VULNERABILITY MANAGEMENT MODULE CHALLENGE

If you have any questions, please ask them in the "Vuln-mgmt-module" channel, under the "Operation Chimera" category on the SBT Discord server.

If you feel you're familiar with what Vulnerability Management is, how to conduct simple scans,, and keep up to date with the latest vulnerabilities, then you may be ready for the Challenge! We suggest you still do some of your own research using the 'Useful Links' on the training PDF before attempting the Challenge.

What will I need for this Challenge?

- Virtualbox (https://www.virtualbox.org/wiki/Downloads)
- Kali Linux VM (https://www.kali.org/downloads/)
- Nessus (https://www.tenable.com/downloads/nessus)

Challenge Brief:

Part 1) You will be asked a number of questions about the Nessus GUI to get you exploring the platform, and you need to launch a vulnerability scan against your local machine (127.0.0.1). **Want to see some more interesting and life-like results?** Set up a Metasploitable virtual machine, and scan that to see what real vulnerabilities look like! You may use any scan templates you want, but we recommend using the Basic Network Scan template.

Part 2) Using OSINT sources, report on **two** recent vulnerabilities (NOT RELATED TO THE SCAN YOU JUST CONDUCTED!), and why they are important to watch out for at the moment. You'll need to collect the following information (marks stated below):

- [5] **CVE number** (ex: CVE-2019-0708)
- [5] **CVSS Score**
- [5] **Product/software the vulnerability affects**
- [5] **Exploitation vector** (Remote, Local, Network)
- [10] **Result(s) of successful exploitation**
- [20] **Why it is important to follow this vulnerability?**

Some suggested sources are:

- **National Vulnerability Database -** https://nvd.nist.gov
- **CVE Details -** https://www.cvedetails.com
- **SecurityWeek -** https://www.securityweek.com/virus-threats/vulnerabilities
- **Mitre -** https://cve.mitre.org/cve/
- **Try using your Tweetdeck skills** from the OSINT module! Simple examples include;
    - Vulnerability AND Critical AND Windows OR Linux OR MacOS
    - Vulnerability AND Exploited

Read to submit your Challenge? Head over to the website and click on the 'Challenge Submission' button under the Vulnerability Management module.

Vulnerability Scanning	
Nessus: **How many vulnerabilities have been detected by Nessus when you scan 127.0.0.1, using a Basic Network Scan?** [5]	
Nessus: **How many are rated as CRITICAL severity?** [5]	
Nessus: **How many are rated as HIGH severity?** [5]	
Nessus: **How many are rated as MEDIUM severity?** [5]	
Nessus: **How many are rated as INFORMATIONAL/LOW severity?** [5]	
Nessus: **Under Scan Templates in Nessus, there is a scan for what type of Ransomware?** [5]	
Nessus: **When creating a new Plugin Rule, what 4 fields do you need to enter?** [5]	
Nessus: **How many scan templates are for use against mobile devices and assets?** [5]	
What is WPScan used for? [5]	
Visit https://tools.kali.org/web-applications/wpscan - What is the command to enumerate Themes? (in the format "wpscan (arguments)" with the target url www.example.com) [10]	
Visit https://tools.kali.org/web-applications/wpscan - What is the command to enumerate Plugins? (in the format "wpscan (arguments)" with the target url www.example.com) [10]	

Visit https://tools.kali.org/web-applications/wpscan - What is the command to bruteforce a user named Samuel, with the wordlist 'passwords.txt'? (in the format "wpscan (arguments)" with the target url www.example.com) [10]	
What is OpenVAS short for? [5]	
What year was OpenVAS created? [5]	
How was OpenVAS created? [5]	

Vulnerability One	
CVE Number (or other unique identifier) [5]	
CVSS Score [5]	
Product(s) Affected [5]	
Sources that reference the vulnerability (news articles, blog posts, security advisories) [5]	
Exploitation Vector (Local, Network, Remote) [5]	
Result(s) of successful exploitation (Remote code execution, file upload, DoS, buffer overflow, authentication bypass, etc) [10]	

Why do you think it is important to follow this vulnerability? [20]	

Vulnerability Two	
CVE Number (or other unique identifier) [5]	
CVSS Score [5]	
Product(s) Affected [5]	
Exploitation Vector (Local, Network, Remote) [5]	
Result(s) of successful exploitation (Remote code execution, file upload, DoS, buffer overflow, authentication bypass, etc) [10]	

Why do you think it is important to follow this vulnerability? [20]	