ENPM685 – Security Tools for Information Security

Section: 0101

Homework – 2

Name: Syed Mohammad Ibrahim

UID: *iamibi*

UID Number: 118428369

Email – *iamibi@umd.edu*

Part 1 - Google Dorking/OSINT

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?

A. Google Dork: site: umd.edu intitle:"chief information officer". This provided a recent announcement made by him for the university awareness on a ransomware attack. The post contained his credentials and signatures which can be misused by an attacker as part of social engineering attack(s) like phishing. This information should not be pushed out to public domain-space.

2.A. Who is the CIO (Chief Information Officer) for UMD? How did you find the answer?

A. Jeffrey K. Hollingsworth is the CIO for UMD. Google dork: site: umd.edu intitle:"chief information officer" gave a link to an announcement that was made by Jeffrey recently in which it had their credentials and signature.

2.B. What is the CIO's email address? How did you find the answer?

A. CIO's email is hollings@umd.edu. I google dorked: intext:"chief information officer" site: umd.edu, which gave me the leadership at UMD link. From there I found out who the CIO is, after which I google searched their name and voila, I got their email id.

2.C. Who is the CISO (Chief Information Security Officer) for UMD? How did you find the answer?

A. Gerry Sneeringer is the CISO of UMD. I used google dorking: intext:"information security officer" site: umd.edu which gave a link to the leadership at UMD.

2.D. How many assistants does Dr. Pines, the UMD president, have? How did you find the answer?

A. Dr. Pines have five assistants. Googling “dr pines umd administration staff” provided a URL to Dr. Pines profile information at UMD. At the bottom, there was a URL to the list of administration staff that are associated with him.

2.E. What is the autonomous system number (ASN) for UMD? How did you find the answer?

A. ASN for UMD is 27. Google Dork: site: umd.edu intext: "university of maryland" | intitle: "asn". This provided a url to a website which provided full list of ASN’s in the USA.

Part 2 - Vulnerability Assessment

1. How many vulnerabilities did you detect? How was this different from the uncredentialed scan?

A. A total of 77 vulnerabilities were detected in the credential scan by Nessus. The following table displays the difference between the number of vulnerabilities detected by Nessus for different configurations:

Severity⇩	Credentialed Scan	Uncredentialed Scan
Critical	1	0
High	1	0
Medium	7	2
Low	1	1
Info	67	42

2. Of the detected vulnerabilities which do you believe is the highest risk? Why?

A. SaltStack vulnerability is at highest risk since the severity of it is critical and there are multiple vulnerabilities reported in that same SaltStack version like Salt-API’s SSH is prone to SQL injection and eAuth mechanism related issues. More details can be found here: https://www.tenable.com/plugins/nessus/148112