Network Penetration Test: Project 1 Lab Report

Ifeanyi Uzoukwu

CST 630

April 23rd, 2021

**Section 1: Introduction to Penetration Testing tools**

In this section, we were asked to perform tasks that are similar to a Network Penetration Test. In the first phase, **Reconnaissance,** students screen shotted pictures based on the directions in the lab.

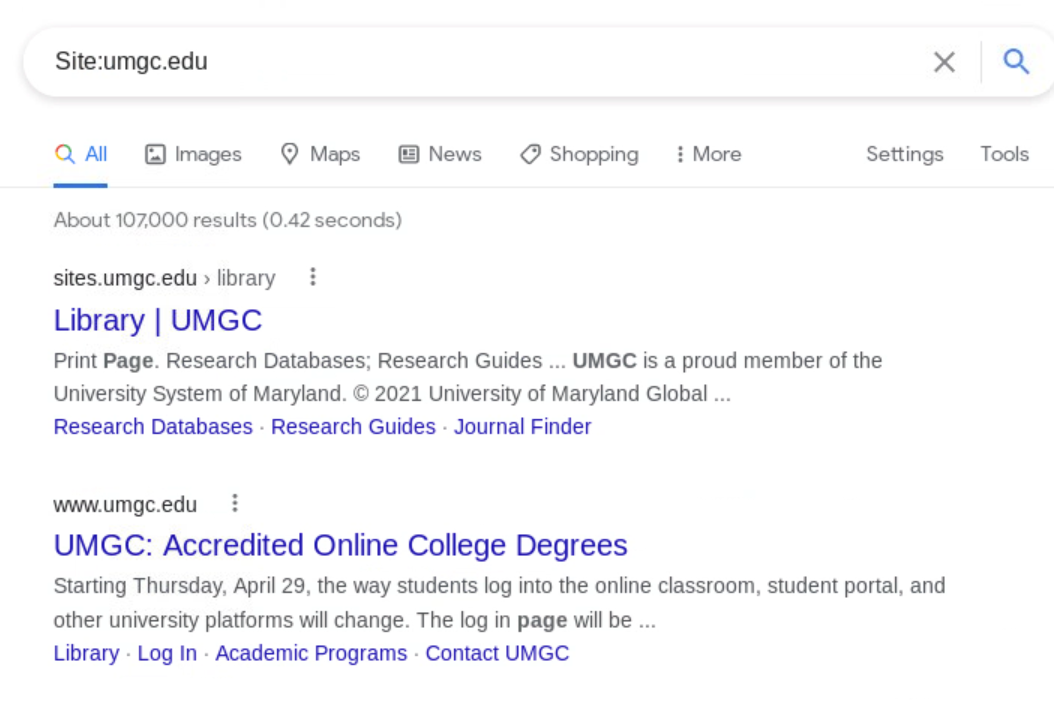


Figure : Using Site: command

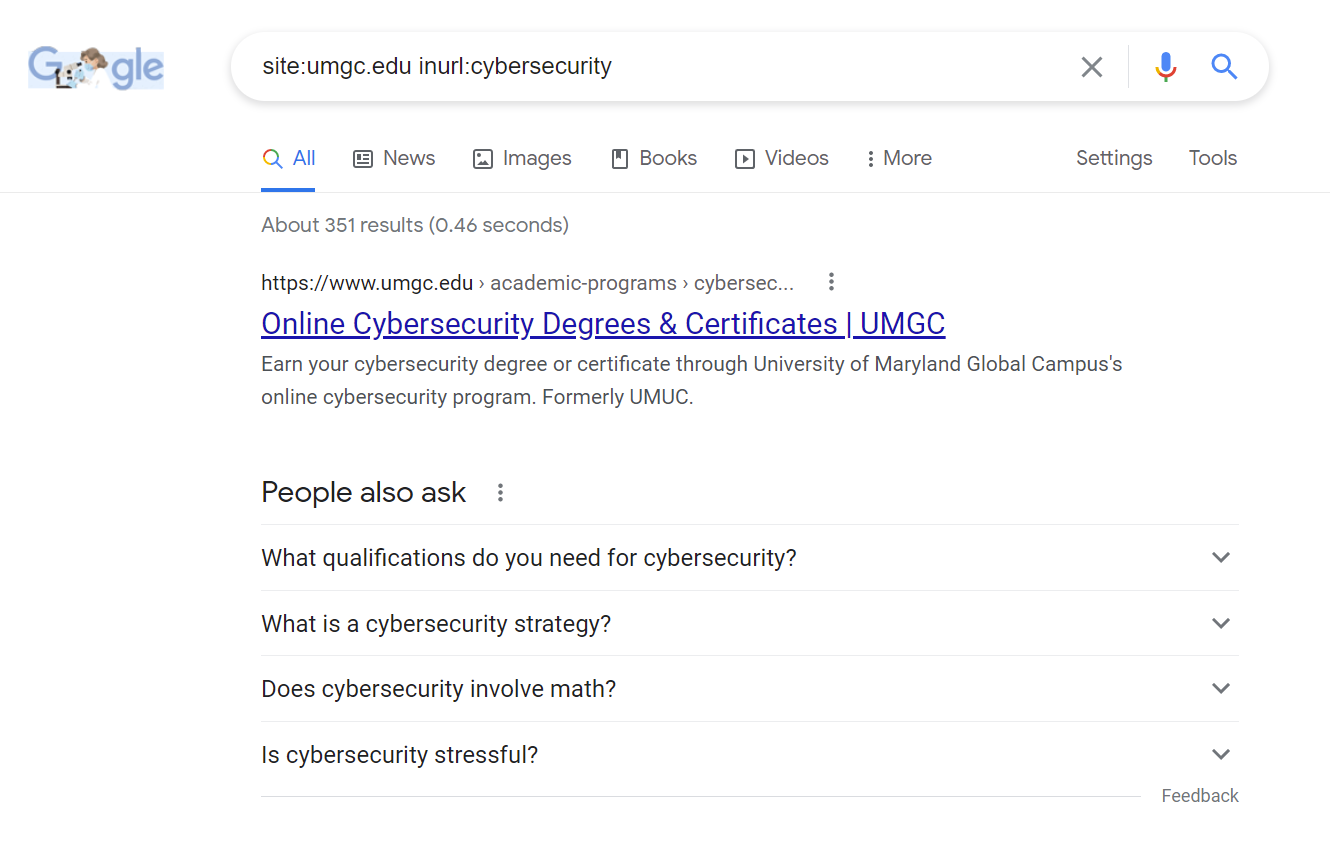


Figure : combining site: and inurl: commands

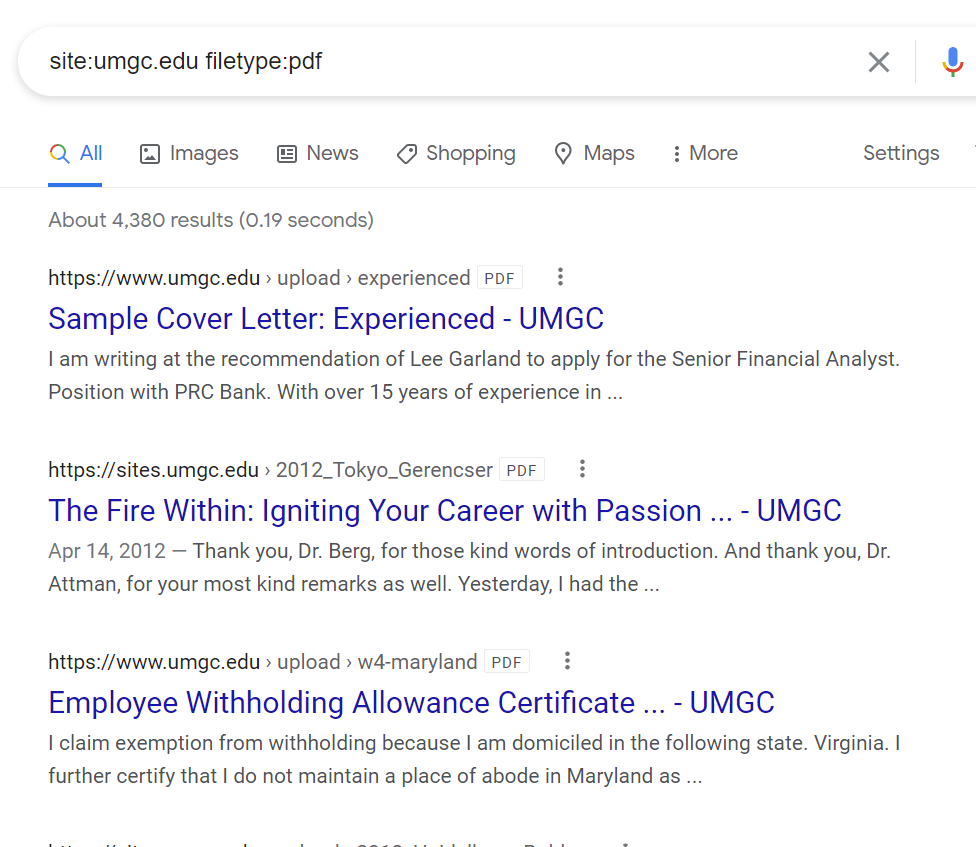


Figure Using Site: and Filetype: commands

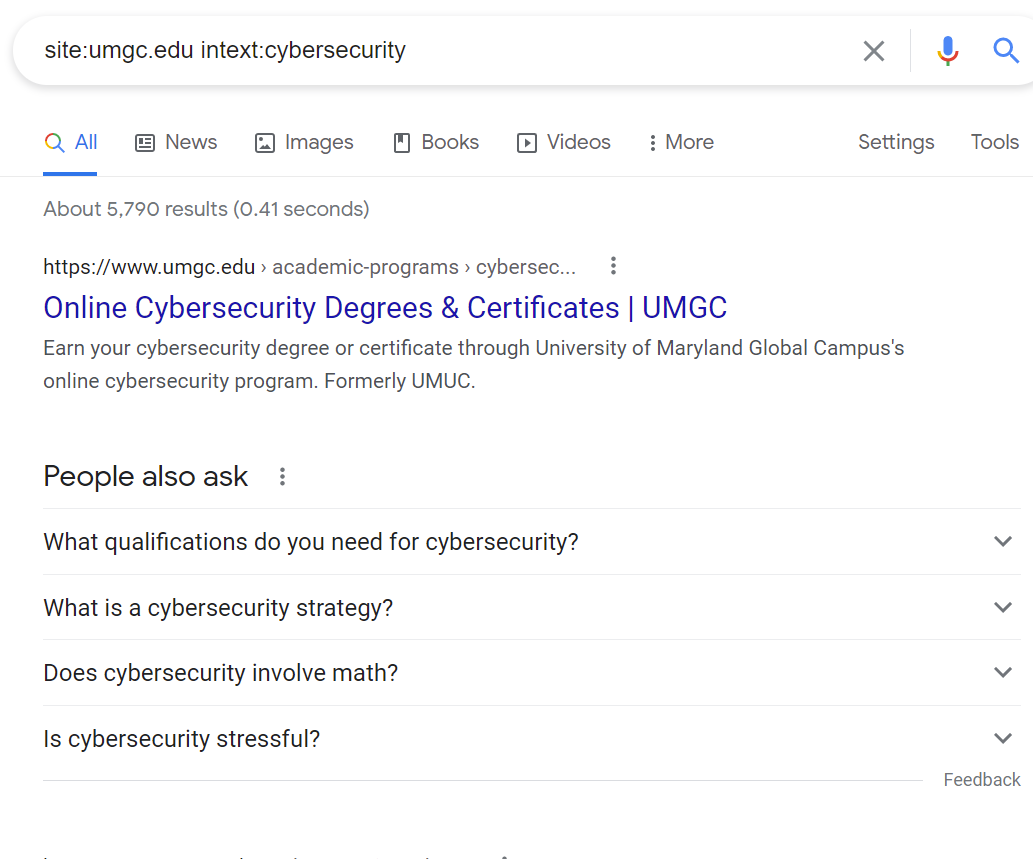


Figure Using site: and intext: commands

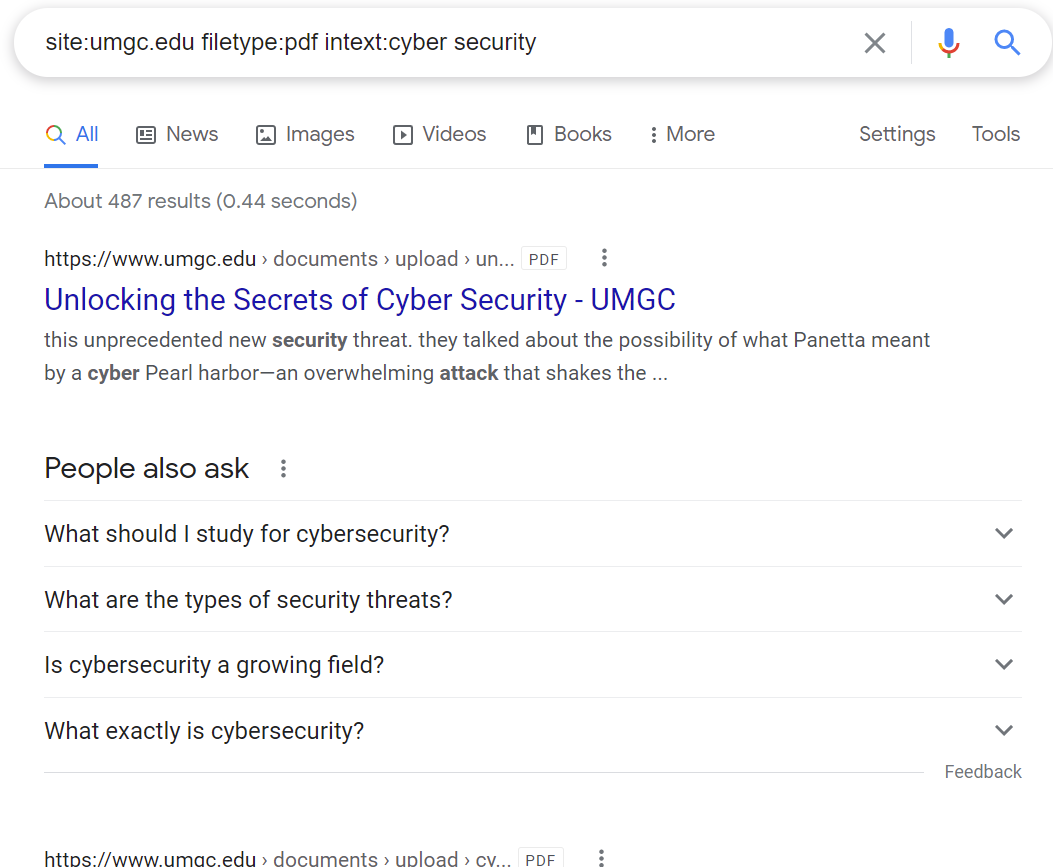


Figure Using site:, intext:, and filetype: commands

Questions:

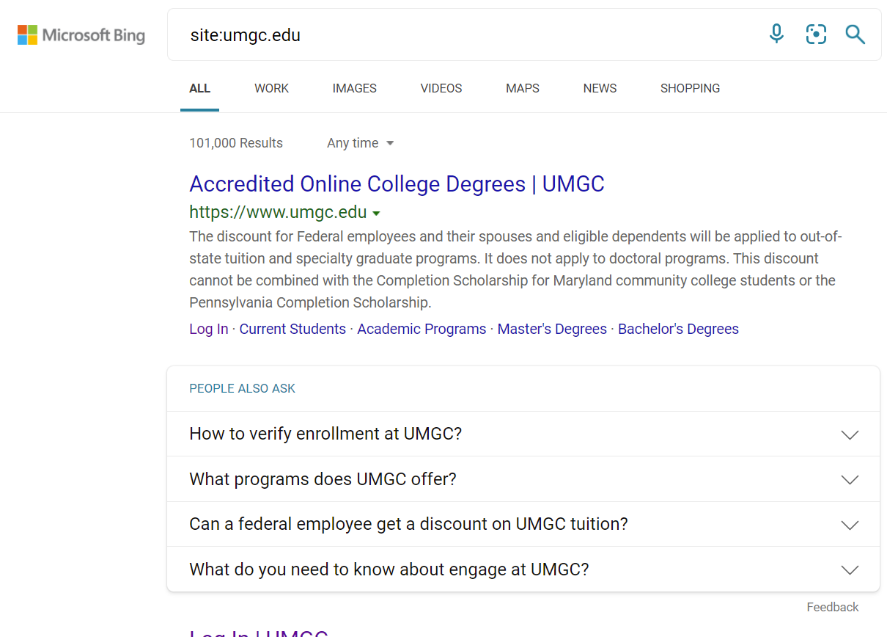
1. Pictures are provided above in Figures 1-6B.
2. The search results had changed to adapt to the different search requests that were required of the first exercise. When additional filters are added, the search results become more and more varied.
3. The typical Black Hat hacker would use these advanced search methods to find public information that would not show up in a basic search. A White hat hacker would use advanced searches like these to identify vulnerabilities within their own network.
4. While I am conducting information gathering, I would search for relevant information that would give me some insight as to what their network security posture consists of. I would also look for information on workers at the target company that should be kept private, such as names, positions, and workplace procedures.
5. Passive Reconnaissance is when you conduct a general search that gets millions of hits; whereas Active Reconnaissance brings about fewer results, but the results from this search are vastly more accurate.
6. For this question, I used Microsoft Bing and the AOL search engines. From The pictures I took, the AOL server gave less relevant results at the top. 

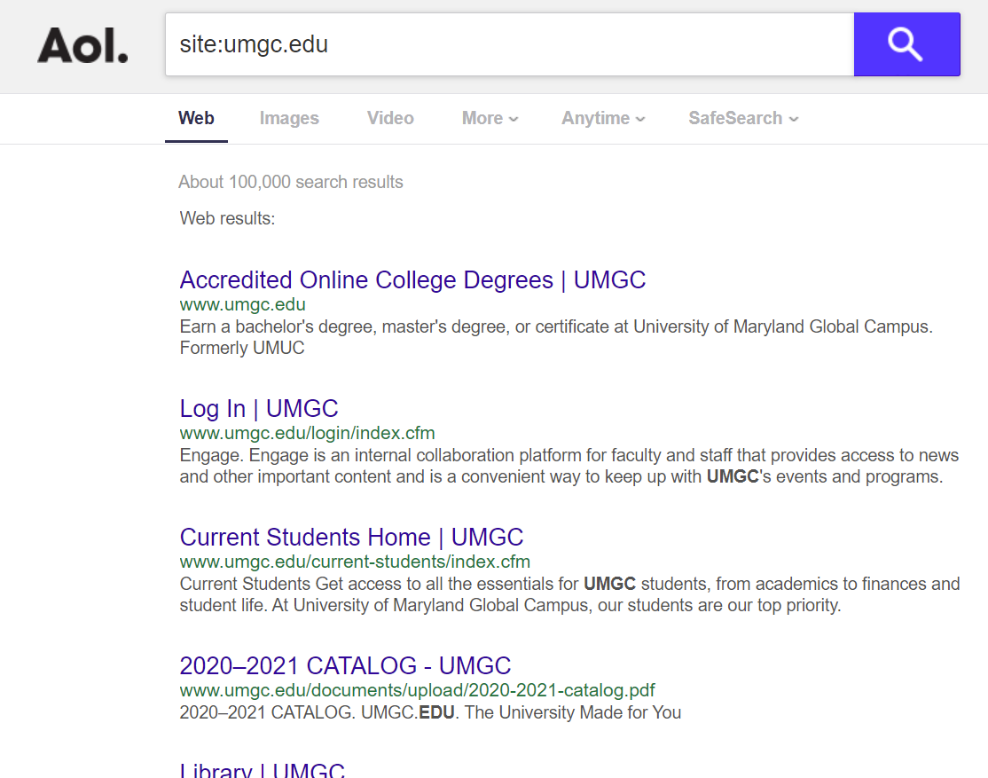
Figure Bing Site :umgc.edu

Figure AOL Site:umgc.edu

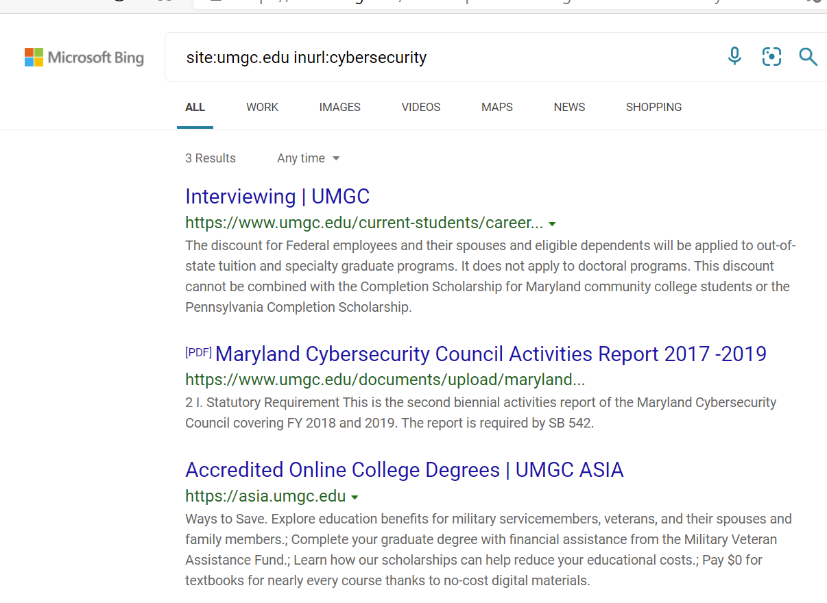


Figure Bing Site: Umgc.edu inurl: cybersecurity

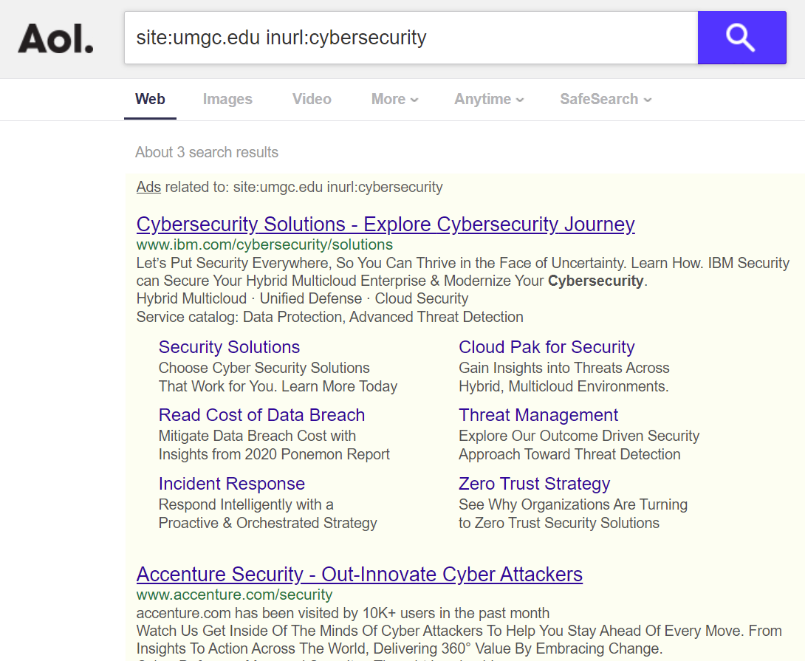


Figure AOL Site: Umgc.edu inurl: cybersecurity

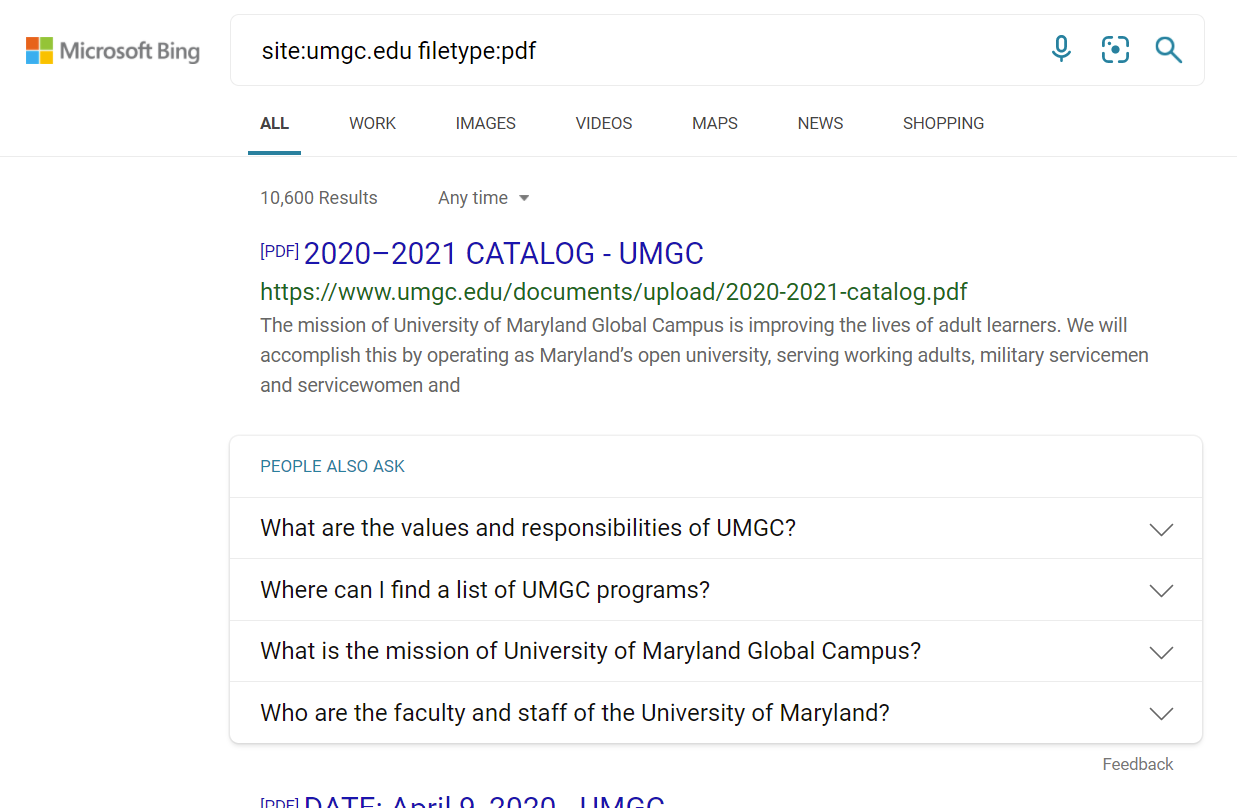


Figure Bing Site:umgc.edu Filetype: PDF

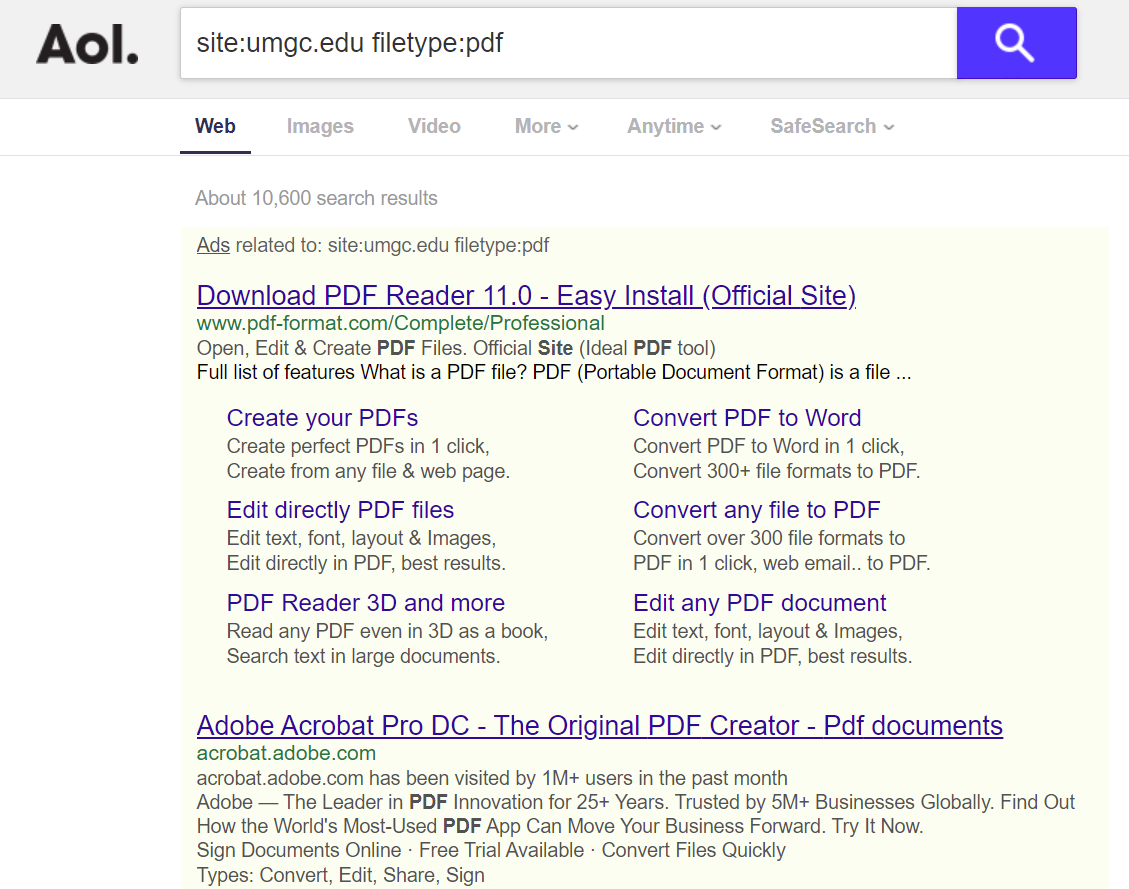


Figure AOL Site:umgc.edu Filetype:PDF

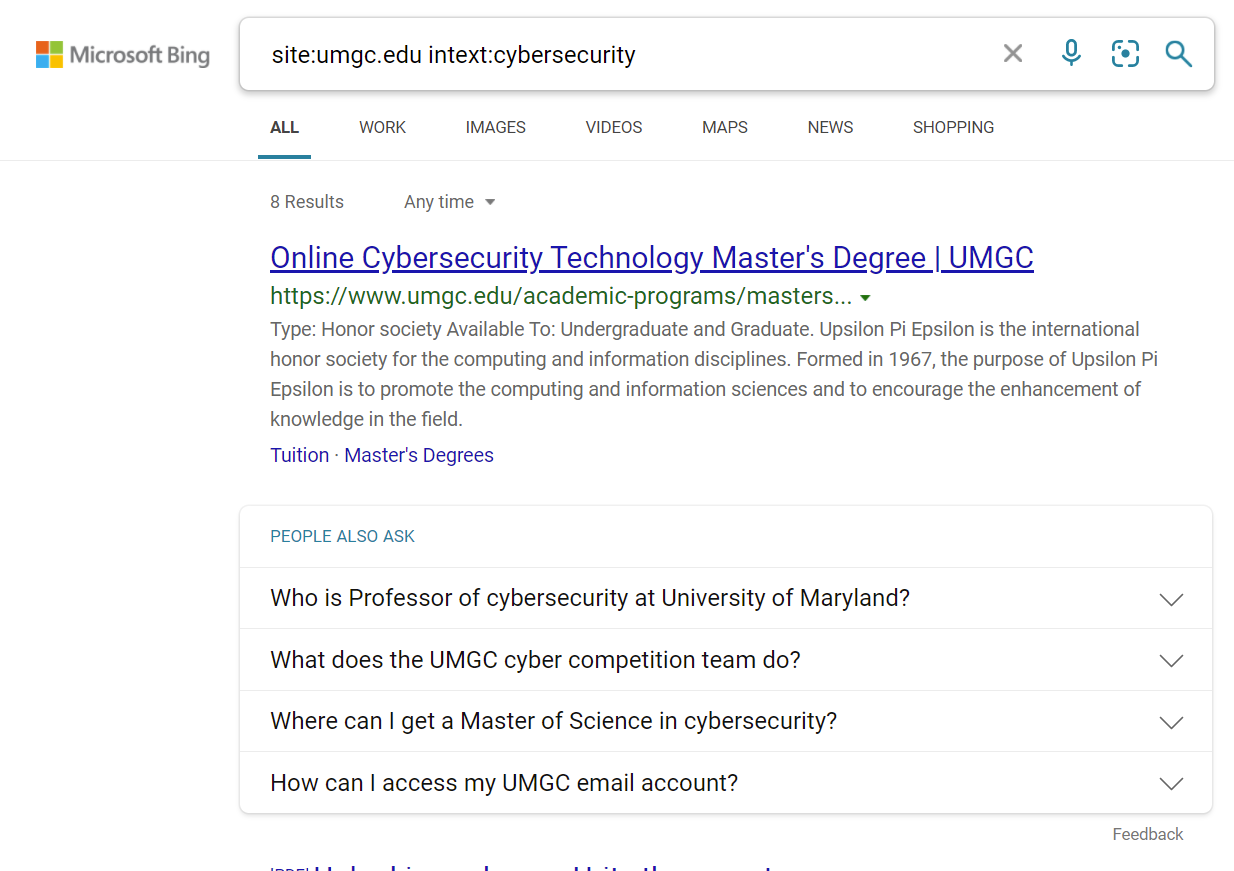


Figure Bing Site:umgc.edu intext:cybersecurity

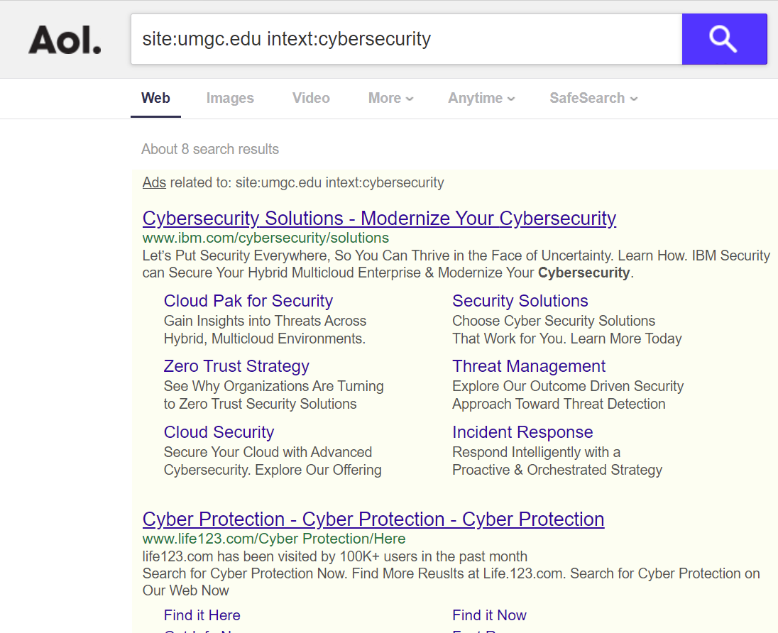


Figure AOL Site:umgc.edu intext: cybersecurity

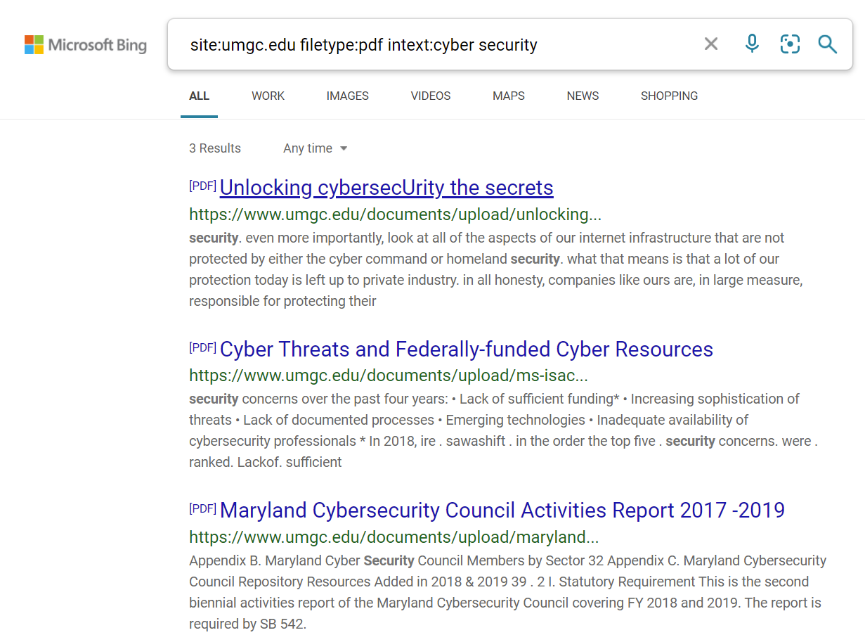


Figure Bing Site:umgc.edu filetype: PDF intext: cybersecurity

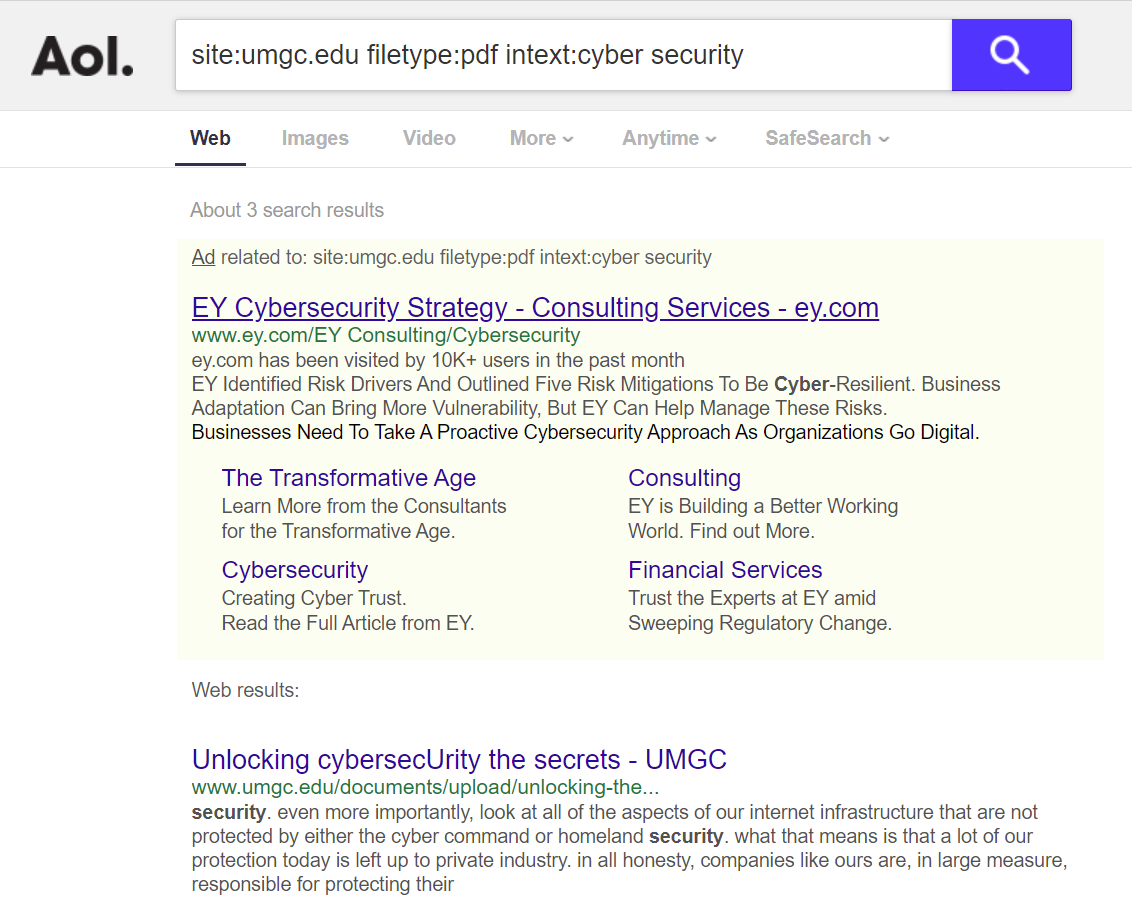


Figure AOL Site:umgc.edu filetype: PDF intext: cybersecurity

1. The email address with the different domain gives us another location to search, that could have either repeat the same information or have new information and targets to pursue.

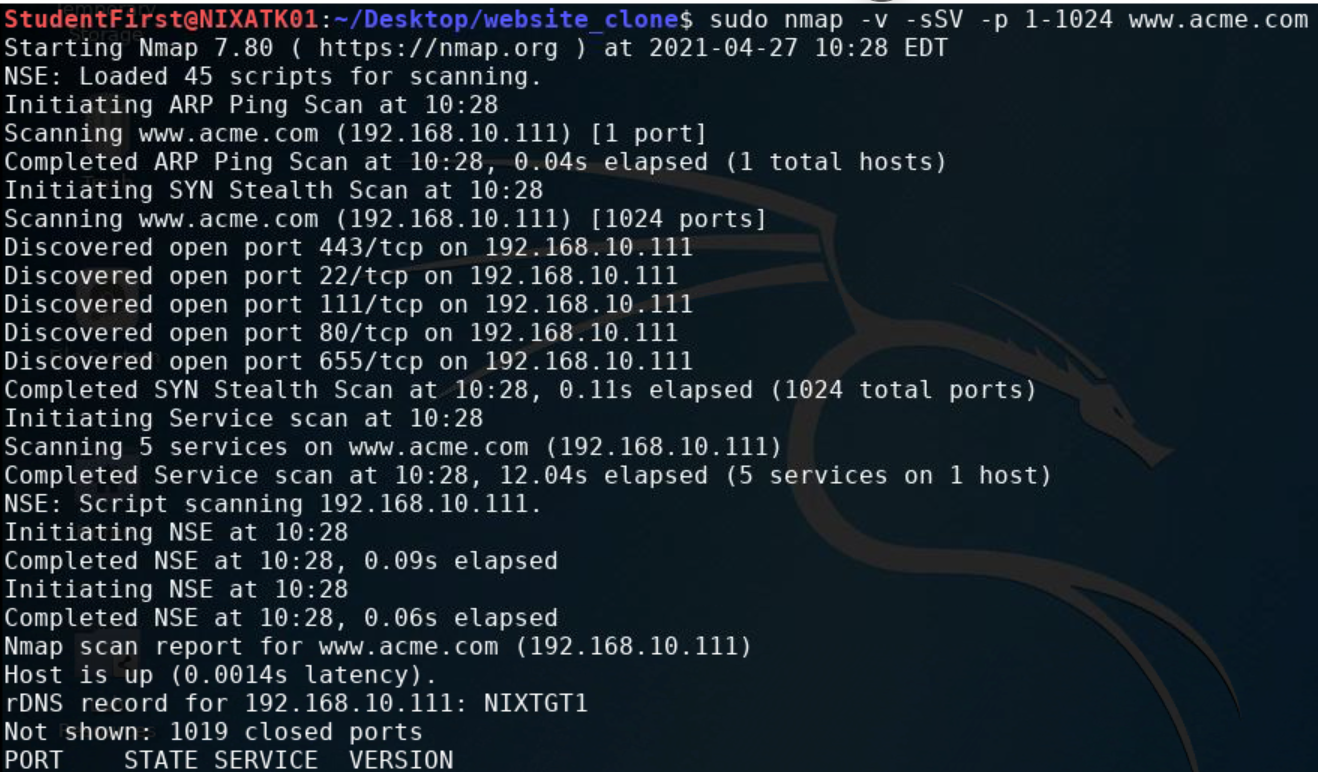
Phase 4: Exploiting or Maintaining Access allows the user to mimic the persistent attacks to a system. The IT infrastructure of any large organization that holds data needs to be ready to fend off persisting threats, so this step of the penetration test is vital. Testers normally utilize trojan horses and backdoors to remain inside of systems.

Phase 5: The final phase of a penetration test is the analysis. At this point, the information from the penetration test has been complied and is being evaluated by the tester and their superiors. In the information that is complied, there is a list of vulnerabilities that were found during the earlier phases of the penetration test. This information would also include insight as to how long the tester was able to remain undetected within the system, and which if any data was compromised.

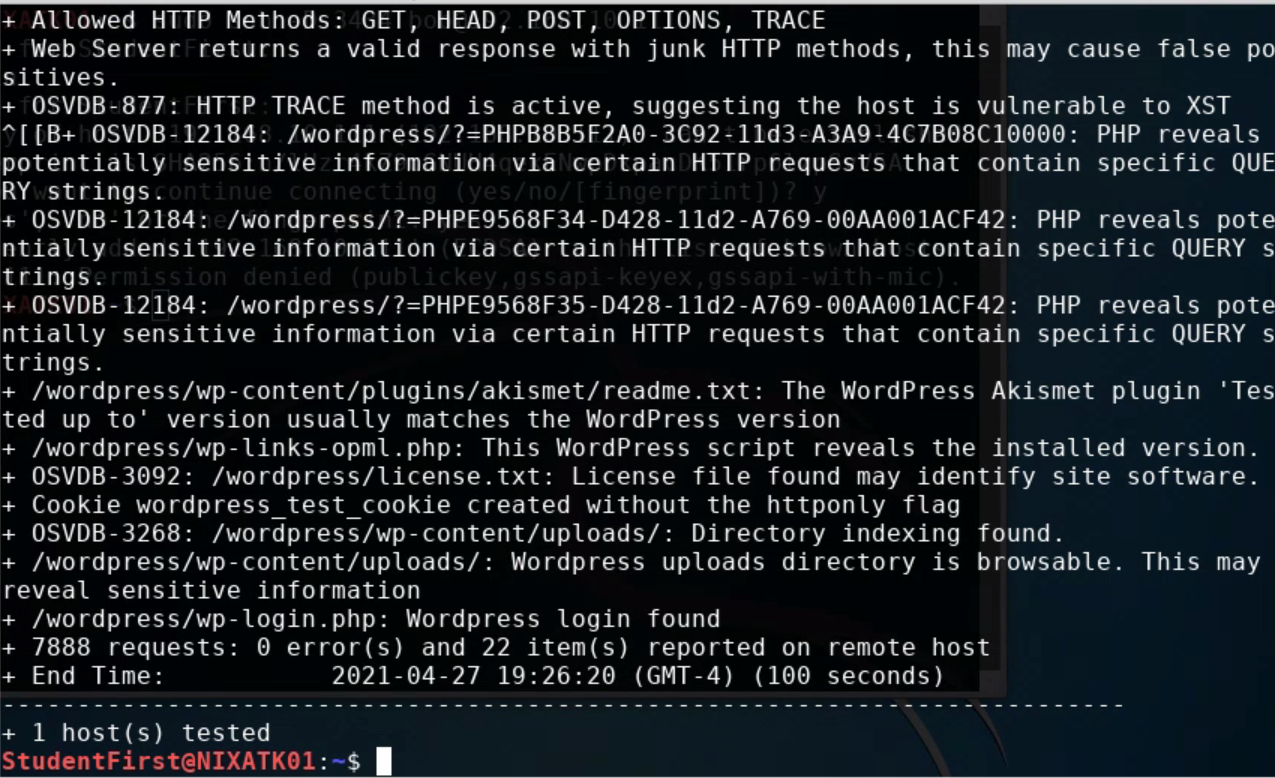
**Section 2**

NMAP

Open Ports were found on ports 22, 80, 111, 443, and 655. Service found on these ports are SSH, ,HTTP,SSL/HTTP and Tinc, a peer-to-peer VPN.



NIKTO



1. The Nmap showed me open ports and services, while the Nikto scan showed me OSVDB results and actually details the vulnerabilities.
2. The wordpress\_test\_cookie was found on the website.
3. OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

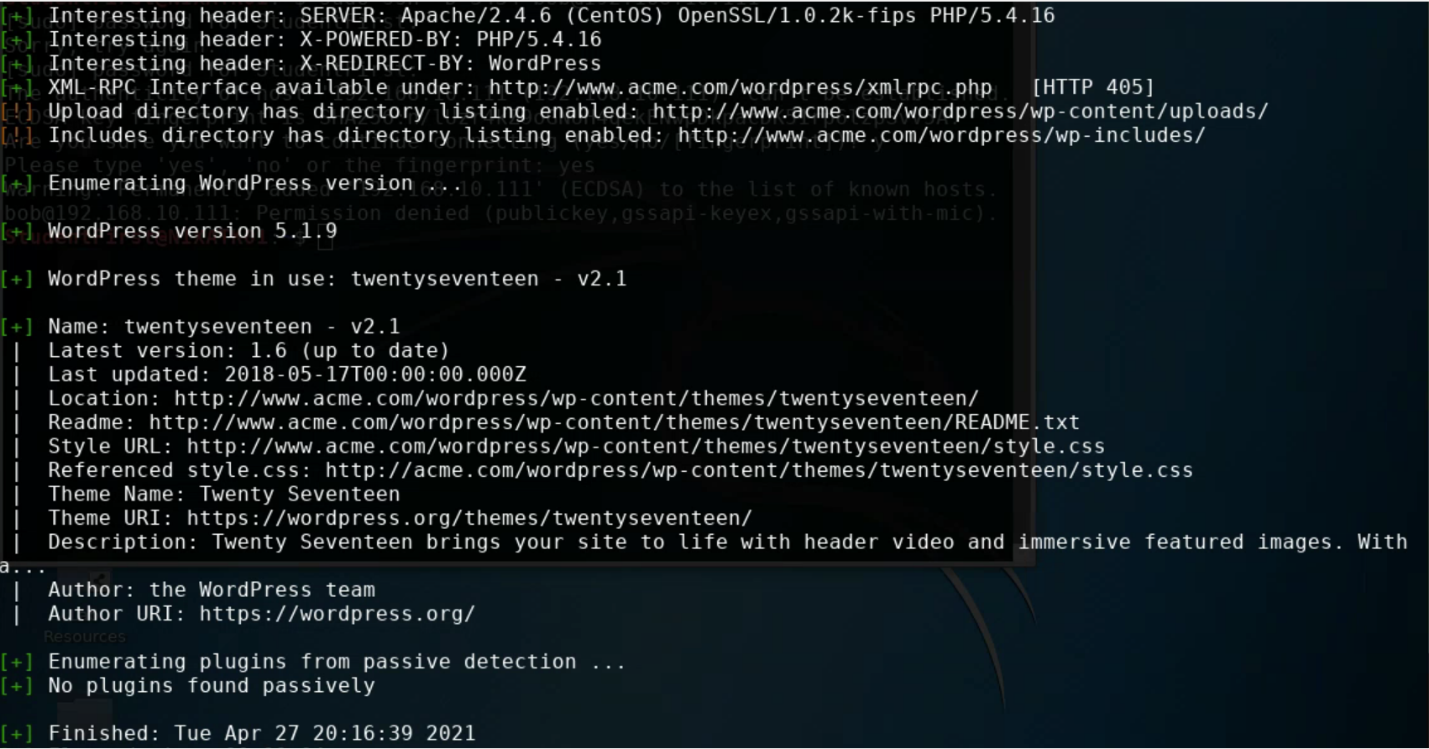
OSVDB-3092: License file found may identify site software.

OSVDB-12184:PHP reveals potentially sensitive information via certain HTTP requests which contain specific QUERY strings

1. Wordpress/wp-content/plugins/akismet/readme.txt
2. The WordPress tool gives its users the ability to create webpages in their own domain.

WPSCAN





1. How many alerts and vulnerabilities were there? 5.
2. How many red, yellow, and green alerts did you see? 22
3. Remote Code Execution (RCE) is the ability for an attacker to inject code into another user’s system no matter where the system is located.