**Summary of Investigation Process**

The investigation process started with gathering information. In the slides from Nitroba we were given some critical information such as IP addresses, who the victim was, what attack vector was used, and possible suspects. After gathering information I looked through the PCAP file provided to me. I started off with filtering the IP address of the dorm room that the original email was traced back to(140.247.62.34) which I documented its connections and MAC address. The only IP address it connected to was 192.168.15.4 which meant if I wanted to make sure packets were from 140.247.62.34 I would have to check the MAC address. I searched for packets containing “lilytuckrige” which was the victim of the attack and started searching for any packets related to the email. I found that the attacker used anonymous emailing services to email Lily Tuckrige. I found which MAC address connected to the mailing services and filtered the displayed packets to only packets from that MAC address. After that I decided to add another filter to search for packets containing “mail” in order to find a possible email address of the attacker. After skimming through packets and cookie information I found the email address jcoachj@gmail.com which belongs to Johnny Coach who is one of Tuchrige’s students.

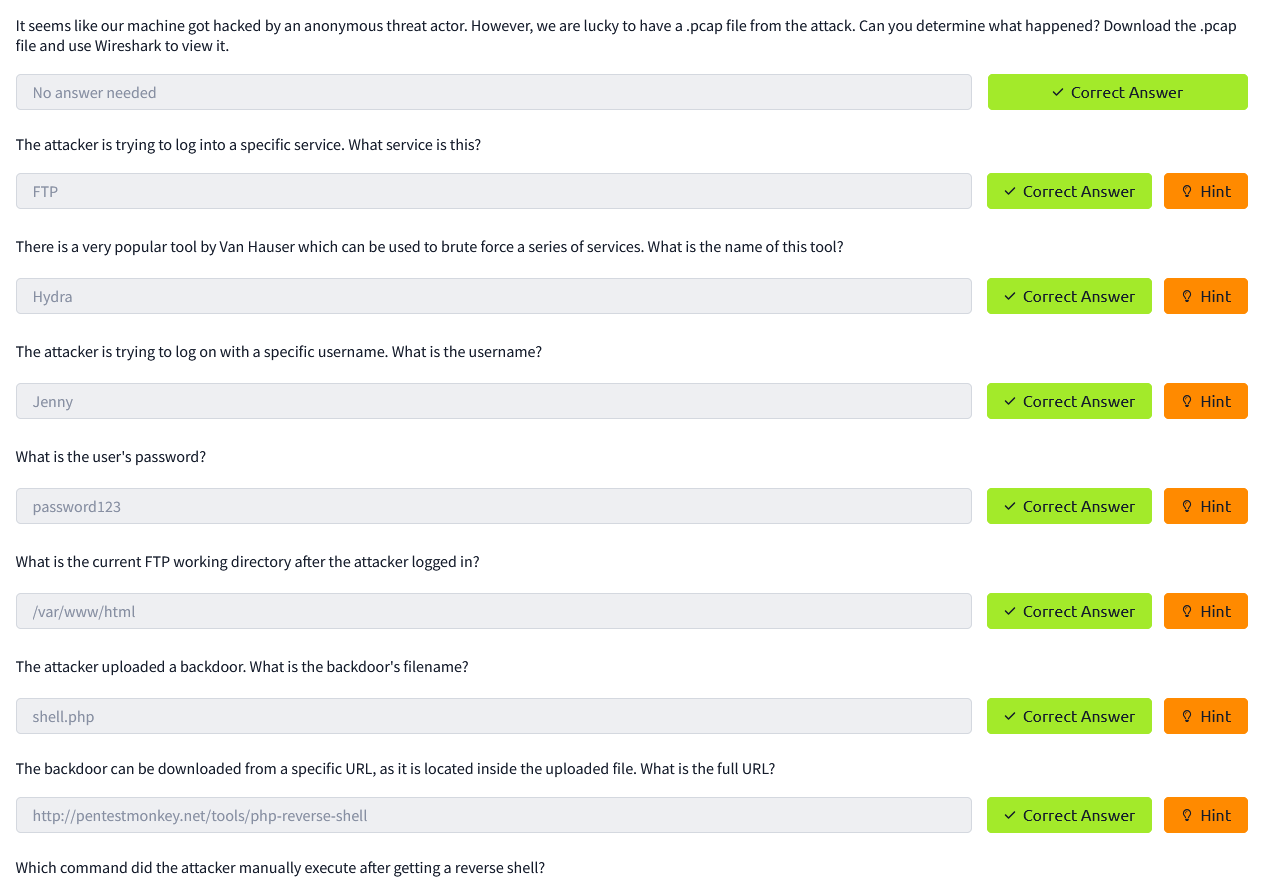
**Common Attack Techniques & Their Network Signatures**

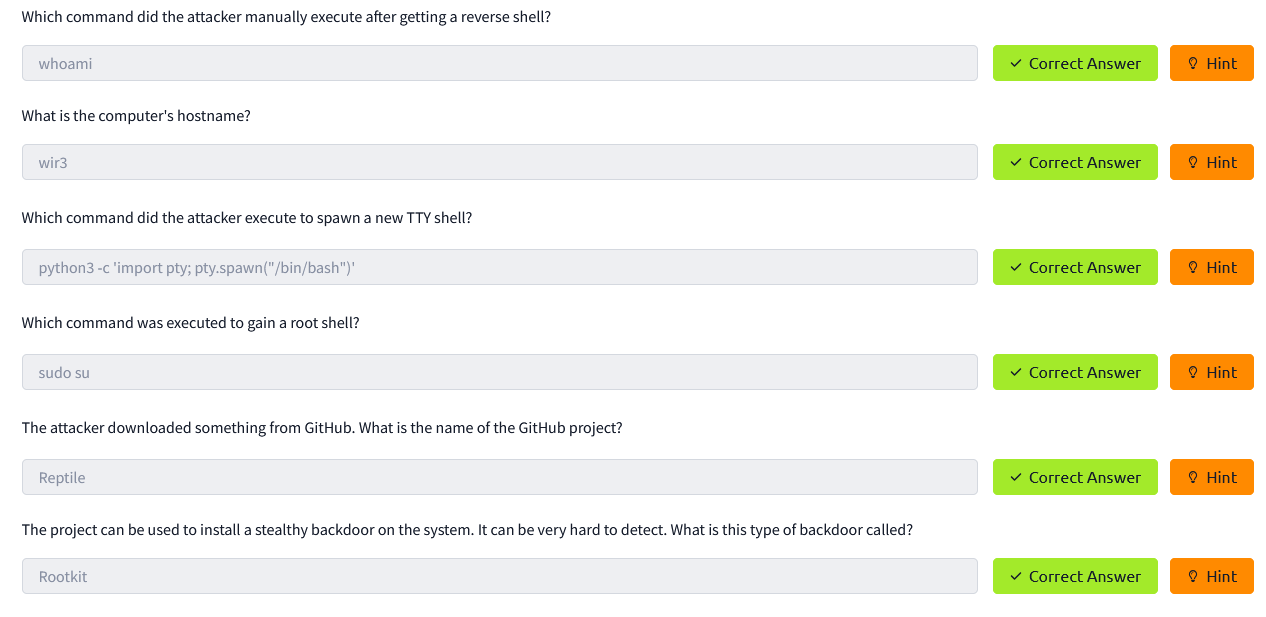
| DoS/DDoS | Network devices down or slowed. Unusual influx of traffic. |
| --- | --- |
| Password Attacks | Excess failed login attempts or pattern of suspicious login traffic |
| Brute-Force Attacks | Repeated failed login attempts in a short amount of time |
| XSS | HTTP request patterns that could indicate code injection |
| MITM | Traffic redirection, latency spikes, suspicious certificates, etc |

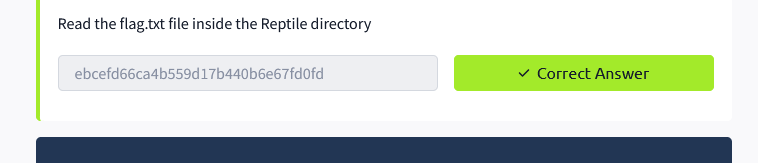
**Step-By-Step Response Procedures for Future Cases**

1. Detect a threat
2. Gather information about the threat such as which devices were affected, what protocols it affected/used, what kind of threat it is. If it is a similar harassment case then interview the victim and narrow down some possible suspects.
3. Mitigation. Close unused ports, ensure authentication is used where needed, encrypt important documents, use secure protocols, etc

**Screenshots from h4acked**

****

****

****