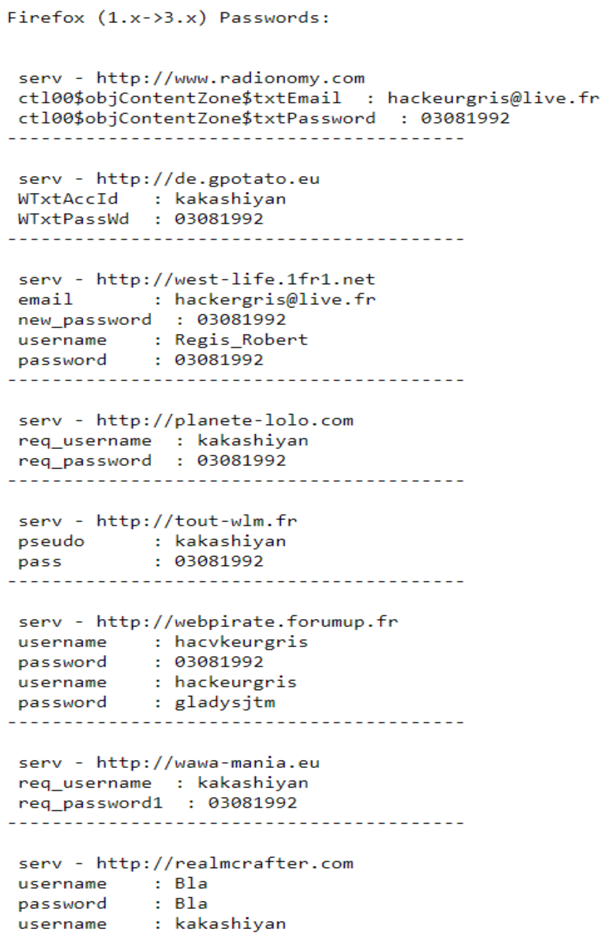
ENPM685 Homework #2 – Vulnerability Scanning

Name: Suprajha Kanna
UID: 118406473
Email: skanna@umd.edu

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.
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?

Query: *filetype:log intext:password intext:(@gmail.com | @yahoo.com | @hotmail.com)*
URL the information was found: http://remikaing.free.fr/HACKEURGRIS-mutXC:%5CUsers%5CYANNBA~1%5CAppData%5CLocal%5CTemp%5Ctemp.log
Explanation: This query returns log files that contains passwords and their corresponding emails. The screenshot is displayed as below having server name, Id and password. Sensitive information like server name along with password possess biggest risks and should not be exposed with the public. Using this information, the attacker can login with the credentials and gain user privileges to access the user personal and confidential information.

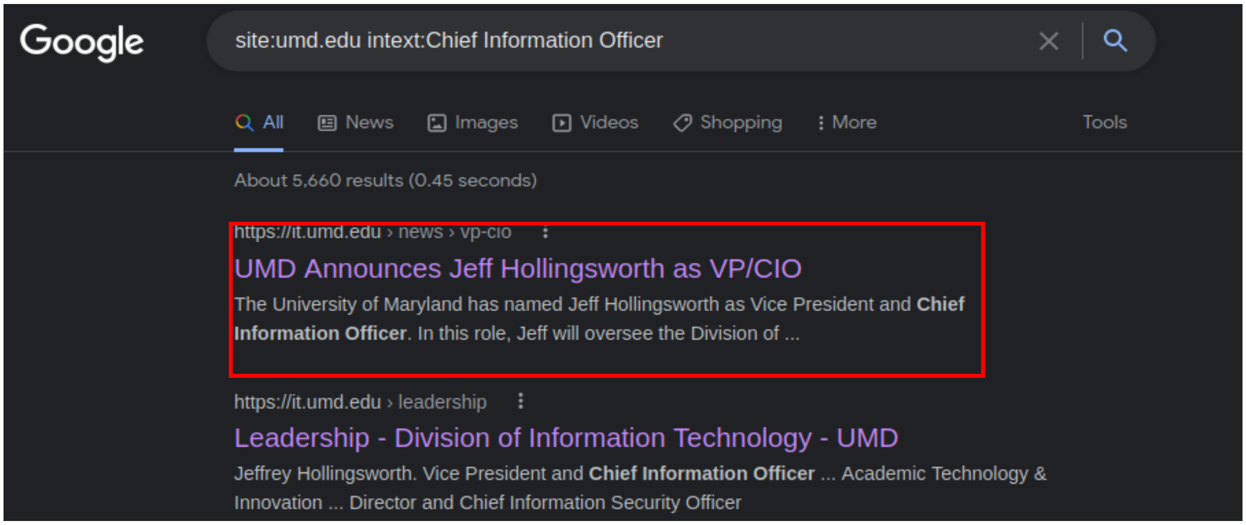


```
Firefox (1.x->3.x) Passwords:


 serv - http://www.radionomy.com
 ctl00$objContentZone$txtEmail   : hackeurgris@live.fr
 ctl00$objContentZone$txtPassword  : 03081992
-----------------------------------------

 serv - http://de.gpotato.eu
 WTxtAccId    : kakashiyan
 WTxtPassWd   : 03081992
-----------------------------------------

 serv - http://west-life.1fr1.net
 email        : hackergris@live.fr
 new_password  : 03081992
 username     : Regis_Robert
 password     : 03081992
-----------------------------------------

 serv - http://planete-lolo.com
 req_username  : kakashiyan
 req_password  : 03081992
-----------------------------------------

 serv - http://tout-wlm.fr
 pseudo       : kakashiyan
 pass         : 03081992
-----------------------------------------

 serv - http://webpirate.forumup.fr
 username     : hacvkeurgris
 password     : 03081992
 username     : hackeurgris
 password     : gladysjtm
-----------------------------------------

 serv - http://wawa-mania.eu
 req_username  : kakashiyan
 req_password1  : 03081992
-----------------------------------------

 serv - http://realmcrafter.com
 username     : Bla
 password     : Bla
 username     : kakashiyan
```

2. Use your Google-Fu and OSINT-Fu to look up the following information about the University of Maryland, College Park.

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

Query: *site: umd.edu intext: Chief Information Officer*
Result: The Chief Information Officer for UMD is Jeffrey Hollingsworth.
The query was run for the University of Maryland website 'umd.edu' that searches for text 'Chief Information Officer' for the university which displays the following result. Also, when the website was clicked, it contained information about the CIO.



site:umd.edu intext:Chief Information Officer

About 5,660 results (0.45 seconds)

https://it.umd.edu › news › vp-cio

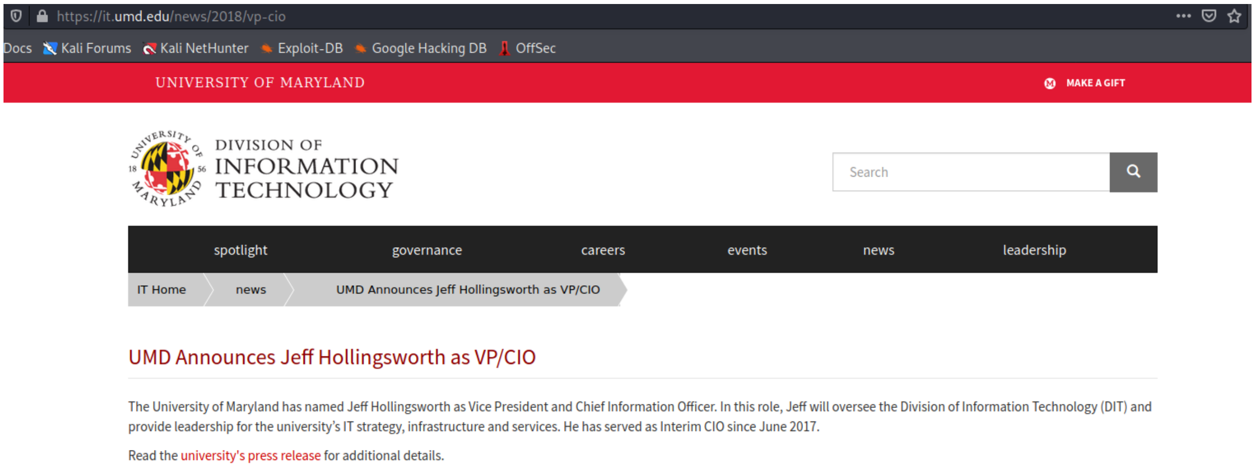
UMD Announces Jeff Hollingsworth as VP/CIO

The University of Maryland has named Jeff Hollingsworth as Vice President and **Chief Information Officer**. In this role, Jeff will oversee the Division of ...

https://it.umd.edu › leadership

Leadership - Division of Information Technology - UMD

Jeffrey Hollingsworth. Vice President and **Chief Information Officer** ... Academic Technology & Innovation ... Director and Chief Information Security Officer



UMD Announces Jeff Hollingsworth as VP/CIO

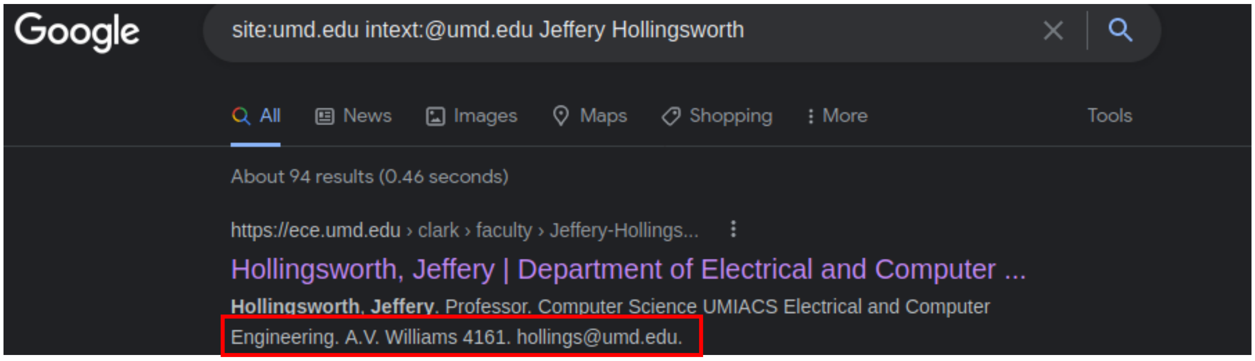
The University of Maryland has named Jeff Hollingsworth as Vice President and Chief Information Officer. In this role, Jeff will oversee the Division of Information Technology (DIT) and provide leadership for the university's IT strategy, infrastructure and services. He has served as Interim CIO since June 2017.

Read the university's press release for additional details.

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

Query: *site: umd.edu intext: @umd.edu Jeffery Hollingsworth*

Result: hollings@umd.edu
To access the E-mail ID of the CIO, a search query for '@umd.edu' (UMD email domain) along with the CIO name was entered. The below image displays the result given person name along with his email address information. Inside the website, the faculty directory displays the CIO's basic details (like name, department, Email address, contact information etc.,).



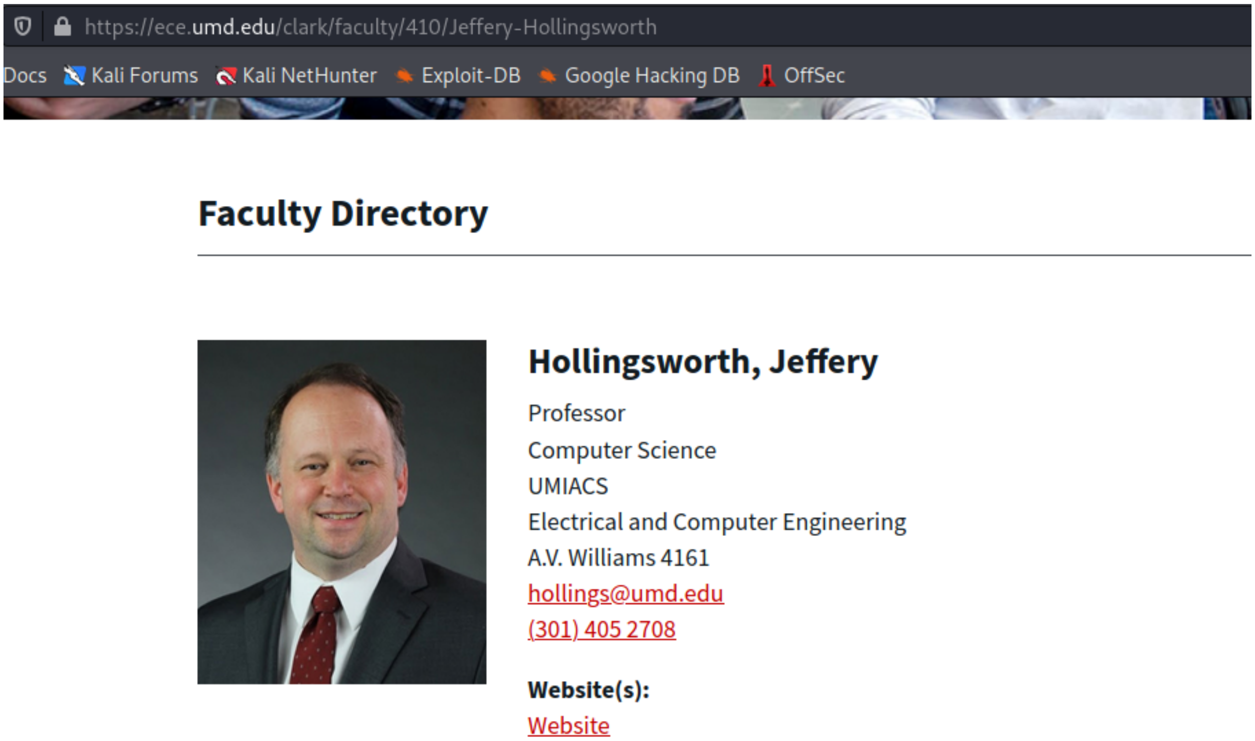
site:umd.edu intext:@umd.edu Jeffery Hollingsworth

About 94 results (0.46 seconds)

https://ece.umd.edu › clark › faculty › Jeffery-Hollings...

Hollingsworth, Jeffery | Department of Electrical and Computer ...

Hollingsworth, Jeffery. Professor. Computer Science UMIACS Electrical and Computer Engineering. A.V. Williams 4161. hollings@umd.edu.



https://ece.umd.edu/clark/faculty/410/Jeffery-Hollingsworth

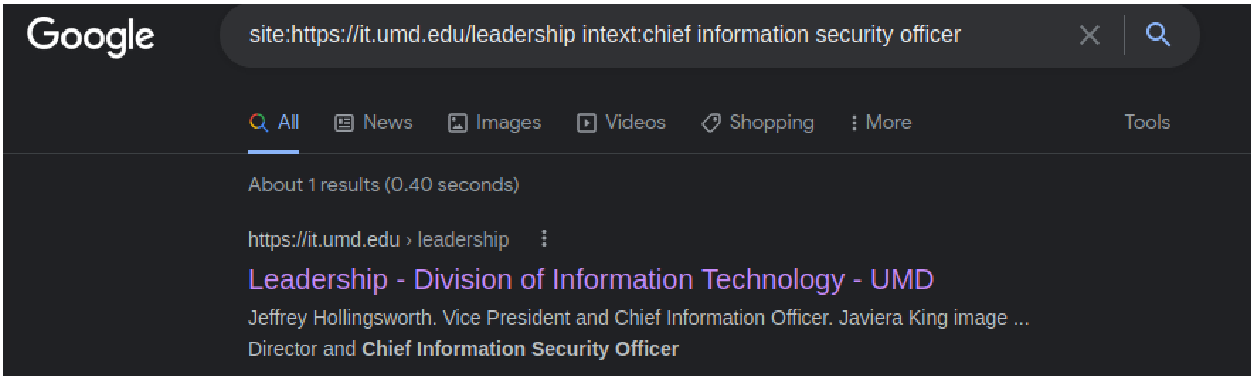
Faculty Directory

Hollingsworth, Jeffery

Professor
Computer Science
UMIACS
Electrical and Computer Engineering
A.V. Williams 4161
hollings@umd.edu
(301) 405 2708

Website(s):
Website

C. Who is the CISO (Chief Information Security Officer) for UMD? How did you find the answer?
Query: *site: umd.edu intext: Chief Information Security Officer*
Result: The Chief Information Officer for UMD is Gerry Sneeringer.
The query was run for the University of Maryland website 'umd.edu' that searches for text 'Chief Information Security Officer' for the university which displays the following result. Also, when the website was clicked, it contained information about the CISO.



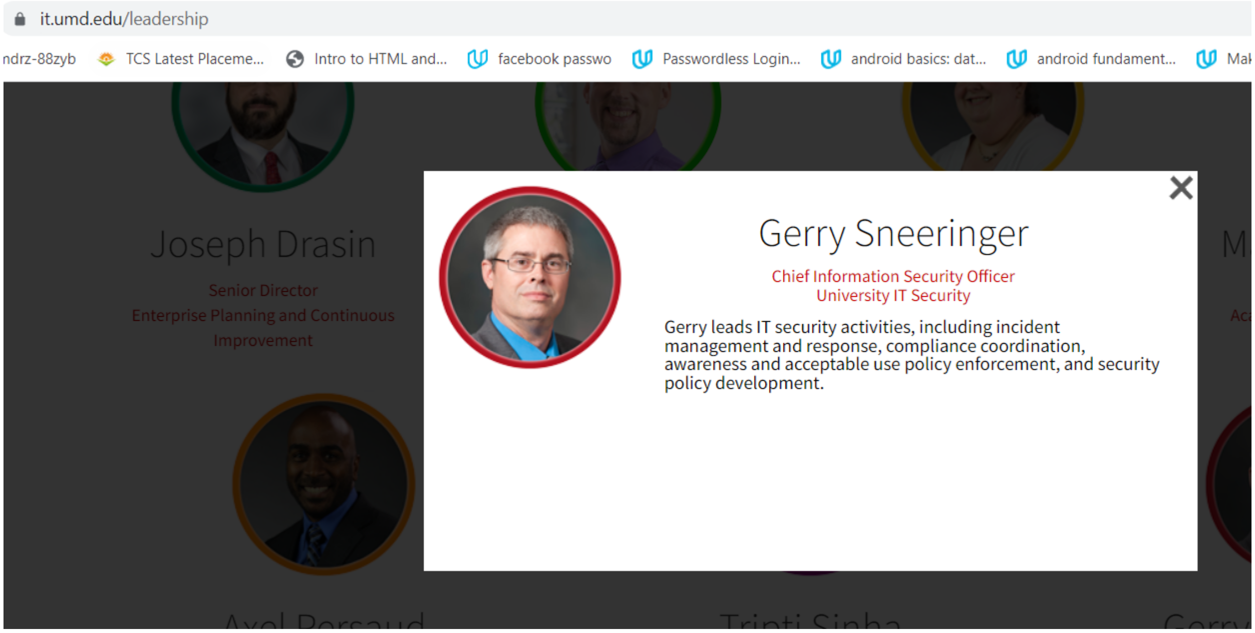
site:https://it.umd.edu/leadership intext:chief information security officer

About 1 results (0.40 seconds)

https://it.umd.edu › leadership

Leadership - Division of Information Technology - UMD

Jeffrey Hollingsworth. Vice President and Chief Information Officer. Javiera King image ... Director and **Chief Information Security Officer**



Joseph Drasin

Senior Director
Enterprise Planning and Continuous Improvement

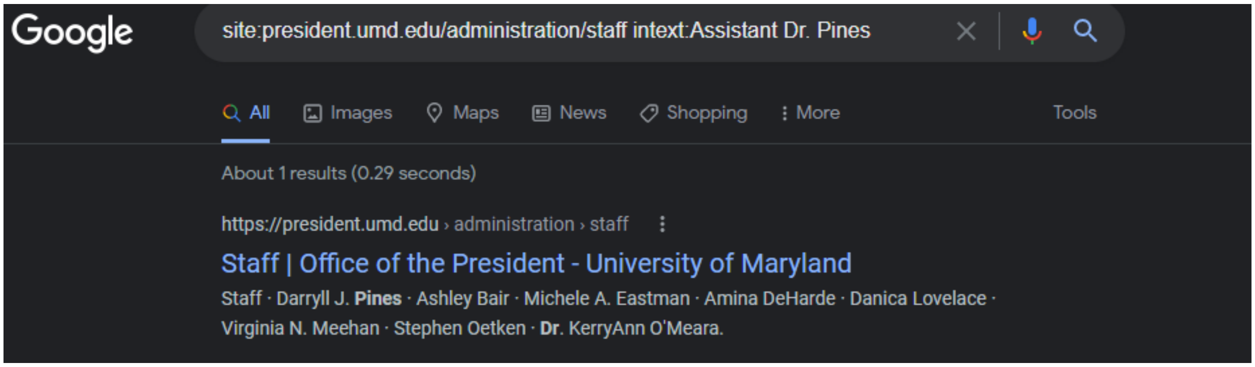
Gerry Sneeringer

Chief Information Security Officer
University IT Security

Gerry leads IT security activities, including incident management and response, compliance coordination, awareness and acceptable use policy enforcement, and security policy development.

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

The search query containing ‘assistant’ for Dr. Pines was run for the website ‘umd.edu’ which displays the following result. There are 5 assistants profiles to the President listed when we click the website as displayed in the second image.



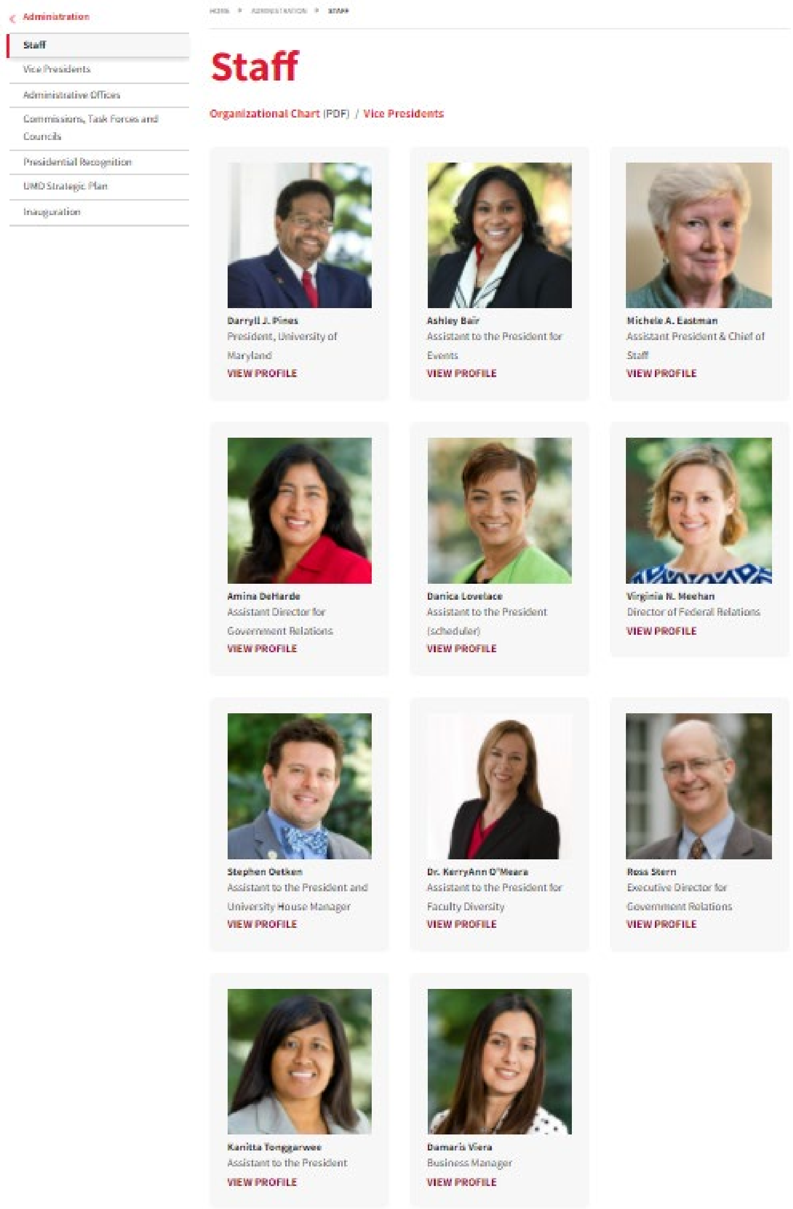
site:president.umd.edu/administration/staff intext:Assistant Dr. Pines

About 1 results (0.29 seconds)

https://president.umd.edu › administration › staff

Staff | Office of the President - University of Maryland

Staff · Darryll J. **Pines** · Ashley Bair · Michele A. Eastman · Amina DeHarde · Danica Lovelace · Virginia N. Meehan · Stephen Oetken · **Dr.** KerryAnn O'Meara.



HOME > ADMINISTRATION > STAFF

< Administration

- Staff
- Vice Presidents
- Administrative Offices
- Commissions, Task Forces and Councils
- Presidential Recognition
- UMD Strategic Plan
- Inauguration

Staff

Organizational Chart (PDF) / Vice Presidents

Darryll J. Pines
President, University of Maryland
VIEW PROFILE

Ashley Bair
Assistant to the President for Events
VIEW PROFILE

Michele A. Eastman
Assistant President & Chief of Staff
VIEW PROFILE

Amina DeHarde
Assistant Director for Government Relations
VIEW PROFILE

Danica Lovelace
Assistant to the President (scheduler)
VIEW PROFILE

Virginia N. Meehan
Director of Federal Relations
VIEW PROFILE

Stephen Oetken
Assistant to the President and University House Manager
VIEW PROFILE

Dr. KerryAnn O'Meara
Assistant to the President for Faculty Diversity
VIEW PROFILE

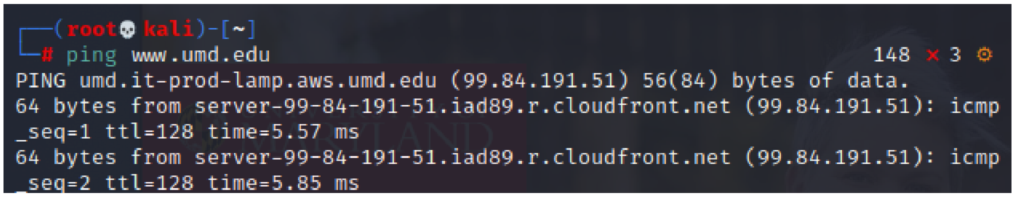
Ross Stern
Executive Director for Government Relations
VIEW PROFILE

Kanitta Tonggarwee
Assistant to the President
VIEW PROFILE

Damaris Viera
Business Manager
VIEW PROFILE

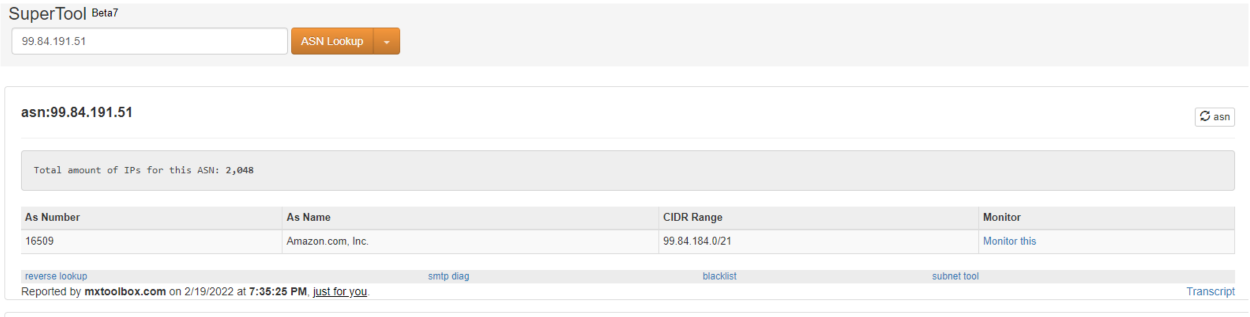
E. What is the autonomous system number (ASN) for UMD? How did you find the answer?

While performing PING on www.umd.edu, the following IP address is displayed 99.84.191.51.



```
┌──(root💀kali)-[~]
└─# ping www.umd.edu                                               148 ✕ 3 ⚙
PING umd.it-prod-lamp.aws.umd.edu (99.84.191.51) 56(84) bytes of data.
64 bytes from server-99-84-191-51.iad89.r.cloudfront.net (99.84.191.51): icmp
_seq=1 ttl=128 time=5.57 ms
64 bytes from server-99-84-191-51.iad89.r.cloudfront.net (99.84.191.51): icmp
_seq=2 ttl=128 time=5.85 ms
```

Using MX tool, the ASN option is selected, and the IP address is entered.
Total amount of IPs for this ASN: 16509
In the above picture you can see here AS Name - amazon.com is visible (amazon.com provides cloud service here which is a third party).



asn:99.84.191.51

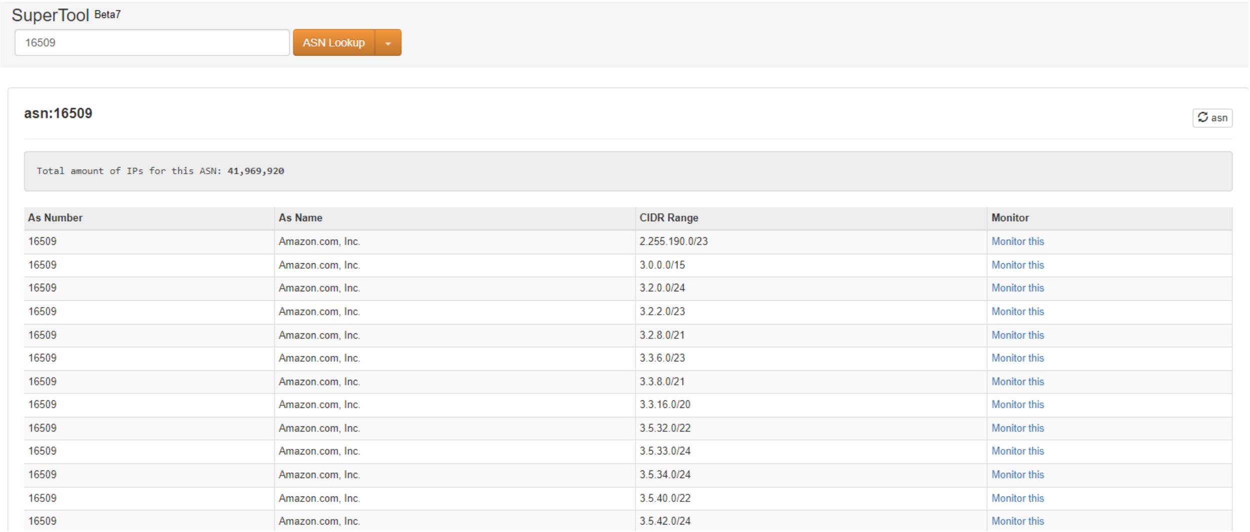
```
Total amount of IPs for this ASN: 2,048
```

As Number	As Name	CIDR Range	Monitor
16509	Amazon.com, Inc.	99.84.184.0/21	Monitor this

reverse lookup smtp diag blacklist subnet tool

Reported by **mxtoolbox.com** on 2/19/2022 at **7:35:25 PM**, just for you. Transcript

When ASN lookup is performed for the total ASN found, the below IP address ranges are displayed.

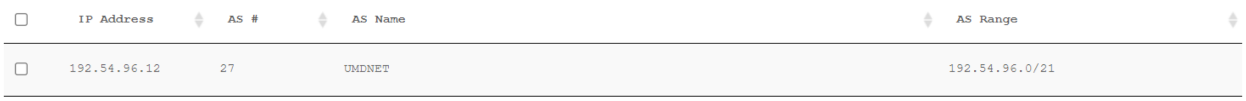


asn:16509

```
Total amount of IPs for this ASN: 41,969,920
```

As Number	As Name	CIDR Range	Monitor
16509	Amazon.com, Inc.	2.255.190.0/23	Monitor this
16509	Amazon.com, Inc.	3.0.0.0/15	Monitor this
16509	Amazon.com, Inc.	3.2.0.0/24	Monitor this
16509	Amazon.com, Inc.	3.2.2.0/23	Monitor this
16509	Amazon.com, Inc.	3.2.8.0/21	Monitor this
16509	Amazon.com, Inc.	3.3.6.0/23	Monitor this
16509	Amazon.com, Inc.	3.3.8.0/21	Monitor this
16509	Amazon.com, Inc.	3.3.16.0/20	Monitor this
16509	Amazon.com, Inc.	3.5.32.0/22	Monitor this
16509	Amazon.com, Inc.	3.5.33.0/24	Monitor this
16509	Amazon.com, Inc.	3.5.34.0/24	Monitor this
16509	Amazon.com, Inc.	3.5.40.0/22	Monitor this
16509	Amazon.com, Inc.	3.5.42.0/24	Monitor this

The lowest ASN number was found as 27.

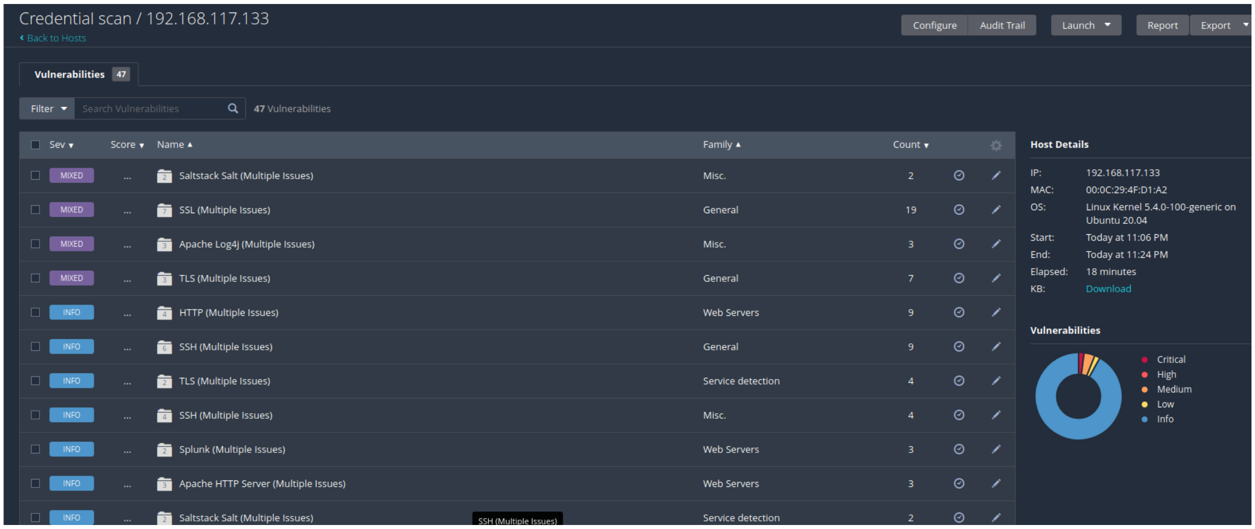


□	IP Address	AS #	AS Name	AS Range
□	192.54.96.12	27	UMDNET	192.54.96.0/21

Part 2 - Vulnerability Assessment

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

   There are 31 vulnerabilities in uncredentialed scan and 47 vulnerabilities in credential scan for Ubuntu machine.
   It was found that credential scan happens to identify all vulnerabilities existing on the machine rather than uncredential scan.



Credential scan / 192.168.117.133

‹ Back to Hosts

47 Vulnerabilities

Sev	Score	Name	Family	Count
MIXED	...	Saltstack Salt (Multiple Issues)	Misc.	2
MIXED	...	SSL (Multiple Issues)	General	19
MIXED	...	Apache Log4j (Multiple Issues)	Misc.	3
MIXED	...	TLS (Multiple Issues)	General	7
INFO	...	HTTP (Multiple Issues)	Web Servers	9
INFO	...	SSH (Multiple Issues)	General	9
INFO	...	TLS (Multiple Issues)	Service detection	4
INFO	...	SSH (Multiple Issues)	Misc.	4
INFO	...	Splunk (Multiple Issues)	Web Servers	3
INFO	...	Apache HTTP Server (Multiple Issues)	Web Servers	3
INFO	...	Saltstack Salt (Multiple Issues)	Service detection	2

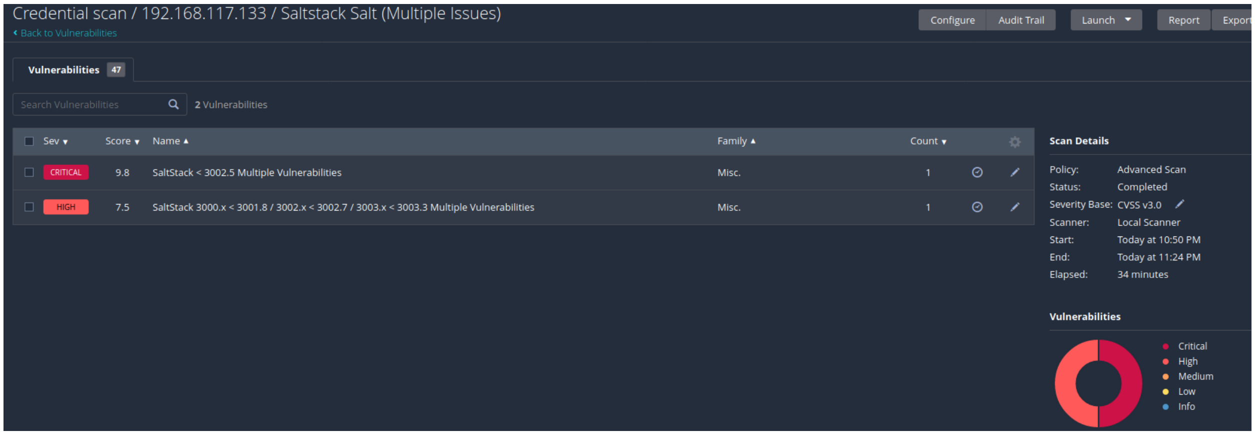
SSH (Multiple Issues)

Host Details

IP:	192.168.117.133
MAC:	00:0C:29:4F:D1:A2
OS:	Linux Kernel 5.4.0-100-generic on Ubuntu 20.04
Start:	Today at 11:06 PM
End:	Today at 11:24 PM
Elapsed:	18 minutes
KB:	Download

Vulnerabilities

Credential Scan 1



Credential scan / 192.168.117.133 / Saltstack Salt (Multiple Issues)

‹ Back to Vulnerabilities

2 Vulnerabilities

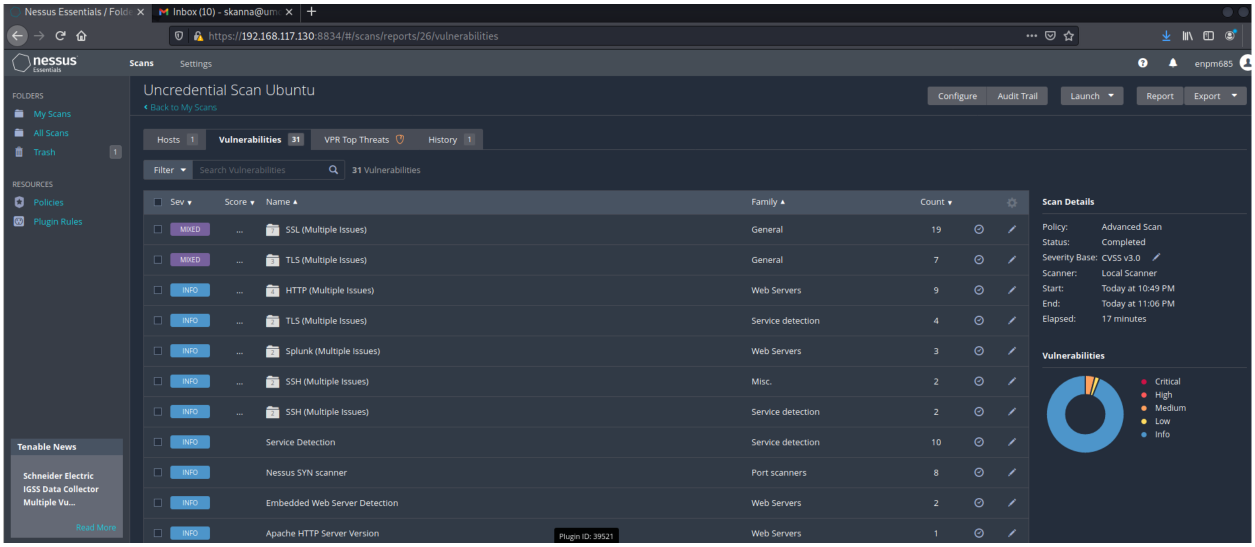
Sev	Score	Name	Family	Count
CRITICAL	9.8	SaltStack < 3002.5 Multiple Vulnerabilities	Misc.	1
HIGH	7.5	SaltStack 3000.x < 3001.8 / 3002.x < 3002.7 / 3003.x < 3003.3 Multiple Vulnerabilities	Misc.	1

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:50 PM
End:	Today at 11:24 PM
Elapsed:	34 minutes

Vulnerabilities

Credential Scan 2



https://192.168.117.130:8834/#/scans/reports/26/vulnerabilities

Schneider Electric IGSS Data Collector Multiple Vu...

Uncredential Scan Ubuntu

‹ Back to My Scans

31 Vulnerabilities

Sev	Score	Name	Family	Count
MIXED	...	SSL (Multiple Issues)	General	19
MIXED	...	TLS (Multiple Issues)	General	7
INFO	...	HTTP (Multiple Issues)	Web Servers	9
INFO	...	TLS (Multiple Issues)	Service detection	4
INFO	...	Splunk (Multiple Issues)	Web Servers	3
INFO	...	SSH (Multiple Issues)	Misc.	2
INFO	...	SSH (Multiple Issues)	Service detection	2
INFO		Service Detection	Service detection	10
INFO		Nessus SYN scanner	Port scanners	8
INFO		Embedded Web Server Detection	Web Servers	2
INFO		Apache HTTP Server Version	Web Servers	1

Plugin ID: 39521

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:49 PM
End:	Today at 11:06 PM
Elapsed:	17 minutes

Vulnerabilities

Uncredentialed Scan

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

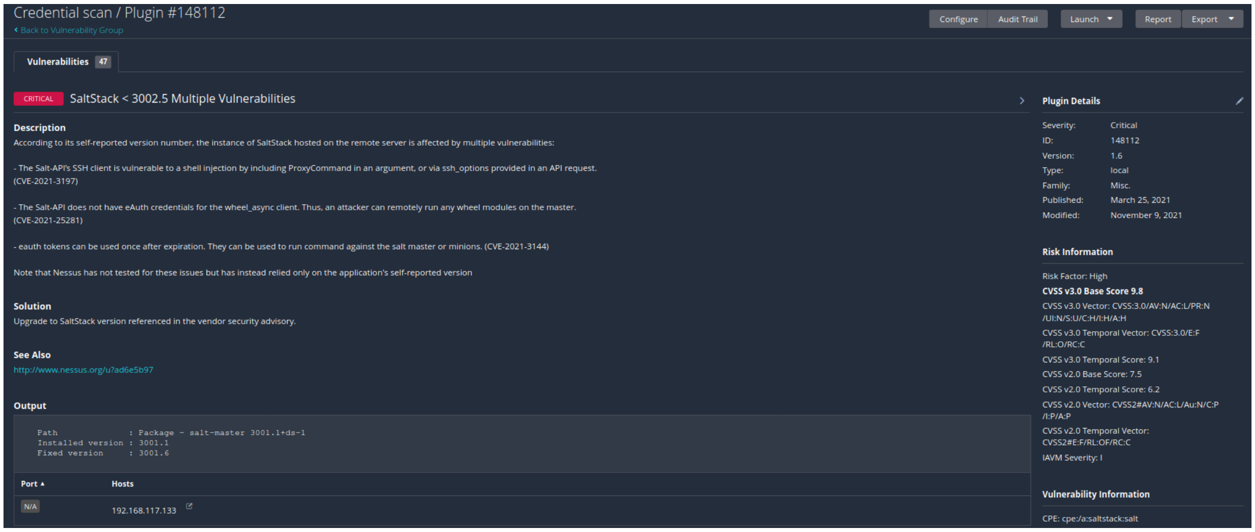
One critical vulnerability was identified to be the “SaltStack”

Description: According to its self-reported version number, the instance of SaltStack hosted on the remote server is affected by multiple vulnerabilities:

- The Salt-API's SSH client is vulnerable to a shell injection by including ProxyCommand in an argument, or via ssh_options provided in an API request. (CVE-2021-3197)
- The Salt-API does not have eAuth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master. (CVE-2021-25281)
- eauth tokens can be used once after expiration. They can be used to run command against the salt master or minions. (CVE-2021-3144)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version.

Solution: To upgrade the SaltStack version referenced in the vendor security advisory.



Credential scan / Plugin #148112

SaltStack < 3002.5 Multiple Vulnerabilities

Description

According to its self-reported version number, the instance of SaltStack hosted on the remote server is affected by multiple vulnerabilities:

- The Salt-API's SSH client is vulnerable to a shell injection by including ProxyCommand in an argument, or via ssh_options provided in an API request. (CVE-2021-3197)

- The Salt-API does not have eAuth credentials for the wheel_async client. Thus, an attacker can remotely run any wheel modules on the master. (CVE-2021-25281)

- eauth tokens can be used once after expiration. They can be used to run command against the salt master or minions. (CVE-2021-3144)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version

Solution

Upgrade to SaltStack version referenced in the vendor security advisory.

See Also

http://www.nessus.org/u?ad6e5b97

Output

```
  Path              : Package - salt-master 3001.1+ds-1
  Installed version : 3001.1
  Fixed version     : 3001.6
```

Port ▲	Hosts
N/A	192.168.117.133

Plugin Details

Severity:	Critical
ID:	148112
Version:	1.6
Type:	local
Family:	Misc.
Published:	March 25, 2021
Modified:	November 9, 2021

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:F/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.1
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 6.2
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:saltstack:salt