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

Target Scan with Creds

Report generated by Nessus™ Fri, 18 Feb 2022 21:02:27 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.81.131

Vulnerabilities Total: 77

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	148112	SaltStack < 3002.5 Multiple Vulnerabilities
HIGH	7.5	154852	SaltStack 3000.x < 3001.8 / 3002.x < 3002.7 / 3003.x < 3003.3 Multiple Vulnerabilities
MEDIUM	6.7	157353	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5267-1)
MEDIUM	6.6	156327	Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	157843	Ubuntu 20.04 LTS : util-linux vulnerabilities (USN-5279-1)
MEDIUM	5.9	156183	Apache Log4j 2.x < 2.17.0 DoS
MEDIUM	4.7	157356	Ubuntu 18.04 LTS / 20.04 LTS / 21.10 : MySQL vulnerabilities (USN-5270-1)
MEDIUM	N/A	57582	SSL Self-Signed Certificate
LOW	N/A	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	142640	Apache HTTP Server Site Enumeration
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	156000	Apache Log4j Installed (Linux / Unix)
INFO	N/A	34098	BIOS Info (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)

INFO	N/A	55472	Device Hostname
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	33276	Enumerate MAC Addresses via SSH
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	147817	Java Detection and Identification (Linux / Unix)
INFO	N/A	130595	Jenkins Installed (Linux)
INFO	N/A	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	95928	Linux User List Enumeration
INFO	N/A	65914	MongoDB Detection
INFO	N/A	129468	MySQL Server Installed (Linux)
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	64582	Netstat Connection Information
INFO	N/A	14272	Netstat Portscanner (SSH)
INFO	N/A	11936	OS Identification
INFO	N/A	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	117887	OS Security Patch Assessment Available
INFO	N/A	148373	OpenJDK Java Detection (Linux / Unix)

INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	102094	SSH Commands Require Privilege Escalation
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	90707	SSH SCP Protocol Detection
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	62563	SSL Compression Methods Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	136734	SaltStack Salt Master Detection
INFO	N/A	136355	SaltStack Salt Master Installed (Linux)
INFO	N/A	22964	Service Detection
INFO	N/A	22869	Software Enumeration (SSH)
INFO	N/A	49069	Splunk Management API Detection
INFO	N/A	47619	Splunk Web Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	110385	Target Credential Issues by Authentication Protocol - Insufficient Privilege
INFO	N/A	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided

INFO	N/A	56468	Time of Last System Startup
INFO	N/A	10287	Traceroute Information
INFO	N/A	157458	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel regression (USN-5267-2)
INFO	N/A	110483	Unix / Linux Running Processes Information
INFO	N/A	152743	Unix Software Discovery Commands Not Available
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	52703	vsftpd Detection

Target Scan without Creds

Report generated by Nessus™ Fri, 18 Feb 2022 21:33:36 EST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.81.131

Vulnerabilities Total: 45

SEVERITY	CVSS V3.0	PLUGIN	NAME
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	N/A	57582	SSL Self-Signed Certificate
LOW	N/A	62565	Transport Layer Security (TLS) Protocol CRIME Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	65914	MongoDB Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	62563	SSL Compression Methods Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	136734	SaltStack Salt Master Detection
INFO	N/A	22964	Service Detection
INFO	N/A	49069	Splunk Management API Detection
INFO	N/A	47619	Splunk Web Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10302	Web Server robots.txt Information Disclosure

INFO	N/A	52703	vsftpd Detection