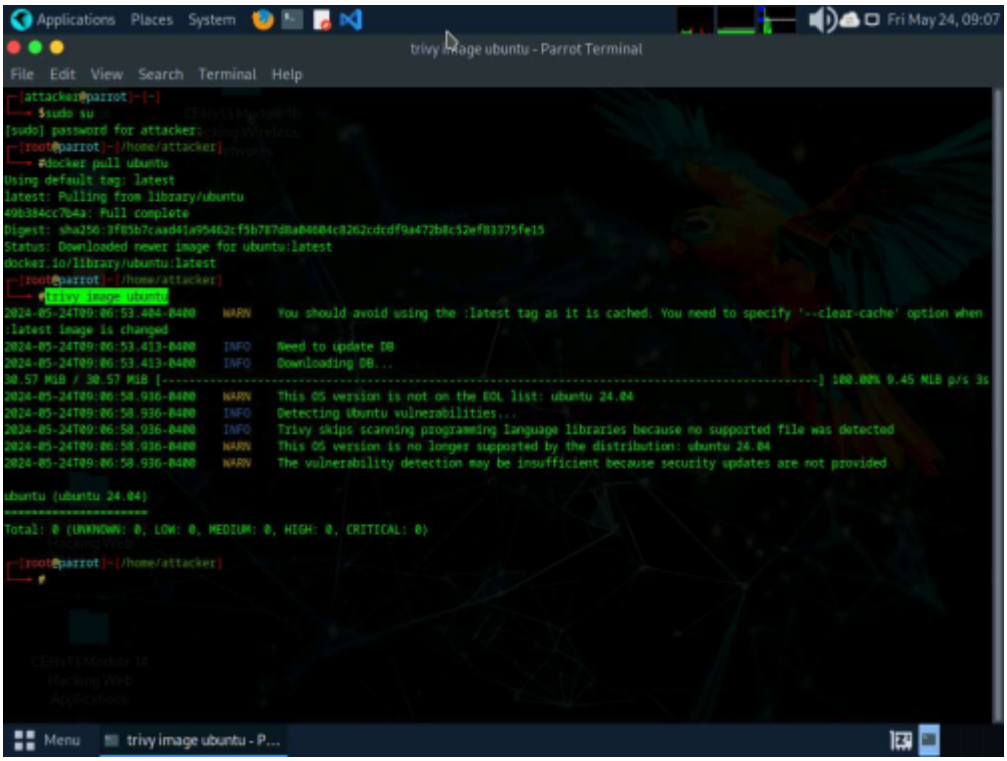
Task 1: Escalate IAM User Privileges by Exploiting Misconfigured User Policy

Lab 4: Perform Vulnerability Assessment on Docker Images

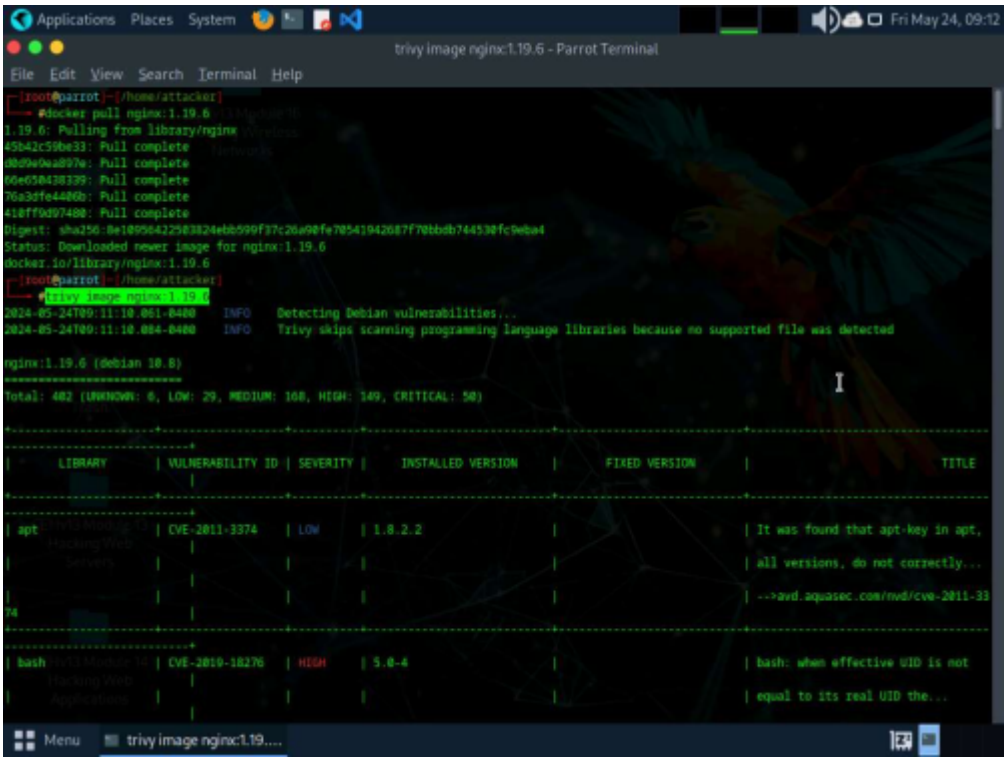
Task 1: Vulnerability Assessment on Docker Images using Trivy

Trivy is a powerful security scanner that detects vulnerabilities and misconfigurations across a wide range of targets, including container images, file systems, Git repositories, virtual machine images, Kubernetes, and AWS. With its comprehensive scanners, Trivy identifies OS package vulnerabilities, sensitive information, IaC issues, and more, providing a robust security solution for your infrastructure.

1. In the Parrot Security machine, click the MATE Terminal icon in the menu to launch the terminal.
2. A Parrot Terminal window appears. In the terminal window, type sudo su and press Enter to run the programs as a root user.
3. In this lab we will be scanning two docker images, first the secure one and second the vulnerable one.
4. Execute command **docker pull ubuntu** to install the first docker image.
5. Once the image is pulled we will be performing vulnerability assessment. Execute command **trivy image ubuntu**.



6. In the above screenshot, we can observe that we have total 0 vulnerability and it's completely secure.
7. Now, we will analyse the vulnerbale image. execute command **docker pull nginx:1.19.6** to pull the vulnerable image.
8. Execute command **trivy image nginx:1.19.6** to scan the image.



9. In the above screenshot we can see that we have total 401 vulnerabilities which is categorized as well along with CVEs mentioned.