

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.

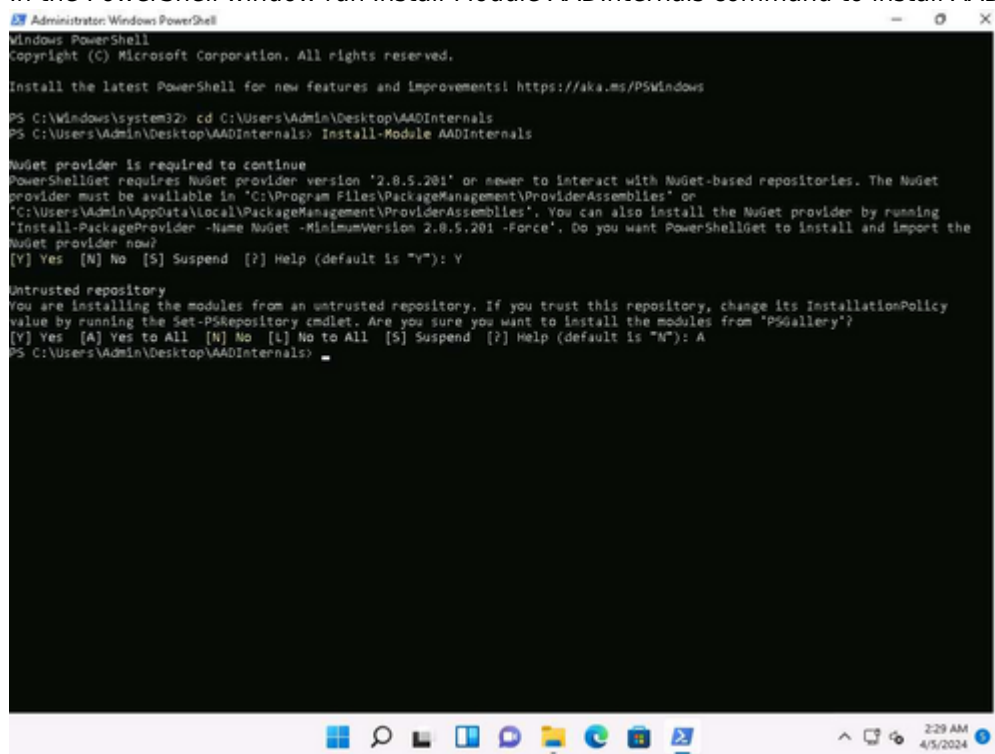
Reconnaissance tools serve as indispensable assets for attackers in cloud hacking, providing them with the essential information and insights needed to orchestrate successful attacks against cloud environments.

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.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

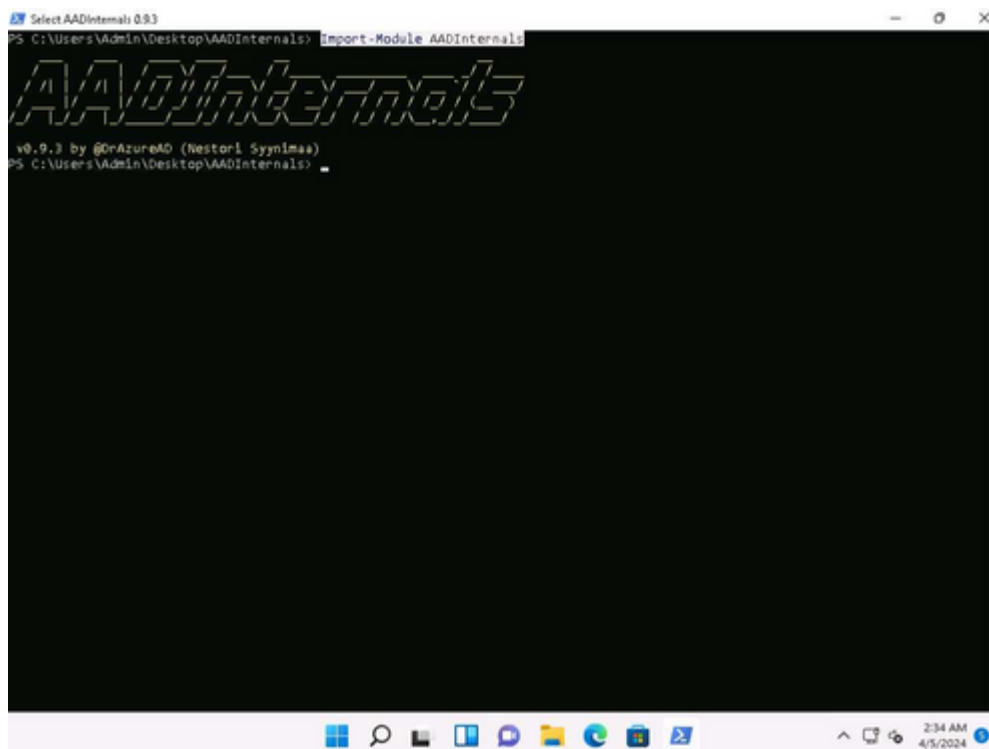
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> cd C:\Users\Admin\Desktop\AADInternals
PS C:\Users\Admin\Desktop\AADInternals> Install-Module AADInternals

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.0.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Admin\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.0.5.201 -Force'. Do you want PowerShellGet to install and import the
NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its InstallationPolicy
value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from "PSGallery"?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): A
PS C:\Users\Admin\Desktop\AADInternals>
```

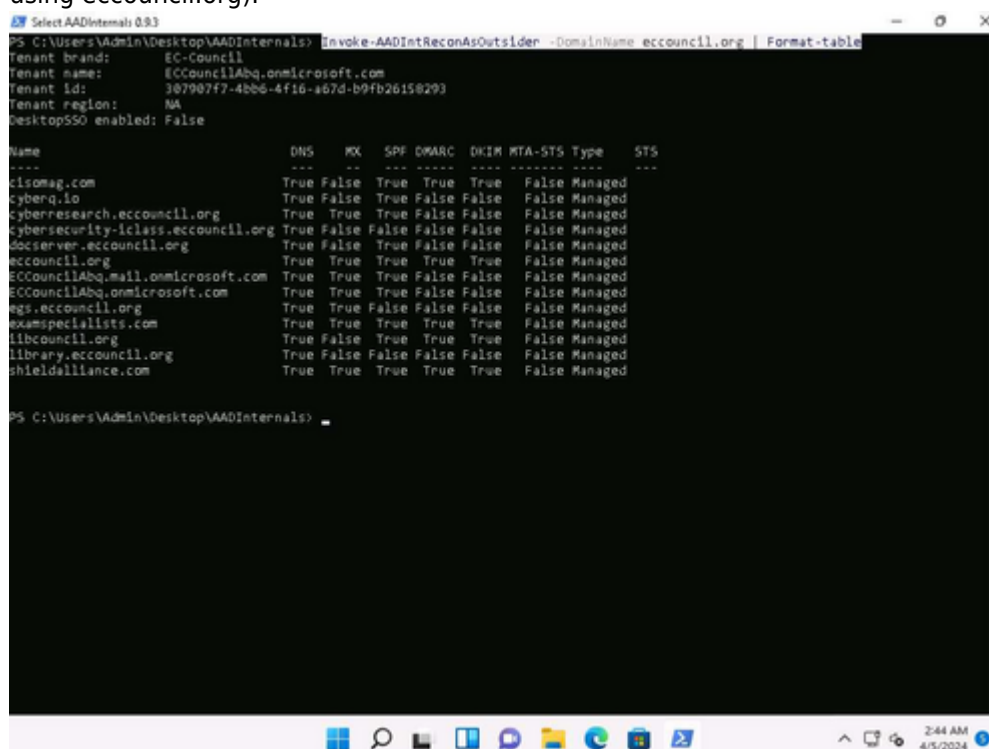
3. Now, run Import-Module AADInternals command, to import AADInternals module.



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.

```

AADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Invoke-AADIntUserEnumerationAsOutsider -UserName k@eccouncil.org

UserName      Exists
-----
k@eccouncil.org True

PS C:\Users\Admin\Desktop\AADInternals>

```

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.

```

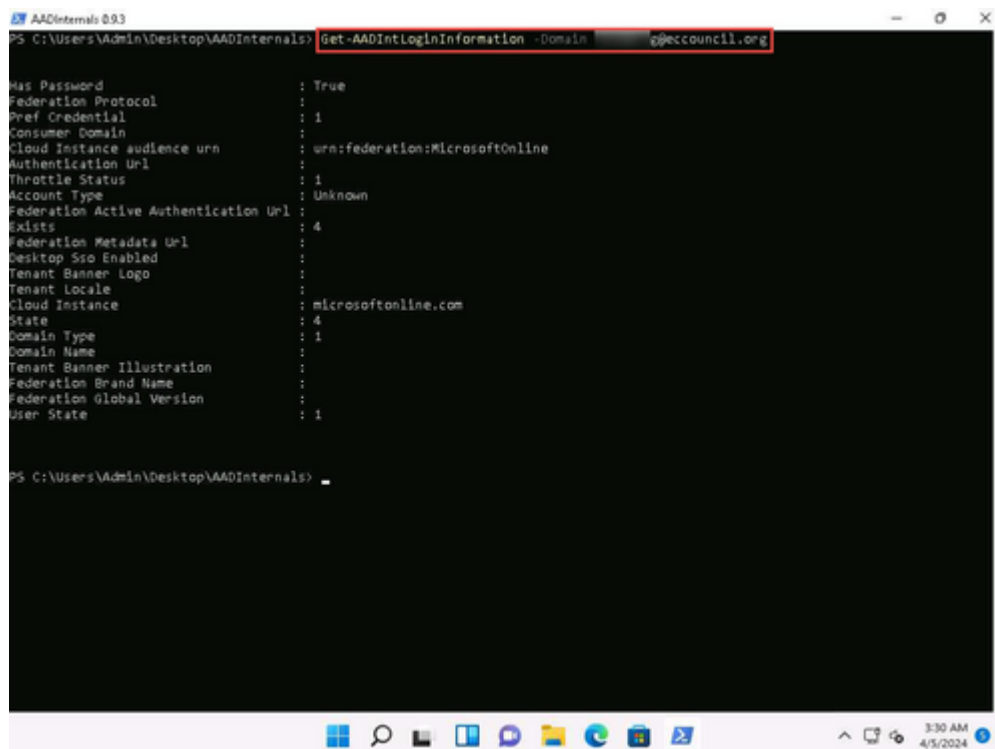
Select AADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntLoginInformation -Domain eccouncil.org

Has Password           : True
Federation Protocol    : 
Pref Credential        : 1
Consumer Domain       : 
Cloud Instance audience urn : urn:federation:MicrosoftOnline
Authentication Url     : 
Throttle Status       : 0
Account Type          : Managed
Federation Active Authentication Url : 
Exists                : 1
Federation Metadata Url : 
Desktop Sso Enabled   : 
Tenant Banner Logo    : https://aadcdn.msauthimages.net/dbd5a2dd-vr1b0buqdhxox5jqyhrpb5-9e18ndfounlwh6zqtu/logintenantbranding/0/bannerlogo/ts=636842772025334280
Tenant Locale         : 0
Cloud Instance        : microsoftonline.com
State                 : 4
Domain Type           : 3
Domain Name           : eccouncil.org
Tenant Banner Illustration : https://aadcdn.msauthimages.net/dbd5a2dd-vr1b0buqdhxox5jqyhrpb5-9e18ndfounlwh6zqtu/logintenantbranding/0/illustration/ts=636844291552047322
Federation Brand Name : EC-Council
Federation Global Version : 
User State            : 1

PS C:\Users\Admin\Desktop\AADInternals>

```

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

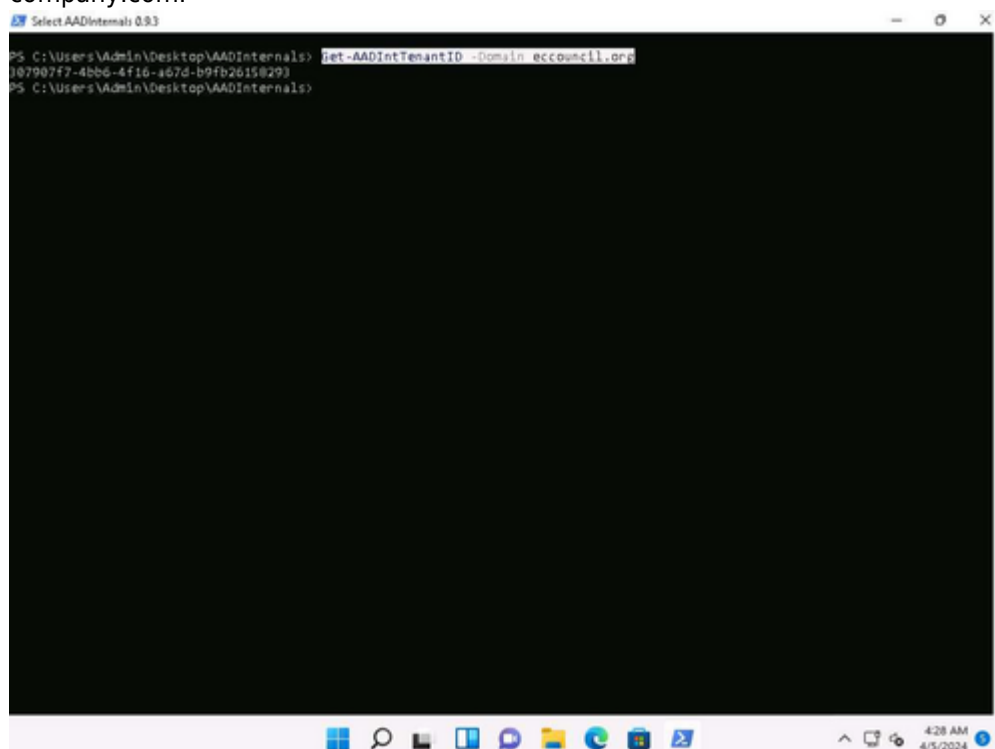


```
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntLoginInformation -Domain eccouncil.org

Has Password           : True
Federation Protocol    : 
Pref Credential        : 1
Consumer Domain       : 
Cloud Instance audience urn : urn:federation:MicrosoftOnline
Authentication Url     : 
Throttle Status       : 1
Account Type          : Unknown
Federation Active Authentication Url : 
Exists                : 4
Federation Metadata Url : 
Desktop Sso Enabled   : 
Tenant Banner Logo    : 
Tenant Locale         : 
Cloud Instance        : microsoftonline.com
State                 : 4
Domain Type           : 1
Domain Name           : 
Tenant Banner Illustration : 
Federation Brand Name  : 
Federation Global Version : 
User State            : 1

PS C:\Users\Admin\Desktop\AADInternals>
```

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



```
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntTenantID -Domain eccouncil.org
187907f7-4bb6-4f16-a67d-b9fb26150293

PS C:\Users\Admin\Desktop\AADInternals>
```

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

```

Select AADInternals 0.9.3
PS C:\Users\Admin\Desktop\AADInternals> Get-AADIntTenantDomains -Domain eccouncil.org
cismag.com
cyberg.io
cyberresearch.eccouncil.org
cybersecurity-iclass.eccouncil.org
docserver.eccouncil.org
eccouncil.org
ECCouncilAbq.mail.onmicrosoft.com
ECCouncilAbq.onmicrosoft.com
egs.eccouncil.org
examspecialists.com
ilbcouncil.org
library.eccouncil.org
nhieldalliance.com
PS C:\Users\Admin\Desktop\AADInternals>

```

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.

Note: CBA status is valid ONLY if email of an **existing user** is given. Using tenant id, domain name, or email of non-existing user may show false negatives.

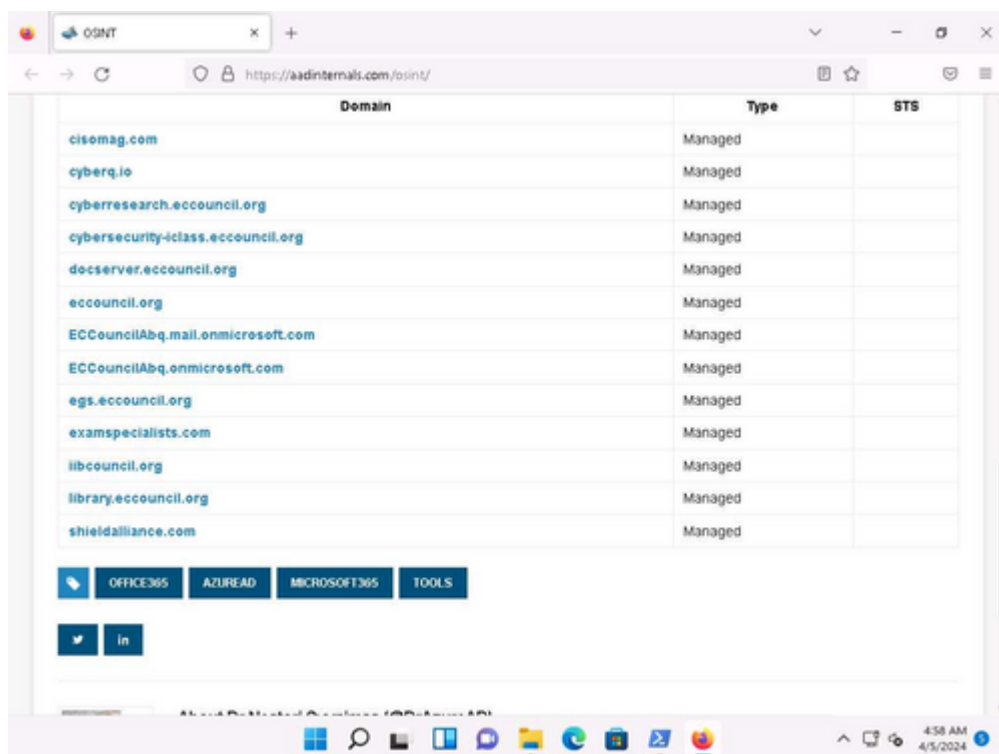
Note: AAD Connect cloud sync status may return false negatives.

Enter **tenant id, domain name, or email**

Get information

EC-Council

Property	Value
Default domain	eccouncil.org
Tenant name	ECCouncilAbq.onmicrosoft.com
Tenant brand	EC-Council
Tenant id	307907f7-4bb6-4f16-a67d-b9fb26158293
Tenant region	NA
Seamless single sign-on (SSSO)	disabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
Verified domains	13



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**.

```

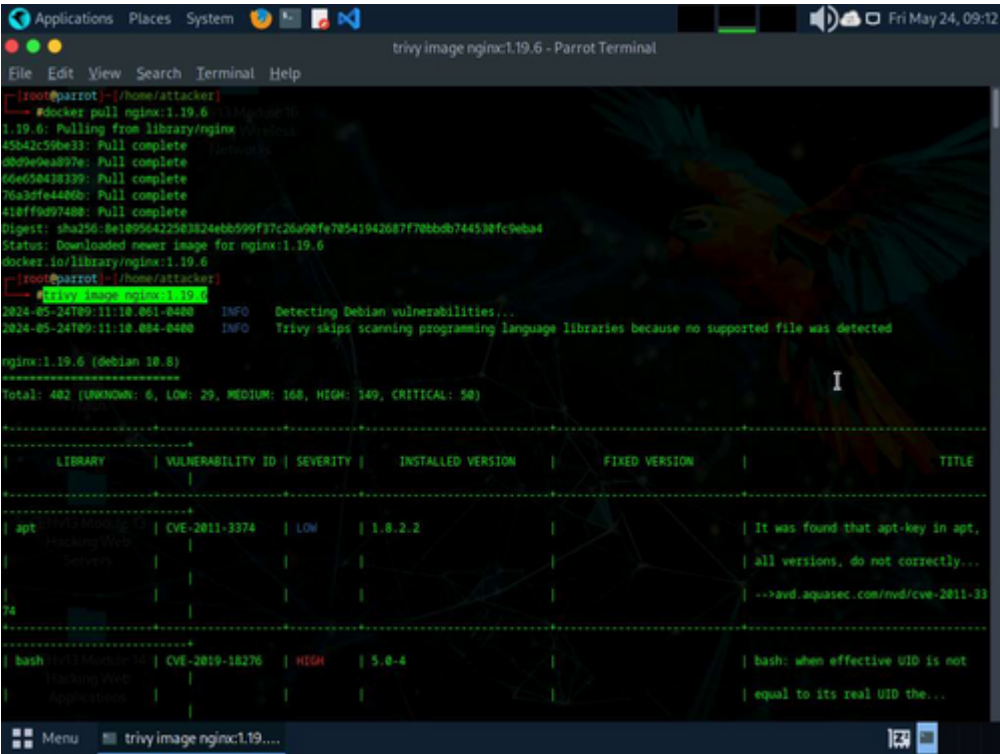
[attacker@parrot:~]$ sudo su
[sudo] password for attacker: 
[root@parrot:~/#] # docker pull ubuntu
Using default tag: latest
latest: Pulling from library/ubuntu
49b384cc7b4a: Pull complete
Digest: sha256:3f85b7caad41a95462cf5b787d8a04604c8262cdcf9a472b8c52ef83375fe15
Status: Downloaded newer image for ubuntu:latest
docker.io/library/ubuntu:latest
[root@parrot:~/#] # trivy image ubuntu
2024-05-24T09:06:53.484-0400 WARN You should avoid using the :latest tag as it is cached. You need to specify '--clear-cache' option when
latest image is changed
2024-05-24T09:06:53.413-0400 INFO Need to update DB
2024-05-24T09:06:53.413-0400 INFO Downloading DB...
[-----] 100.00% 9.45 MiB p/s 3s
2024-05-24T09:06:58.936-0400 WARN This OS version is not on the EOL list: ubuntu 24.04
2024-05-24T09:06:58.936-0400 INFO Detecting ubuntu vulnerabilities...
2024-05-24T09:06:58.936-0400 INFO Trivy skips scanning programming language libraries because no supported file was detected
2024-05-24T09:06:58.936-0400 WARN This OS version is no longer supported by the distribution: ubuntu 24.04
2024-05-24T09:06:58.936-0400 WARN The vulnerability detection may be insufficient because security updates are not provided

ubuntu (ubuntu 24.04)
=====
Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)

[root@parrot:~/#] #

```

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 vulnerable 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.

From:
<https://matebcn.eu/> - miguel angel torres egea

Permanent link:
<https://matebcn.eu/info:ursos:pue:ethical-hacker:sesion5:lab19>

Last update: 21/02/2025 12:40

