

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



Phishing Prevention | TryHackMe | Solution



Neharidha Murali · [Follow](#)

3 min read · Nov 2, 2023



Listen



Share

... More

Phishing Prevention

Learn how to defend against phishing emails.

Task1:

After visiting the [link](#) in the task, what is the **MITRE ID** for the “Software Configuration” mitigation technique?

Correct Answer: M1054

Task2:

Referencing the [dmarcian SPF syntax table](#), what prefix character can be added to the “all” mechanism to ensure a “softfail” result?

Correct Answer: ~

What is the meaning of the **-all** tag?

Correct Answer: fail

Task3:

Which email header shows the status of whether DKIM passed or failed?

Correct Answer: Authentication-Results

Task4:

Which DMARC policy would you use not to accept an email if the message fails the DMARC check?

Correct Answer: p=reject

Task5:

What is nonrepudiation? (The answer is a full sentence, including the “.”)

Correct Answer: The uniqueness of a signature prevents the owner of the signature from disowning the signature.

Task6:

What Wireshark filter can you use to narrow down the packet output using SMTP status codes?

Correct Answer: smtp.response.code

Per the network traffic, what was the message for status code 220? (Do not include the status code (220) in the answer)

Correct Answer: <domain> service ready

One packet shows a response that an email was blocked using spamhaus.org. What were the packet number and status code? (no spaces in your answer)

Correct Answer: 156,553

Based on the packet from the previous question, what was the message regarding the mailbox?

Correct Answer: mailbox name not allowed

What is the status code that will typically precede a SMTP DATA command?

Correct Answer: 354

Task7:

What port is the SMTP traffic using?

Correct Answer: 25

How many packets are specifically SMTP?

Correct Answer: 512

What is the source IP address for all the SMTP traffic?

Correct Answer: 10.12.19.101

What is the filename of the third file attachment?

Correct Answer: attachment.scr

How about the last file attachment?

Correct Answer: .zip

Task8:

Per MITRE ATT&CK, which software is associated with using SMTP and POP3 for C2 communications?

Correct Answer: Zebrocy

Task9:

Per the playbook, what framework was used for the IR process?

Correct Answer:nist

Happy Learning — Hope this helps you out :)

For in-depth solutions, check this out — <https://github.com/neharidha?tab=repositories>

-Neharidha Murali

Phishing Prevention

Tryhackme

Neha

Neharidhamurali



Follow

Written by Neharidha Murali

37 Followers · 3 Following

Neharidha Murali - Security Engineer | : <https://github.com/neharidha>: Interested in Development & Hacking, University of Maryland US

No responses yet



What are your thoughts?

Respond

Open in app ↗

Medium

🔍 Search



More from Neharidha Murali



Neharidha Murali

Governance & Regulation | TryHackMe | Solution

Governance & Regulation

Jan 12, 2024 🖱 4





Neharidha Murali

Vulnerabilities 101 | TryHackMe | Solutions

Vulnerabilities 101

Apr 9, 2024 🖱️ 52



Neharidha Murali

How websites work | TryHackMe | Solution

How websites work

Nov 4, 2023 🖱️ 2





Neharidha Murali

Linux Fundamentals Part 3 | TryHackMe | Solution

Module - Linux Fundamentals

Nov 26, 2023




See all from Neharidha Murali

Recommended from Medium

Please sign in

✓ You have successfully logged out

 Rahul Kumar

Phishing | Tryhackme Walkthrough

Learn what phishing is and why it's important to a red team engagement. You will set up phishing infrastructure, write a convincing...

★ Jul 26, 2024



 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50



Lists



Staff picks

796 stories · 1561 saves



Stories to Help You Level-Up at Work

19 stories · 912 saves



Self-Improvement 101

20 stories · 3193 saves



Productivity 101

20 stories · 2707 saves



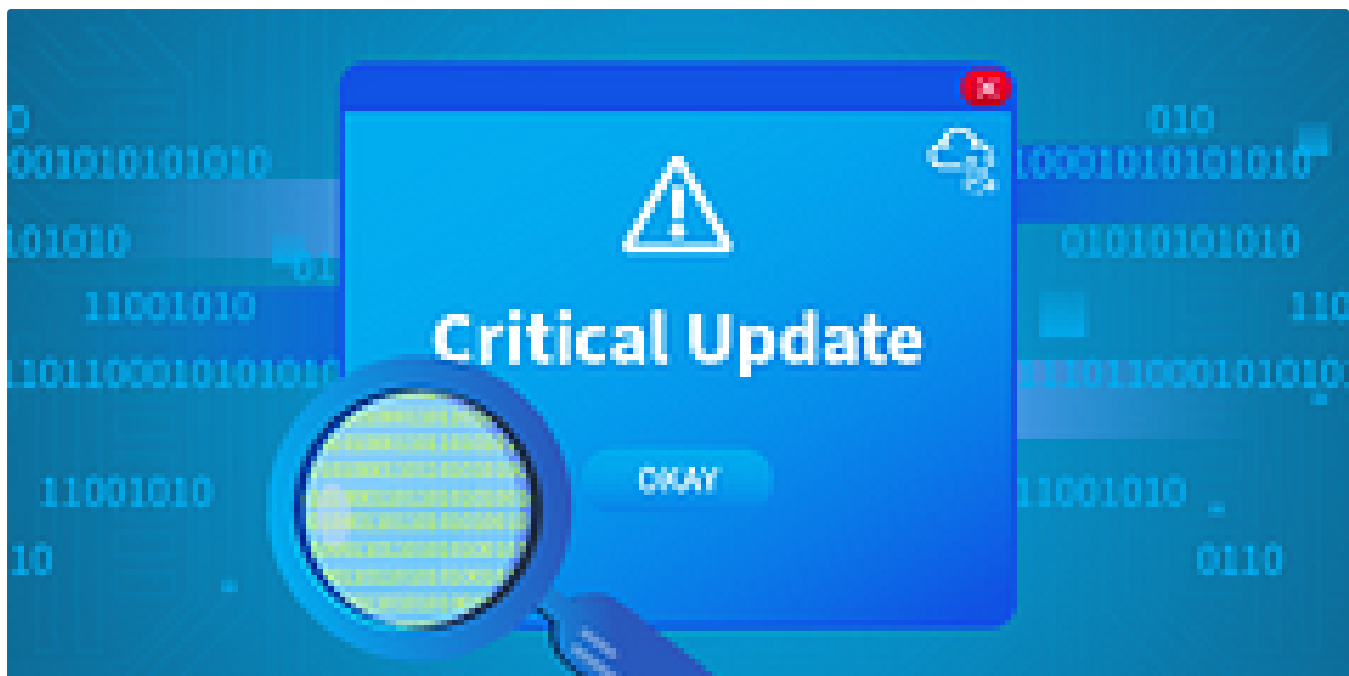
In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60





In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

★ Jul 21, 2024 🖱️ 104



```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc   run   snap  sys  usr      vmlinuz

var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log      lxd      unattended-upgrades
cloud-init.log         fontconfig.log  landscape     syslog    wtmp
dist-upgrade          journal       lastlog       tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

T Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:

<https://tryhackme.com/room/disgruntled>

Oct 22, 2024



In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario



Nov 23, 2024



50

[See more recommendations](#)