

ENPM685 Homework #2 – Vulnerability Scanning

Version 4.1 – January 19th 2022

Estimated time to complete this assignment: 2 hours.

Part 1 - Google Dorking/OSINT

1. Use your Google-Fu to find an interesting Google Dork that you feel discloses some kind of information that should not be public. A virtual high five and thumbs up if it's a University of Maryland site. (**site:umd.edu**)
2. Use your Google-Fu and OSINT-Fu to look up the following information about the University of Maryland, College Park.
 - Who is the CIO (Chief Information Officer) for UMD?
 - What is the CIO's email address?
 - Who is the CISO (Chief Information Security Officer) for UMD?
 - How many assistants does Dr. Pines, the UMD president, have?
 - What is the autonomous system number (ASN) for UMD? (If you find multiple ASNs provide the lowest number you find. It should be a low number.)

Answer these questions:

1. **What is the Google Dork search you used and URL that you found interesting? Why do you feel this is interesting/sharing some kind of information that should not be public?**
2. **A. Who is the CIO (Chief Information Officer) for UMD? How did you find the answer?**
B. What is the CIO's email address? How did you find the answer?
C. Who is the CISO (Chief Information Security Officer) for UMD? How did you find the answer?
D. How many assistants does Dr. Pines, the UMD president, have? How did you find the answer?
E. What is the autonomous system number (ASN) for UMD? How did you find the answer?

Part 2 - Vulnerability Assessment

1. Boot up your Ubuntu VM and your Kali VM
2. On your Kali VM set up a Nessus scan (Advanced Scan) and target your Ubuntu VM. (Refer to the Exercise document from this week if you need help remembering the steps.)
3. This time we are going to use a credentialed scan vs the un-credentials scan we ran before. We will provide a user name and password of a user who can login to the system and run elevate privileges with sudo so the scanner can run addition checks locally on the system being scanned to reduce false positives and check for vulnerabilities that you cannot scan for remotely.

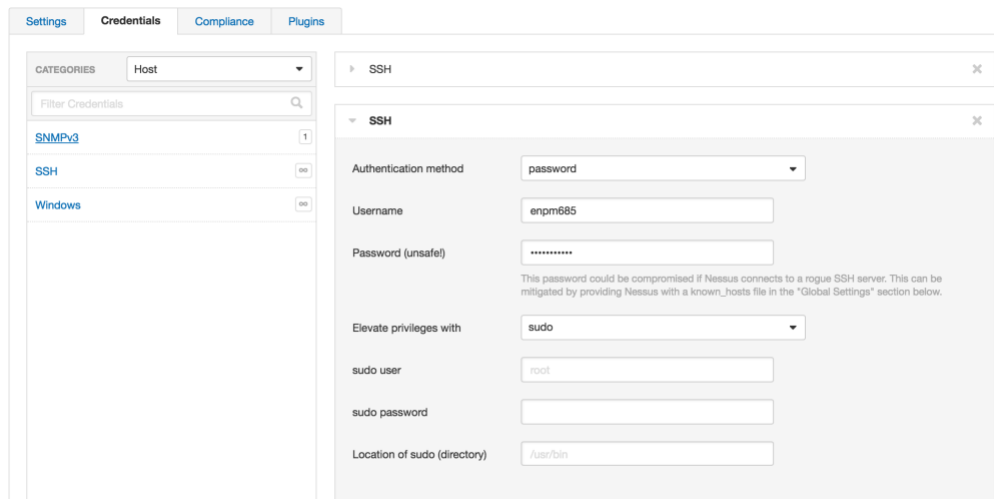
In the **Credentials** tab select “**SSH**” on the left side and then enter the information for the **enpm685** user on your Ubuntu VM.

Authentication method: **password**

Username: **enpm685**

Password: **password** (Unless you changed it, if you did enter what you changed it to)

Elevate privileges with: **sudo**



The screenshot shows the Nessus web interface with the 'Credentials' tab selected. On the left, under 'CATEGORIES', 'Host' is selected, and a list of credential types is shown: 'SNMPv3', 'SSH', and 'Windows'. The 'SSH' option is selected. The main panel displays the configuration for an SSH credential. The 'Authentication method' is set to 'password'. The 'Username' field contains 'enpm685'. The 'Password (unsafe)' field is masked with dots. Below the password field, a warning message states: 'This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.' The 'Elevate privileges with' dropdown is set to 'sudo'. Below this, the 'sudo user' field contains 'root', the 'sudo password' field is empty, and the 'Location of sudo (directory)' field contains '/usr/bin'.

4. Follow the rest of the steps to configure the scan and then run the scan.
5. Review the results and compare these results to the results from when you ran the uncredentialed scan in class.
6. Run and save an Executive Report (PDF) of the scan.

Answer these questions:

- 1. How many vulnerabilities did you detect? How was this different from the uncredentialed scan?**
- 2. Of the detected vulnerabilities which do you believe is the highest risk? Why?**

Deliverables:

Part 1: The answers to questions 1 and 2.

Part 2: The answers to questions 1 and 2 and a copy and a copy of the Executive Report in PDF format.