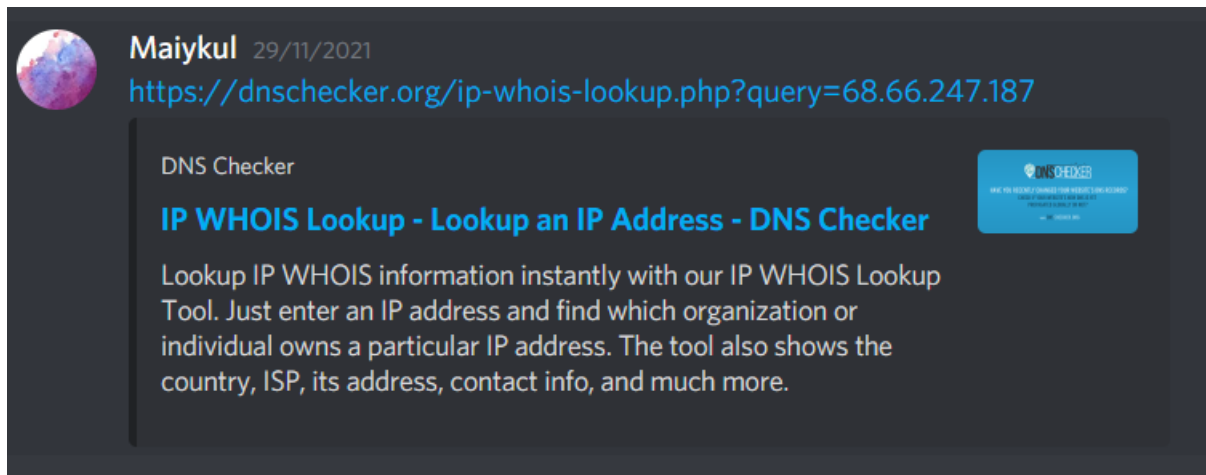


Module Contributions

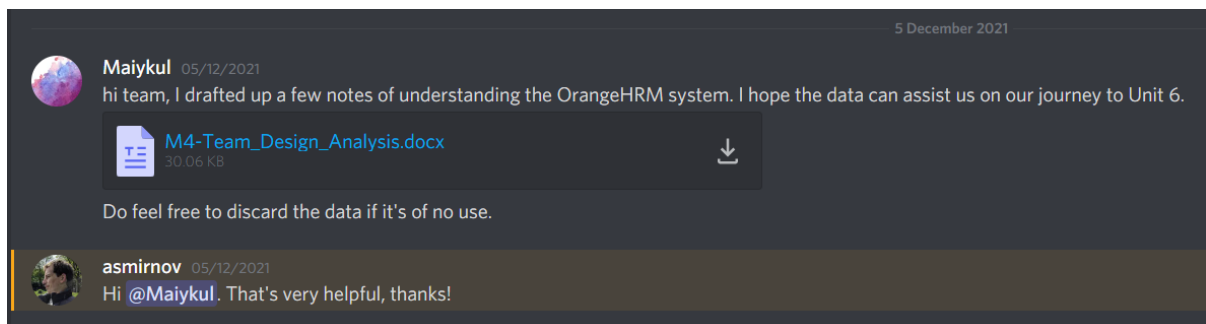
My user handle is “Maiykul” in the screenshots below.

29 November 2021




5 December 2021

Initial investigation into the types of data held by the OrangeHRM system.




13 December 2021

A link to a very useful book about security management

 **Maiykul** 13/12/2021
Hi team, I wanted to share a link to a rather in-depth book that contains detailed information that deals with network and information security. It's a good read because it deals with several topics we have touched on to date.

https://www.google.co.uk/books/edition/Information_Security_Management_Handbook/mBDNBQAAQBAJ?hl=en&gbpv=1&dq=access+controls+data+storage&pg=PA5&printsec=frontcover (edited)


Google Books
Information Security Management Handbook, Volume 3




👍 1

17 December 2021

Link to Gartner for the team to consider in the context of market-rankings of HRM products.

 **Maiykul** 17/12/2021
<https://www.gartner.com/reviews/market/vulnerability-assessment>

Gartner
Vulnerability Management Tools Reviews 2021 | Gartner Peer Insights
Read Vulnerability Management Tools reviews verified by Gartner. Compare and find the best Vulnerability Management Tools for your organization.



Choose enterprise IT solutions with confidence.
Read verified reviews from the IT community.

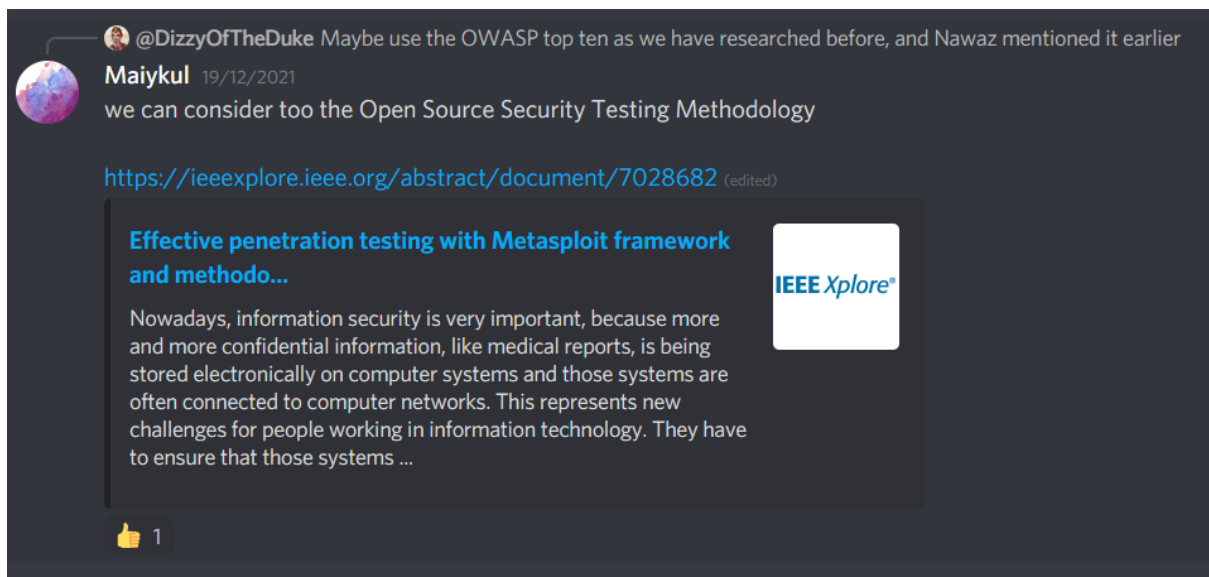
Organisations often refer to the "Gartner Magic Quadrant" which is paid-for research by companies to show customers how amazing their product is.
<https://www.gartner.com/en/research/magic-quadrant>

Gartner
Gartner Magic Quadrant & Critical Capabilities | Gartner
Gartner Magic Quadrant research methodology provides a graphical competitive positioning of four types of technology providers in fast-growing markets: Leaders, Visionaries, Niche Players and Challengers.

👍 1

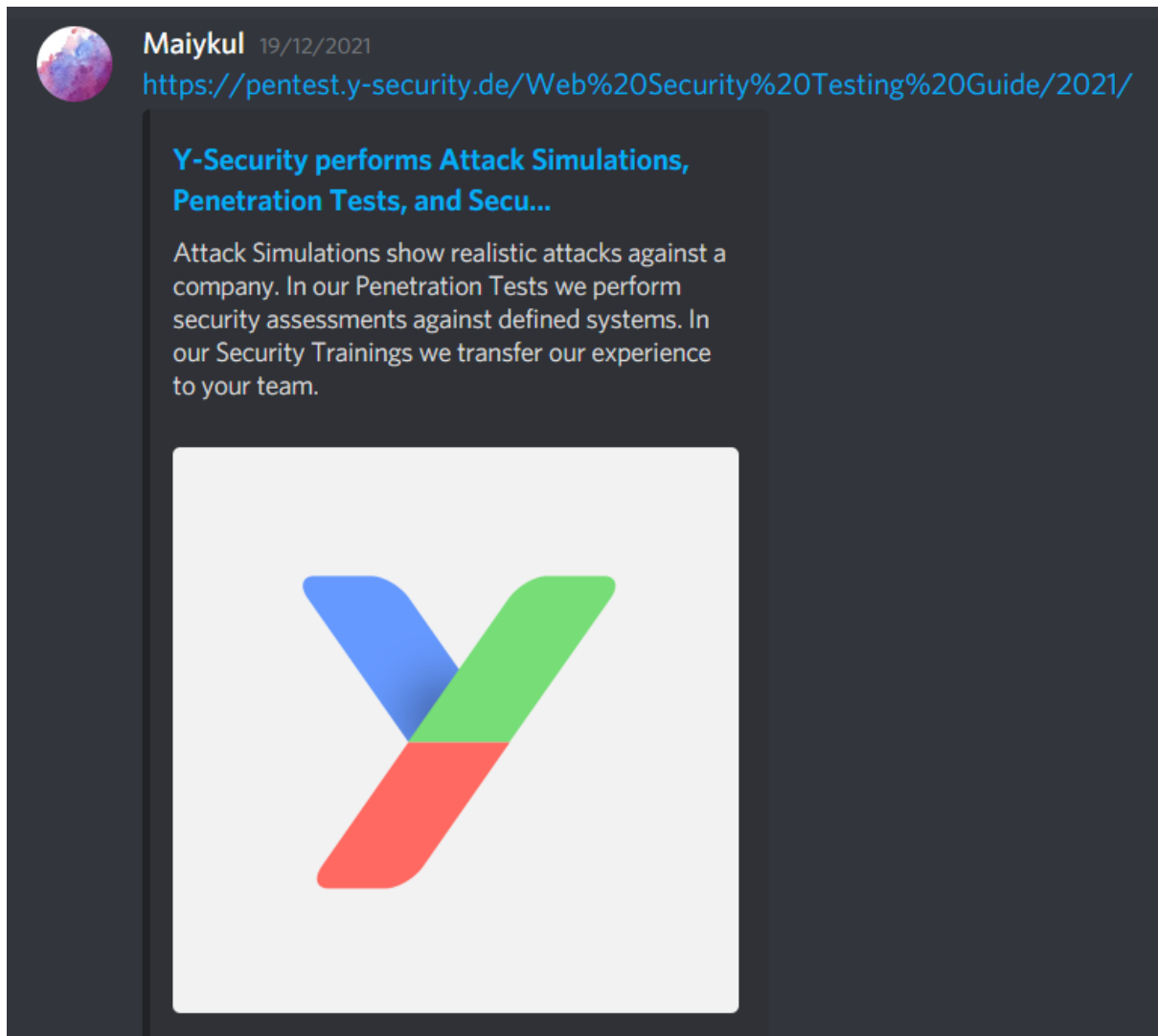
19 December 2021

Considering the frameworks for vulnerability analysis




19 December 2021

Link to penetrsation testing simulations



19 December 20201

Good link to tools for vulnerability testing.

 **Maiykul** 19/12/2021

Quite a nice link that highlights practical steps we can take test for vulnerabilities

13:40

Web Application Security Testing

- 00 Introduction and Objectives >
- 01 Information Gathering >
- 02 Configuration and Deployment Management Testing ▾
- 4.2 Configuration and Deployment Management Testing
- Test Network Infrastructure Configuration
- Test Application Platform Configuration
- Test File Extensions Handling for Sensitive Information
- Review Old Backup and Unreferenced Files for Sensitive Information

Example

```
<cross-domain-policy>
  <allow-access-from domain="*" />
</cross-domain-policy>
```

RESULT EXPECTED

- A list of policy files found.
- A list of weak settings in the policies.

Tools


- Nikto
- OWASP Zed Attack Proxy Project
- W3af

You look familiar...

😊 1

21 December 2021

Notification about Log4j vulnerability

 **Maiykul** 21/12/2021


Hi team, Just wanted to share this link because I thought it was applicable based on what @asmirnov put into the design document regarding open source software...

<https://venturebeat.com/2021/12/18/what-log4shell-teaches-us-about-open-source-security/amp/>

VentureBeat

What Log4Shell teaches us about open source security


Who is minding the gates when it comes to securing 'older' foundational open-source programs like Log4j?



👍 1


1 January 2022

Youtube link about network security.

 **Maiykul** 01/01/2022
Hi everyone, Tibbles (portrait above) wishes y'all a happy new year.
12:54 I came across this link yesternight and thought it (possibly) relevant to the content we're studying related to networks and information security.

<https://youtu.be/CS5o2AFpEJO>


YouTube
Rob Braxman Tech
How Big Tech Finds Your Exact Location -- Even When You're Hiding It



Sneaky Location Tricks

13 January 2022

Side discussion about the end of telegram messages.


 **Maiykul** 13/01/2022
Nay 😊 I was emulating writing a message in telegram style in which messages used the word "STOP" in place of "." (after ~80 characters)

<https://arstechnica.com/civis/viewtopic.php?t=648219>
<https://www.telegramstop.com/>
<https://wps.pearsoned.com/wps/media/objects/6524/6681325/Telegram%20writing.pdf>
https://en.wikipedia.org/wiki/Telegram_style

Here's a real world example: https://repository.tcu.edu/bitstream/handle/116099117/23422/Aviation_First_Flight_01_13.pdf?sequence=1. N
best way to read a message, but their creators decided this was a good idea... (edited)


19:55 And just for completeness of understanding, Samuel Morse sent the first telegram on May 25, 1844, and India sent the last one around July 20
[ever-about-sent](#)) (edited)

The Week
The last telegram ever is about to be sent
India is the last country with regular telegraph service. And the final message will be sent next month



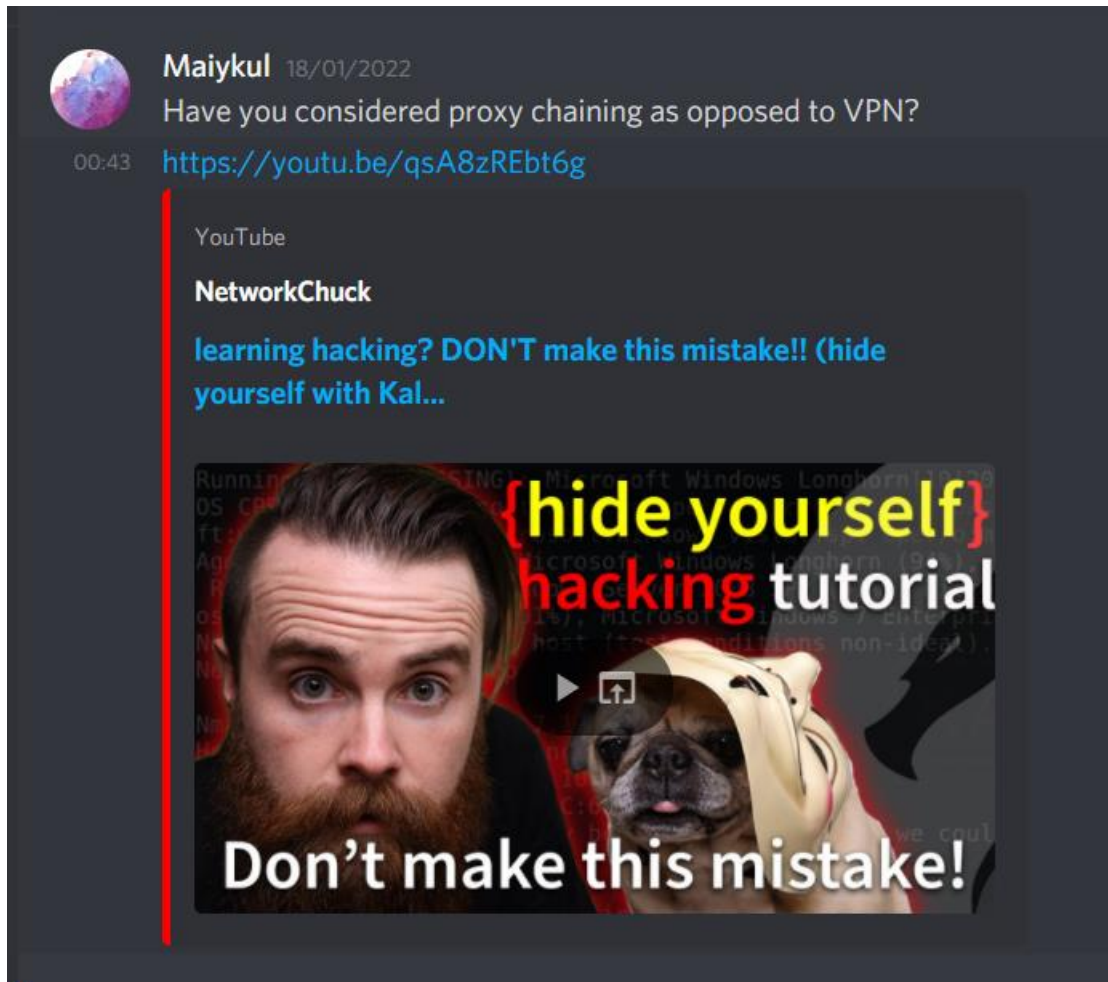
Some message formats do not last because communication requirements change over the years STOP Thank God we now have better telegra

Telegram
Telegram - a new era of messaging
Fast. Secure. Powerful.



18 January 2022

Considering proxy chaining for penetration testing.




18 January 2022

Kali Linux Chat sheet



28 January 2022


Nmap scripts released

 **Maiykul** 28/01/2022
<https://cybersecuritynews.com/new-nmap-scripts/> (edited)

Cyber Security News

NCSC Releases new Nmap Scripts to Find Unpatched Vulnerabilities

In 2016, the National Cyber Security Centre started an initiative called i100 (Industry 100), a collaborative program to secure and identify many critical vulnerabilities. This reduces the impact of Cyber attacks.



Has anyone read up on this interesting news clippage?

It's interesting because it shows that the Essex course material is not outdated 😊 (edited)

<https://thehackernews.com/2022/01/hackers-using-new-malware-packer.html?amp=1>

Hackers Using New Malware Packer DTPacker to Avoid Analysis, Detection