Breaching Active Directory — TryHackMe Writeup

A

Andrew · Follow

6 min read · Jan 4, 2024

Listen Share More

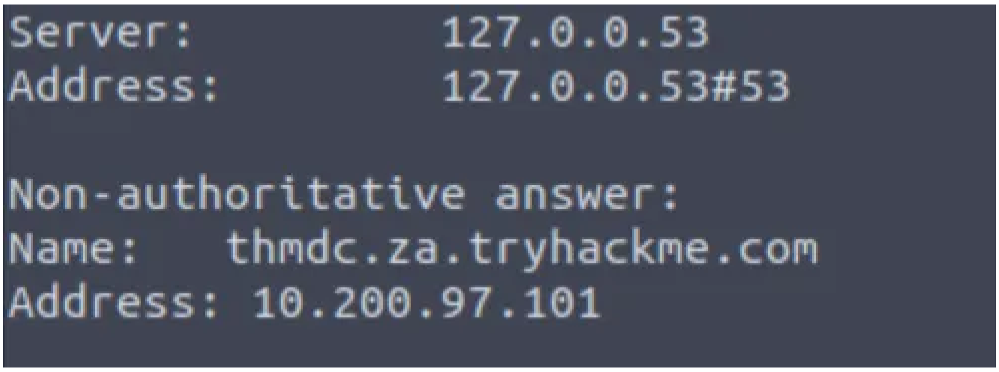
Prerequisites: TryHackMe | Active Directory Basics

This room discusses several different methods of acquiring the initial set of Active Directory Credentials needed for further exploitation and lateral movement. Since there can be a lot of different services on AD the attack surface is usually significant.

Lets get started:

Task 1:

The first step in this room is to set up DNS. You will have to use the diagram at the top of the page to set your DNS server to the "THMDC" IP address. You will have to either use the AttackBox or connect to their "breachingad" network with OpenVPN. After you configure DNS to point to the Domain Controller IP address (found at the top of the page) you can test it by running this Command: nslookup thmdc.za.tryhackme.com. This should return the IP of the domain controller. If you configured it wrong it will give a "server can't find" error. This is what the correct output should look like:



```
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   thmdc.za.tryhackme.com
Address: 10.200.97.101
```

Task 2:

OSINT and Phishing are popular methods for getting those first set of AD credentials. GitHub or Stack Overflow are places where passwords can end up accidentally exposed in plain text. Data breaches are another common source. You can check for data breaches involving your credentials with sites like HaveIBeenPwned and DeHashed.

What popular website can be used to verify if your email address or password has ever been exposed in a publicly disclosed data breach?

Answer: haveibeenpwned

Task 3:

New Technology LAN Manager (NTLM) is one of the security protocols used in active directory for user authentication. It is used with a challenge-response based scheme called NetNTLM. This is also called NTLM Authentication or Windows Authentication.

Exposed services are a good location to try to get valid credentials. You will be running a python script to password spray into an exposed service. To try to lower the chances of account lockout this task has us use one password and try to brute force usernames with that password. The script monitors the HTTP replies for a 200 code to determine if it is a valid login. If it is not a valid login it will get a 401 and output “Failed Login with Username: ” and the username that was tried.

What is the name of the challenge-response authentication mechanism that uses NTLM?

Stated at the top : “TLM can be used for authentication by using a challenge-response-based scheme called NetNTLM. This authentication mechanism is heavily used by the services on a network. However, services that use NetNTLM can also be exposed to the internet.”

Answer: NetNTLM

What is the username of the third valid credential pair found by the password spraying script?

4 total valid credential pairs output from the python script, read the 3rd one down.

Answer: gordon.stevens

How many valid credentials pairs were found by the password spraying script?

Stated earlier, output from terminal shows how many valid credentials were found.

Answer: 4

What is the message displayed by the web application when authenticating with a valid credential pair?

Open a web browser and go to http://ntlmauth.za.tryhackme.com and sign in with one of the credentials we found.

Answer: Hello World

Task 4:

LDAP is another method for Active Directory to authenticate with. LDAP is different from NTLM because the application directly verifies users' credentials. The following steps take place during LDAP authentication:

1. The user sends its credentials to the application which forwards it to the Domain Controller which then gives a bind response.
2. The application requests a LDAP user search which the DC replies to.
3. Finally, the Application sends an LDAP Bind request with the credentials and then is responded to with the Server Bind response which then completes the authentication.

One of the attacks against LDAP is called a pass-back attack. This is common against devices like printers, and is performed after initial access to the internal network has been gained. LDAP pass back is performed when an attacker has access to a devices configuration where LDAP parameters are specified. The attacker can then modify the configuration to specify the LDAP Server's IP has their IP. Then the authentication attempt will send credentials to the attacker.

In the task we have to set up an LDAP server of our own to receive the credentials. We also downgraded the security configurations to pass the credentials in plaintext. When we press "Test settings" it passes the plaintext password to us.

What type of attack can be performed against LDAP Authentication systems not commonly found against Windows Authentication systems?

Answer: LDAP Pass-back attack

What two authentication mechanisms do we allow on our rogue LDAP server to downgrade the authentication and make it clear text?

Answer: LOGIN,PLAIN

What is the password associated with the svcLDAP account?

Answer: tryhackmeldappass1@

Task 5:

Server Message block protocol allows clients to communicate with servers. In Active directory this is very important and used for many things such as file sharing or remote administration. Server message block uses NetNTLM authentication, and so in this task we will be looking at how to attack this protocol. We can use a program called Responder. This allows us to preform a man in the middle attack on SMB: We can intercept the NetNTLM challenge and get the password hash. We can then attempt to crack the hash with a program called hashcat.

Another form of attack on SMB is to relay the challenge. This is harder for many reasons. First you need certain permissions on the account you're using. Second, SMB signing also has to be disabled or not enforced for SMB relay attacks, since we couldn't forge the digital signature. Finally, you have to do a lot of guessing as there is probably many different accounts and since we haven't breached AD yet and done enumeration so we would just have to guess.

What is the name of the tool we can use to poison and capture authentication requests on the network?

Answer: responder

What is the username associated with the challenge that was captured?

Answer: svcFileCopy

What is the value of the cracked password associated with the challenge that was captured?

Answer: FPassword1!

Task 6:

This task goes over Microsoft Deployment toolkit and how it can be used to breach Active Directory. Microsoft deployment toolkit is a service that helps automate the deploying of Microsoft operating systems on a large scale. Another service is SCCM, which stands for Microsoft System Center Configuration Manager. This is often used along with MDT and allows for patch management and updates to software across the organization. For this task we will be focusing on a configuration of MDT called Preboot Execution Environment (PXE) boot.

PXE boot allows new devices to install an OS over the network directly. DHCP will grant the host an IP lease, and then the host is allowed to request the PXE boot image and start the installation. Here is how this process can be exploited: injection of a privilege escalation vector to gain admin access to the OS once the PXE boot has finished, and performing password scraping attacks to recover Active Directory credentials used during the install. This room skips the DHCP step, and goes directly to receiving the boot configuration files.

What Microsoft tool is used to create and host PXE Boot images in organizations?

Answer: Microsoft deployment toolkit

What network protocol is used for recovery of files from the MDT server?

tftp

What is the username associated with the account that was stored in the PXE Boot image?

Answer: svcMDT

What is the password associated with the account that was stored in the PXE Boot image?

Answer: PXEBootSecure1@

Task 7:

This last task goes over configuration files. They are another avenue to recovering Active Directory credentials, but require access to an organizations network initially. Examples of config files that would be useful for enumeration could be: Web app config files, service config files, registry keys, or centrally deployed applications. There are different scripts that can be used to help automate this process. Seatbelt is an example of one. In this room you use a python script.

What type of files often contain stored credentials on hosts?

Answer: Configuration files

What is the name of the McAfee database that stores configuration including credentials used to connect to the orchestrator?

Answer: ma.db

What table in this database stores the credentials of the orchestartor?

Answer: AGENT_REPOSITORIES

What is the username of the AD account associated with the McAfee service?

Answer: svcAV

What is the password of the AD account associated with the McAfee service?

MyStrongPassword!

Conclusion:

There are many different steps organizations can take to prevent these breaches:

- User awareness and training
- Limiting AD service exposure online
- Enforce network access control
- Enforce SMB Signing

Open in app ↗

Medium

Search

Follow

Written by Andrew

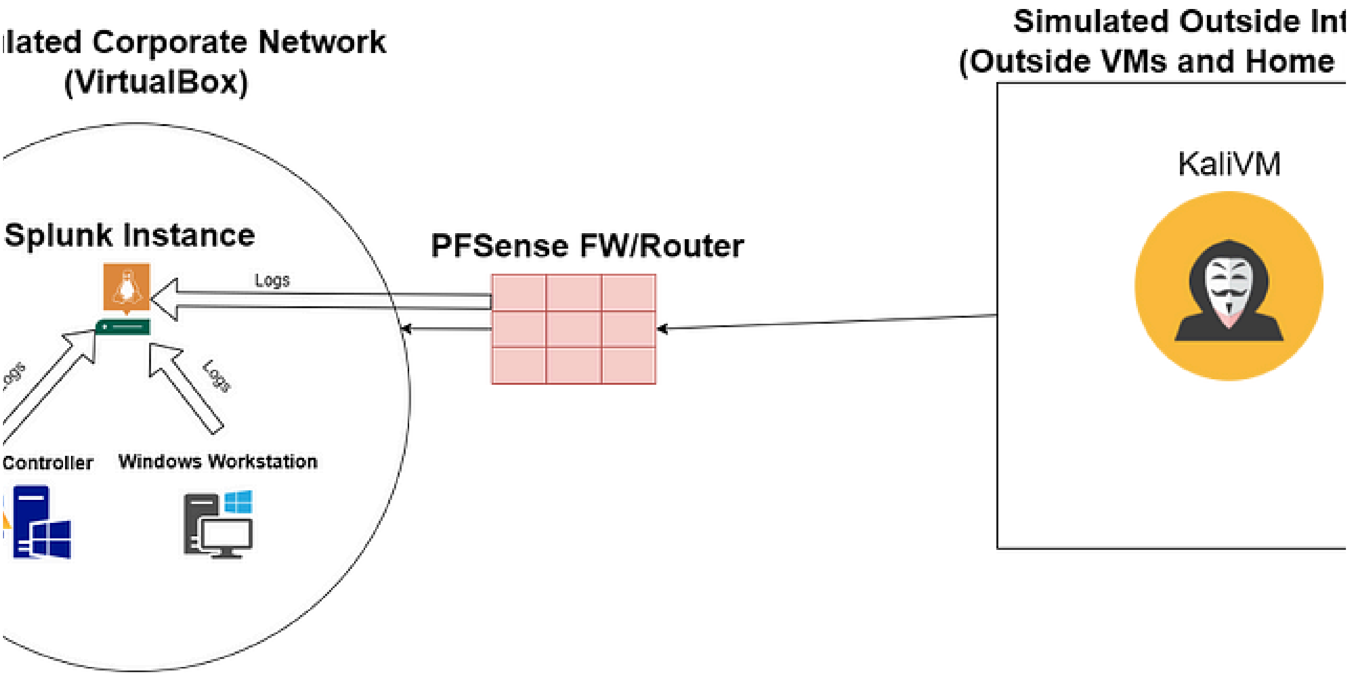
13 Followers · 1 Following

No responses yet

What are your thoughts?

Respond

More from Andrew

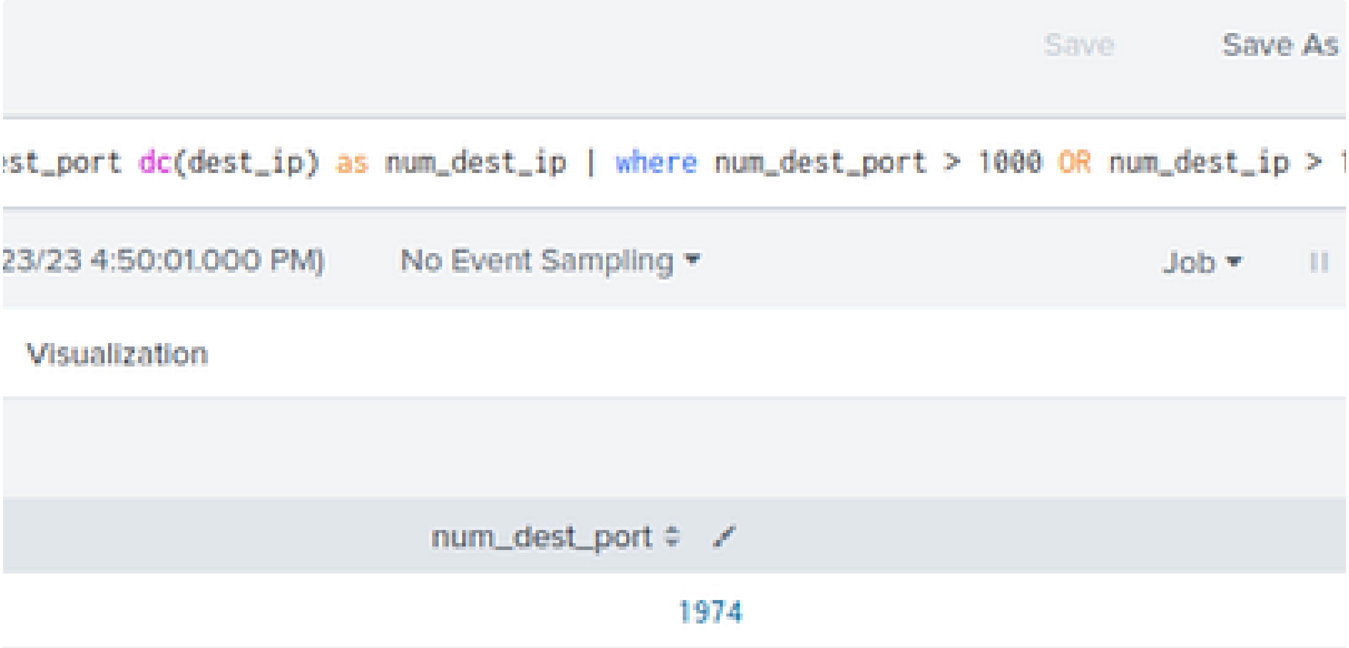


Andrew

SIEM HomeLab — Part 1

In this overview, I'll guide you through setting up a Security Information and Event Management (SIEM) homelab using VirtualBox. The lab...

Dec 24, 2023 8



```
st_port dc(dest_ip) as num_dest_ip | where num_dest_port > 1000 OR num_dest_ip > 1
```

23/23 4:50:01.000 PM)

num_dest_port
1974

Andrew

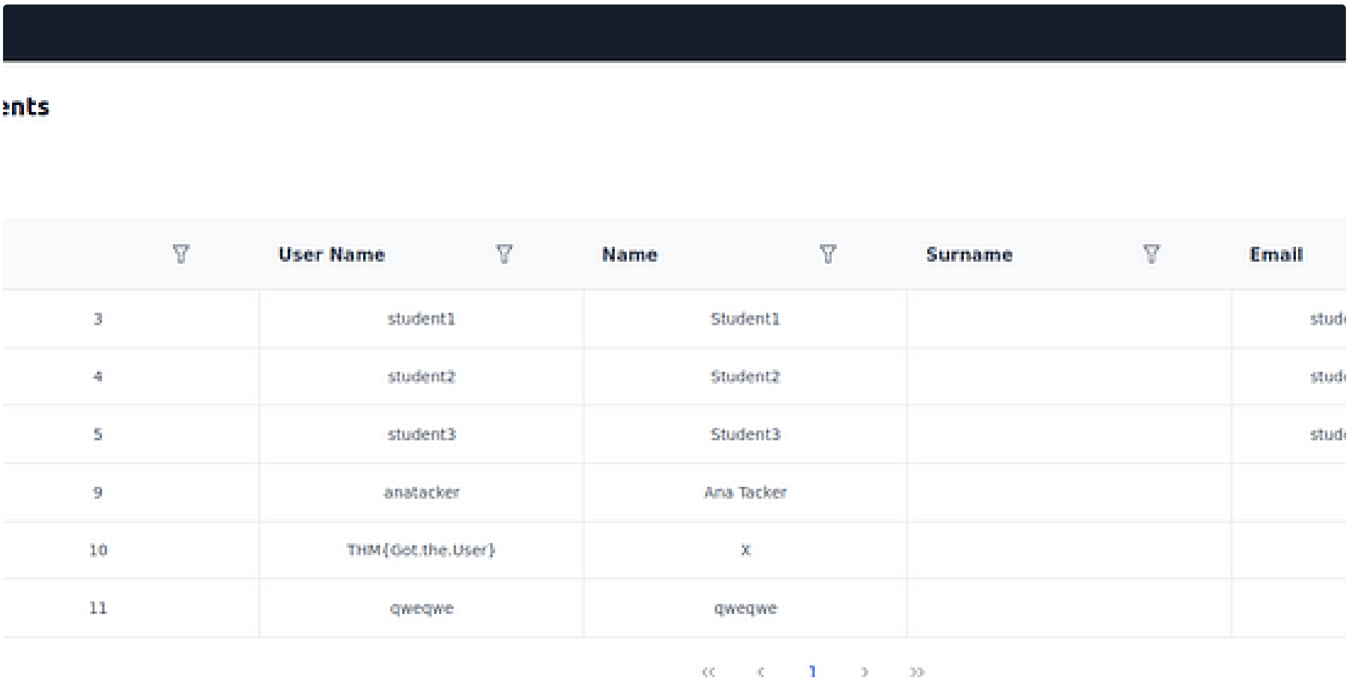
SIEM HomeLab Part 2

Welcome to Part 2 of our SIEM homelab series (part 1 can be found here). In this installment, we'll configure a simple Splunk alert to…

Dec 24, 2023 1

See all from Andrew

Recommended from Medium



ents

	User Name	Name	Surname	Email
3	student1	Student1		stud
4	student2	Student2		stud
5	student3	Student3		stud
9	anatacker	Ana Tacker		
10	THM{Got.the.User}	X		
11	qweqwe	qweqwe		

embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

Aug 7, 2024 27

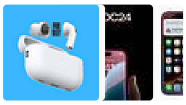
In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

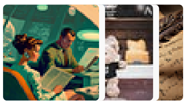
Nov 5, 2024 60

Lists



Tech & Tools

22 stories · 381 saves

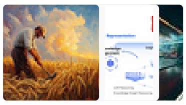


Medium's Huge List of Publications Accepting Submissions

377 stories · 4347 saves

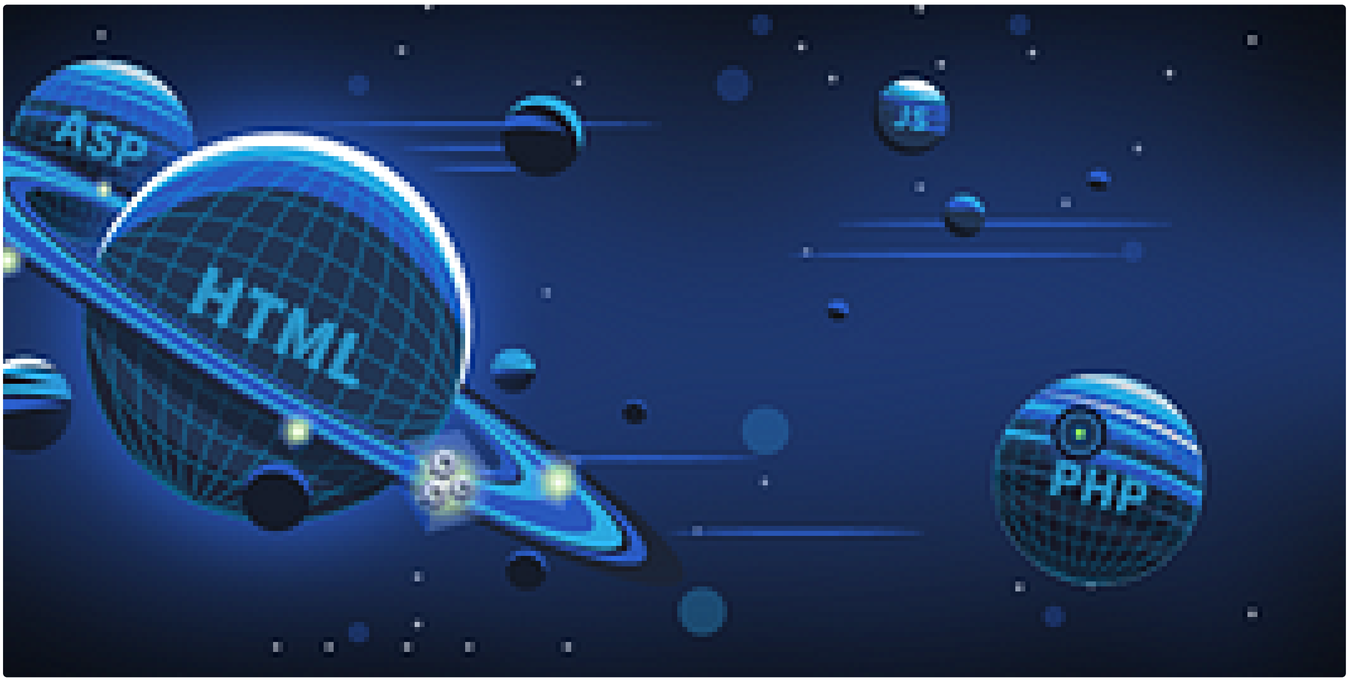
Staff picks

796 stories · 1558 saves



Natural Language Processing

1884 stories · 1530 saves

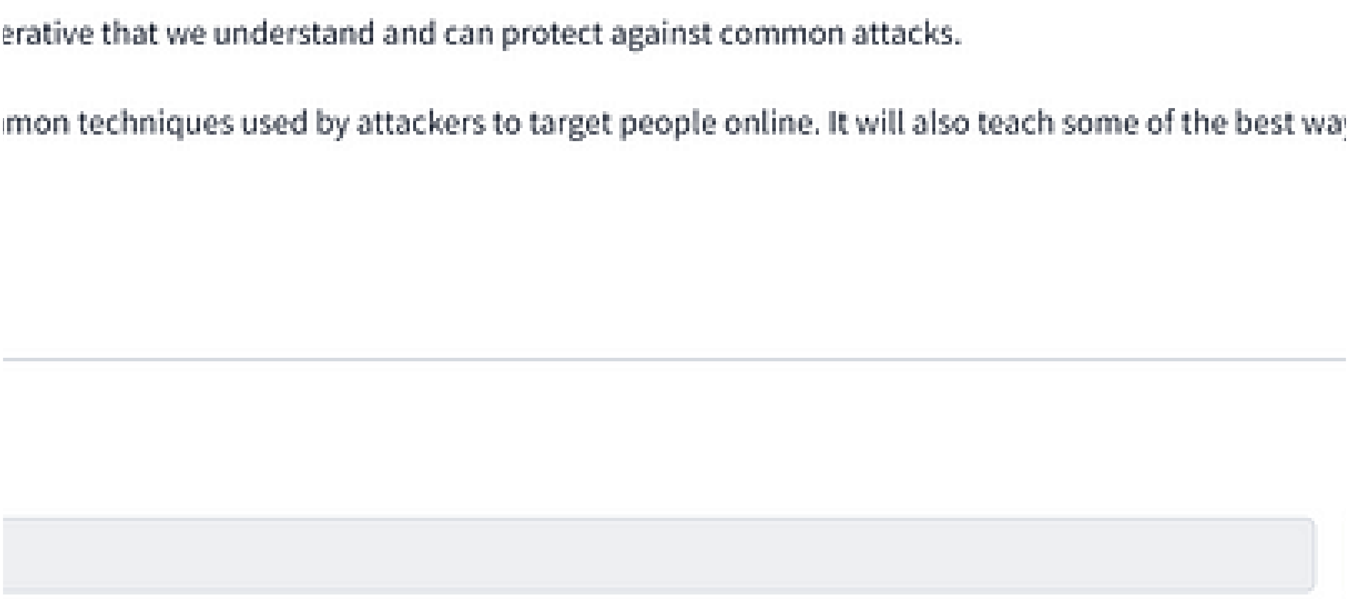


In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

Oct 26, 2024 56



erative that we understand and can protect against common attacks.

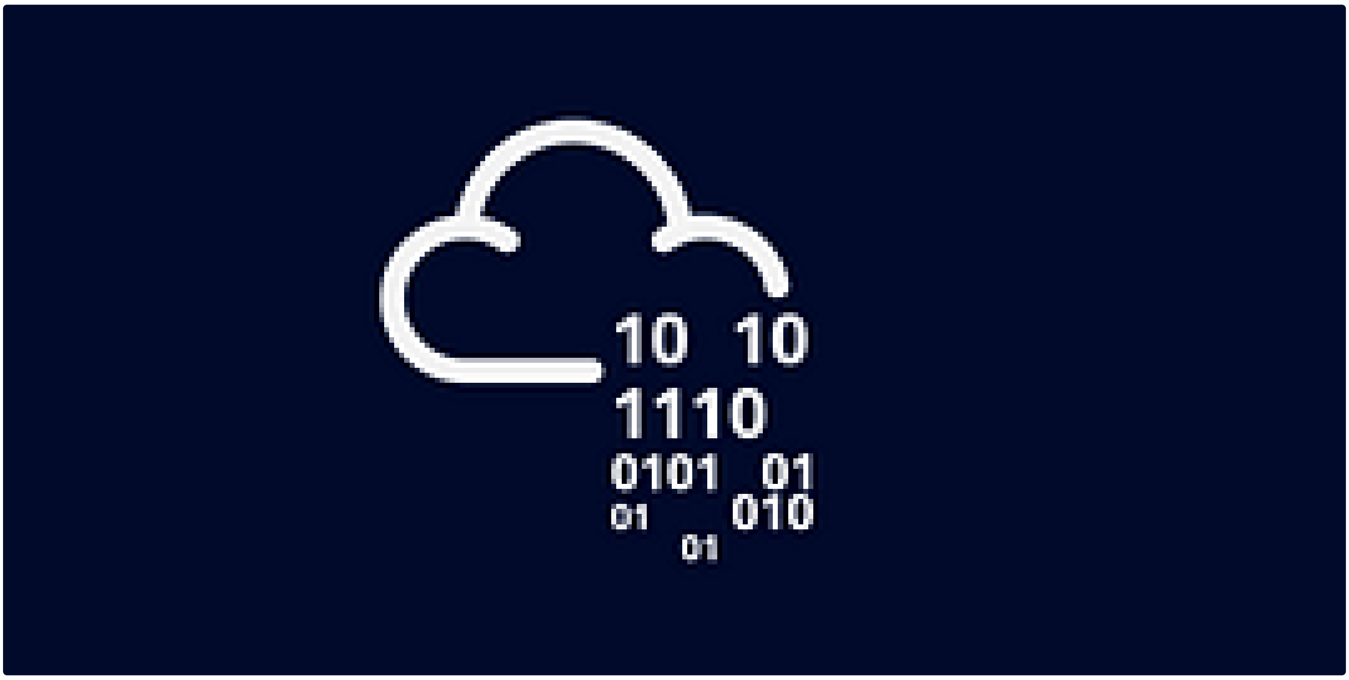
mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

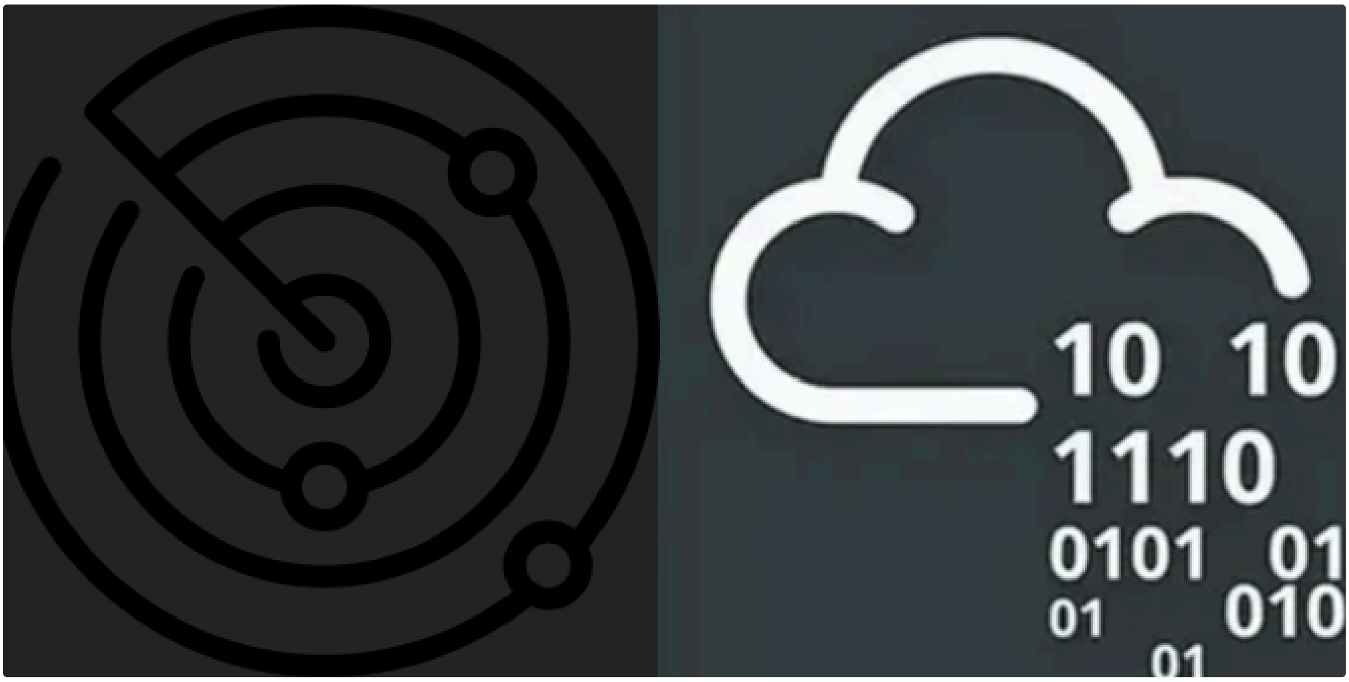


In T3CH by Axoloth

TryHackMe | AD Certificate Templates | WriteUp

Walkthrough on the exploitation of misconfigured AD certificate templates

Sep 11, 2024 70



IritT

Nmap — TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

Dec 23, 2024

See more recommendations