Lab 2: Open-Source Intelligence (Passive Recon)

Grand Canyon University

CYB-610-O500 Penetration Testing and Risk Management

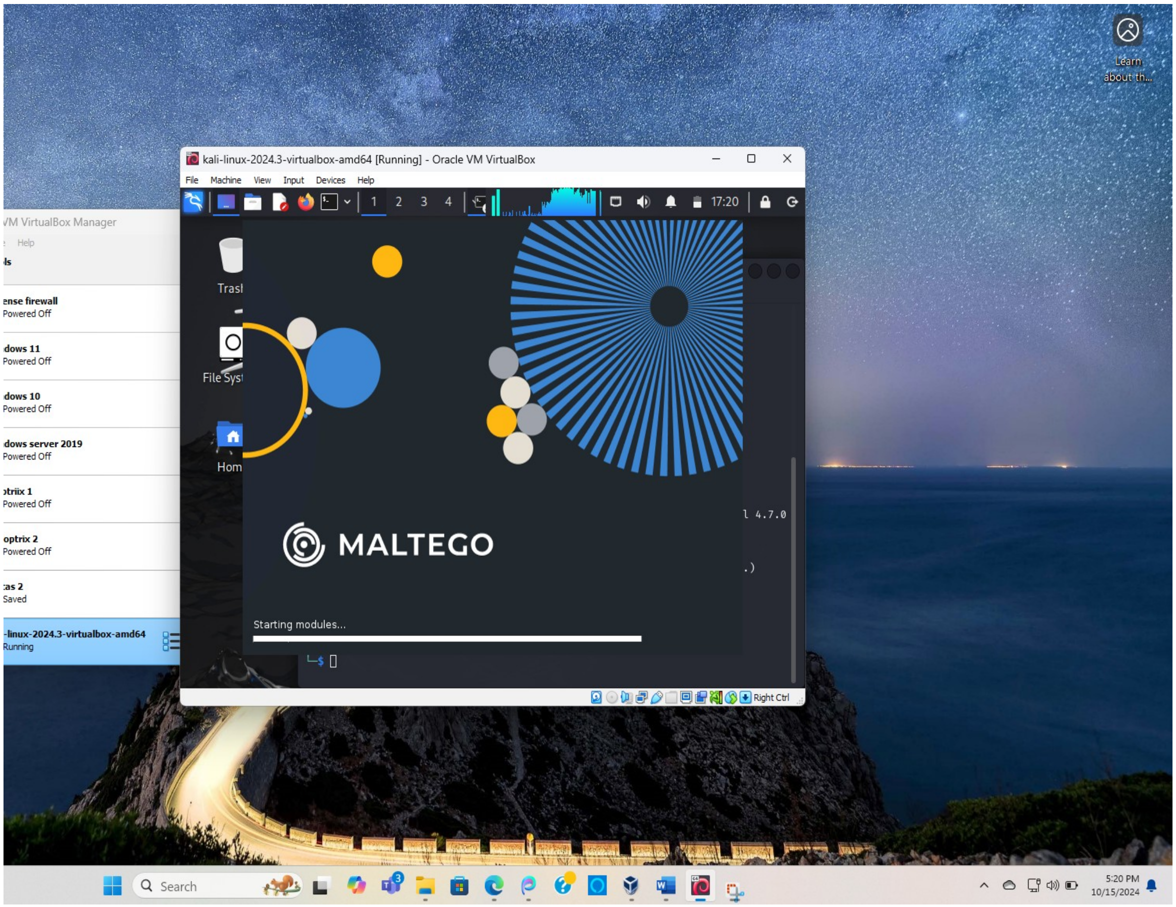
Professor, Luis Pina

October 16th, 2024

YouTube: https://youtu.be/uIEu4hCkSVQ

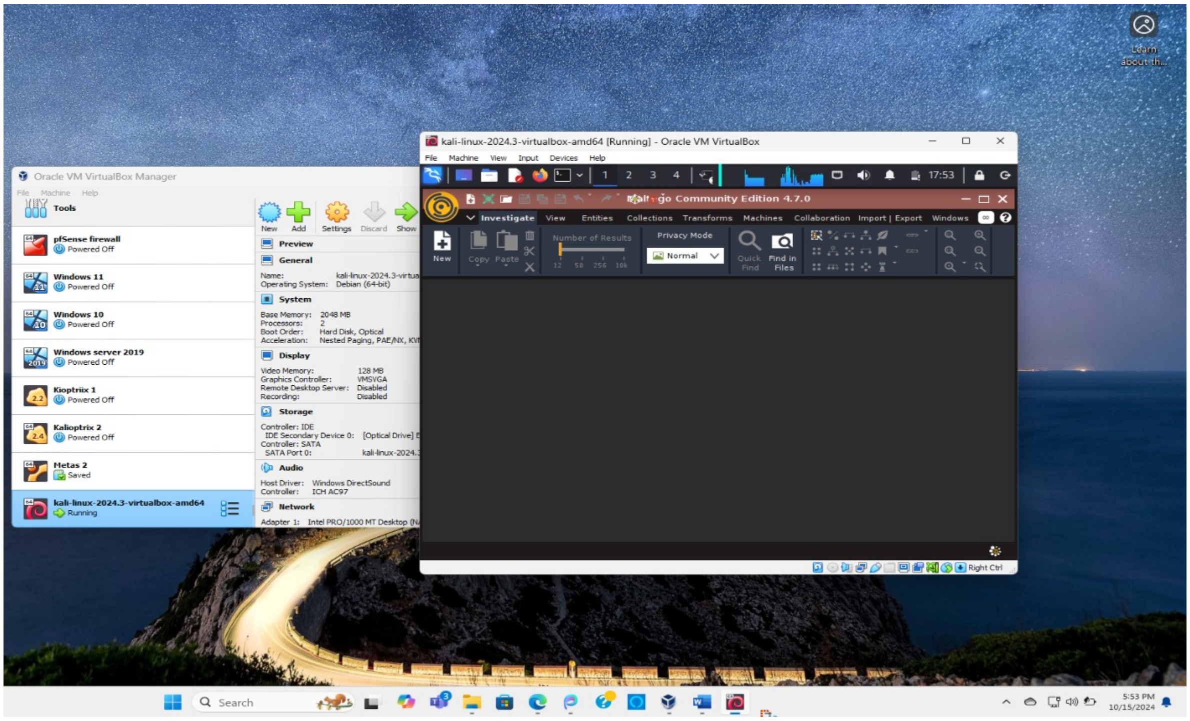
For the assignment, I chose Target as the fortune 500 company to extract passive data. To achieve this, I first had to make sure that my Kali Linux was connected to the internet. Once confirmed, I proceeded to download and register with Maltego, to be used within Kali Linux for part of the recon.

Installation of Maltego



Starting modules...

I ran the free version of Maltego (CE) and went through the installation process which was self-explanatory.


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Maltego Community Edition 4.7.0
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows
New Copy Paste Number of Results Privacy Mode Normal Quick Find Find in Files
Right Ctrl
Search
5:53 PM
10/15/2024

pfSense firewall
Powered Off

Windows 11
Powered Off

Windows 10
Powered Off

Windows server 2019
Powered Off

Kioptriix 1
Powered Off

Kalioptrix 2
Powered Off

Metas 2
Saved

kali-linux-2024.3-virtualbox-amd64
Running

Preview

General

Name: kali-linux-2024.3-virtua
Operating System: Debian (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KV

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] E
Controller: SATA
SATA Port 0: kali-linux-2024.3

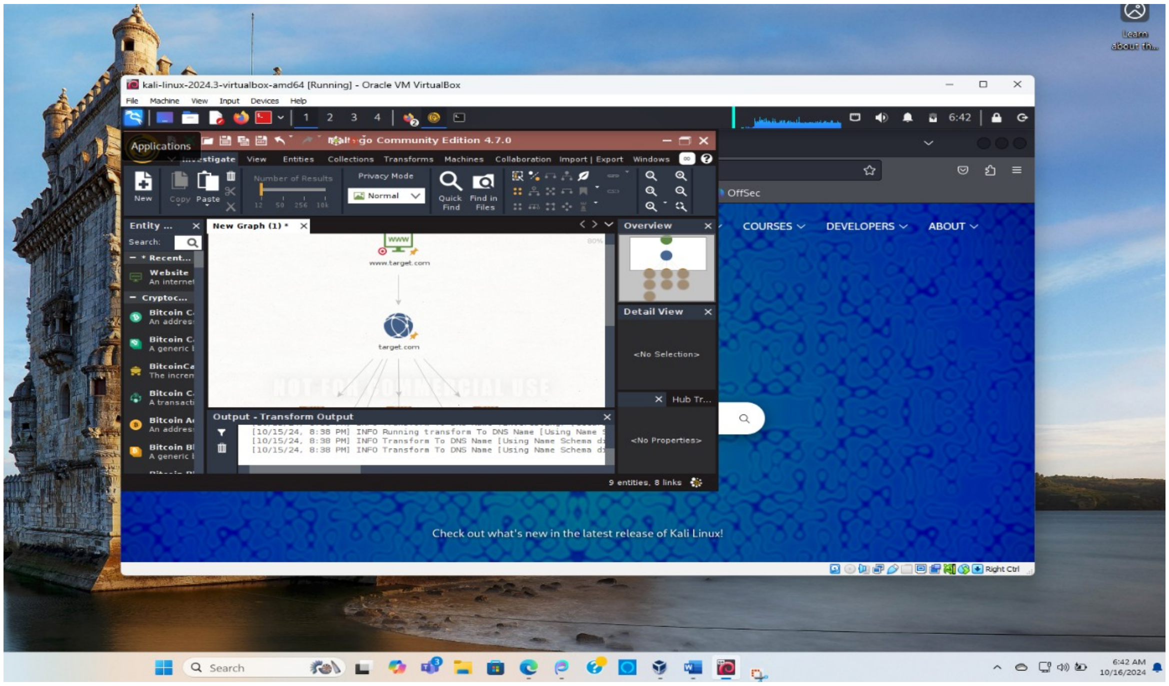
Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (N

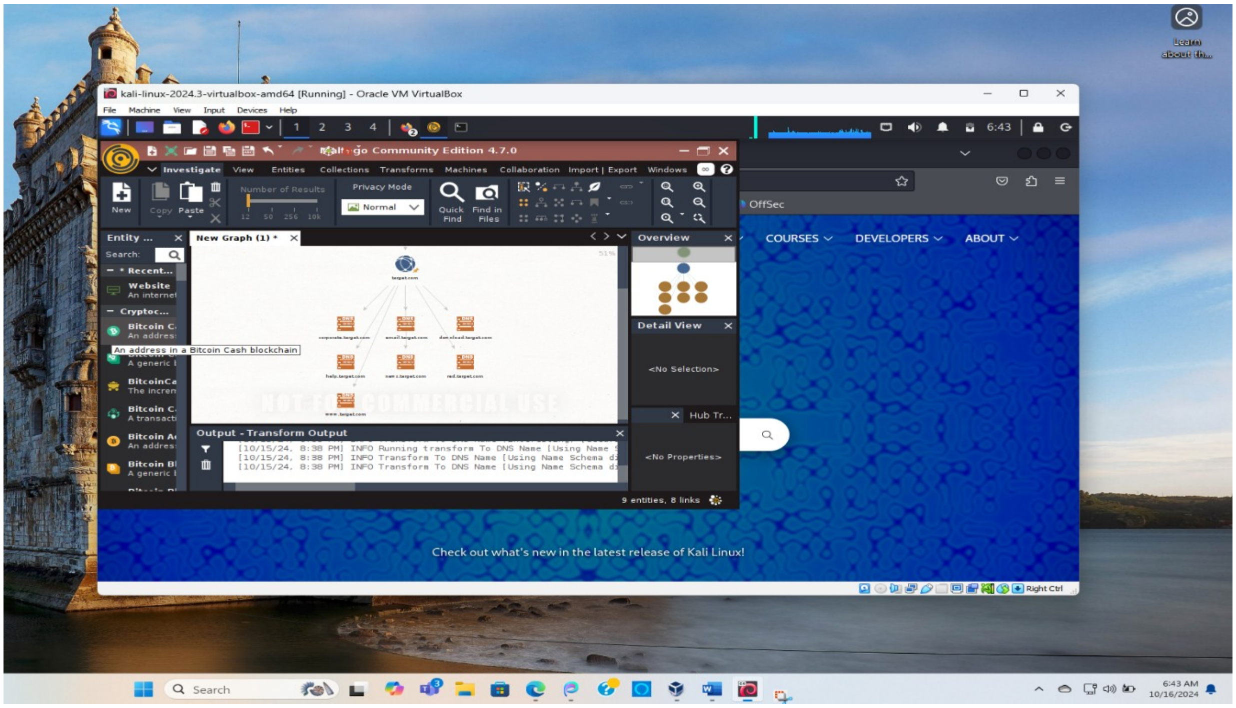
To start the passive recon, I clicked on “new”, and a blank graph screen came up. I then scrolled from the left side under “entity component palette” and clicked on website.



Output - Transform Output

```
[10/15/24, 8:38 PM] INFO Running transform To DNS Name [Using Name S
[10/15/24, 8:38 PM] INFO Transform To DNS Name [Using Name Schema di
[10/15/24, 8:38 PM] INFO Transform To DNS Name [Using Name Schema di
```

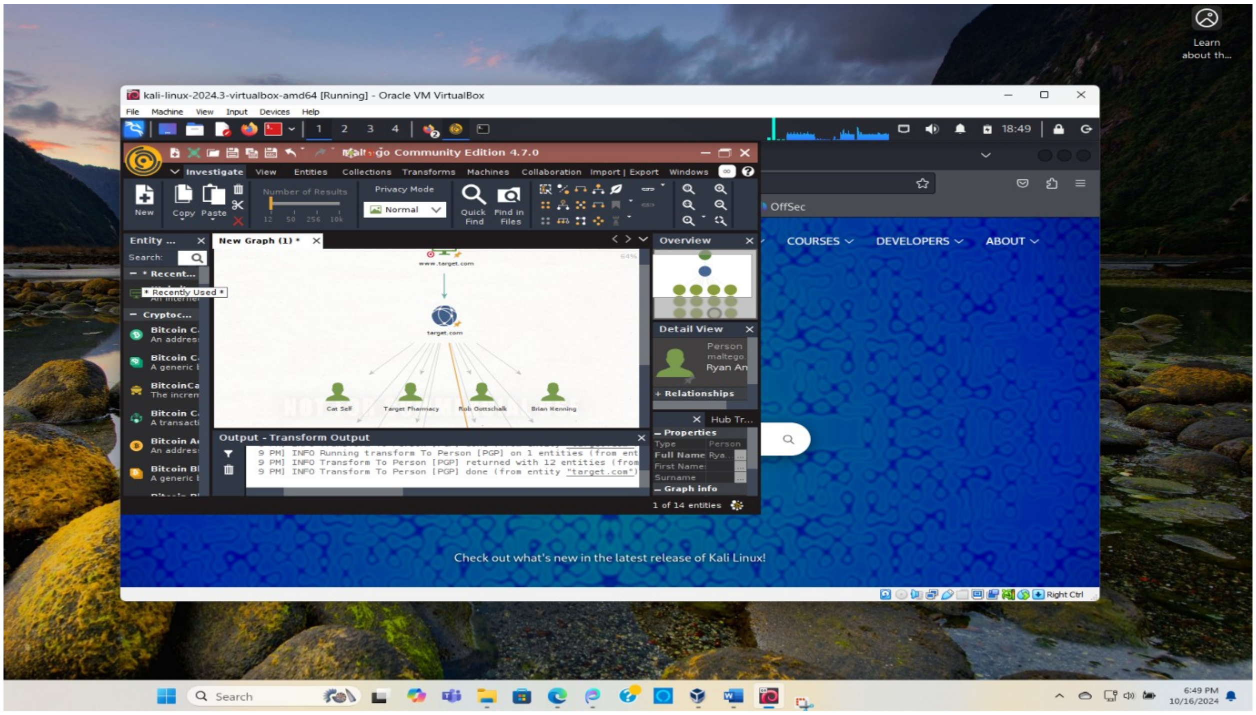
I dragged the website into the graph and changed the address to "www.target.com" then clicked on "ok" and searched by DNS. The results were returned with 7 entities.



Output - Transform Output

```
[10/15/24, 8:38 PM] INFO Running transform To DNS Name [Using Name S
[10/15/24, 8:38 PM] INFO Transform To DNS Name [Using Name Schema di
[10/15/24, 8:38 PM] INFO Transform To DNS Name [Using Name Schema di
```

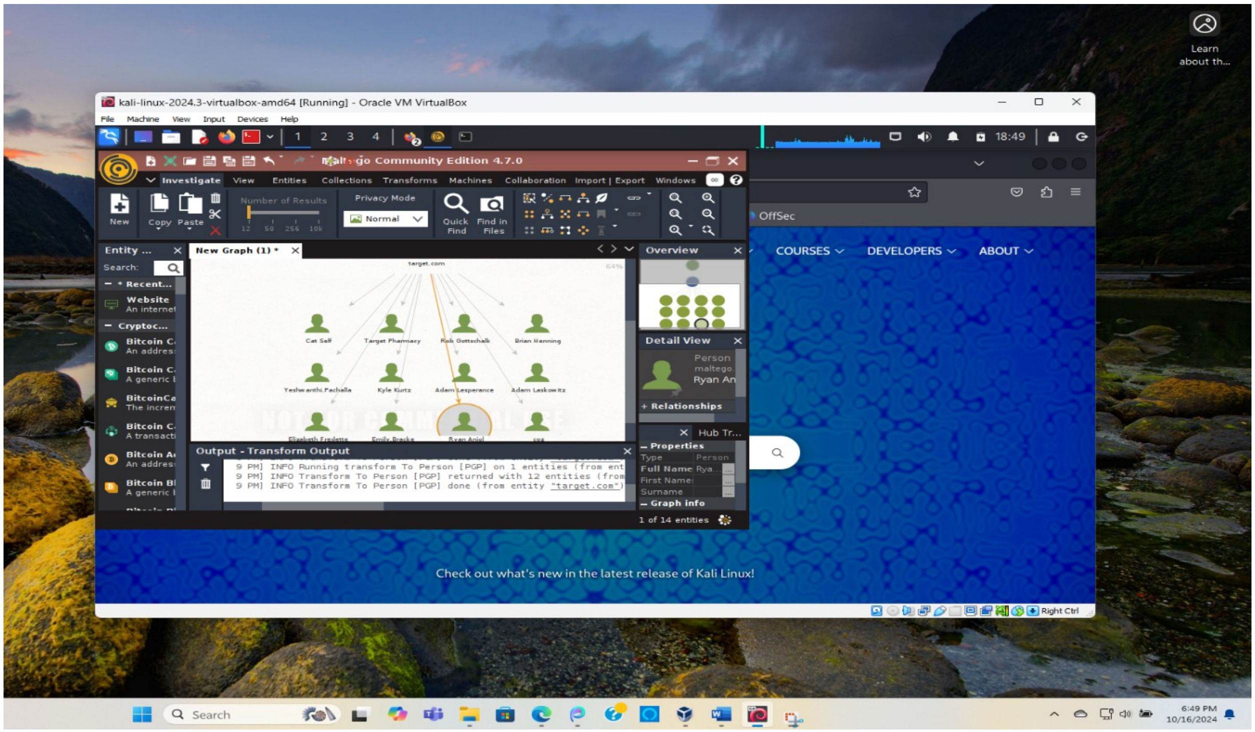
Another search was ran using "To Person (PGP)" and 12 entities was found



Output - Transform Output

```
9 PM] INFO Running transform To Person [PGP] on 1 entities (from ent
9 PM] INFO Transform To Person [PGP] returned with 12 entities (from
9 PM] INFO Transform To Person [PGP] done (from entity "target.com")
```

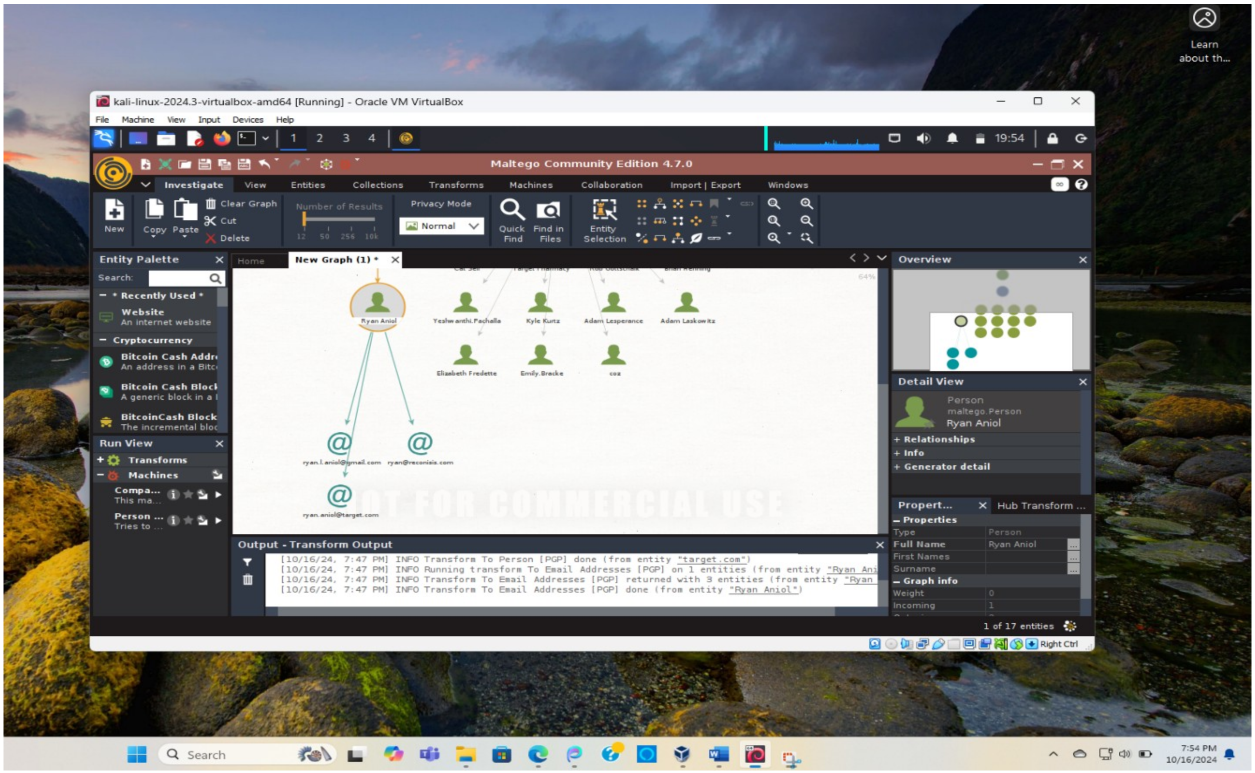
Amongst the 12 entities, I decided to use Ryan Aniol as my perspective target.



Output - Transform Output

```
9 PM] INFO Running transform To Person [PGP] on 1 entities (from ent
9 PM] INFO Transform To Person [PGP] returned with 12 entities (from
9 PM] INFO Transform To Person [PGP] done (from entity "target.com")
```

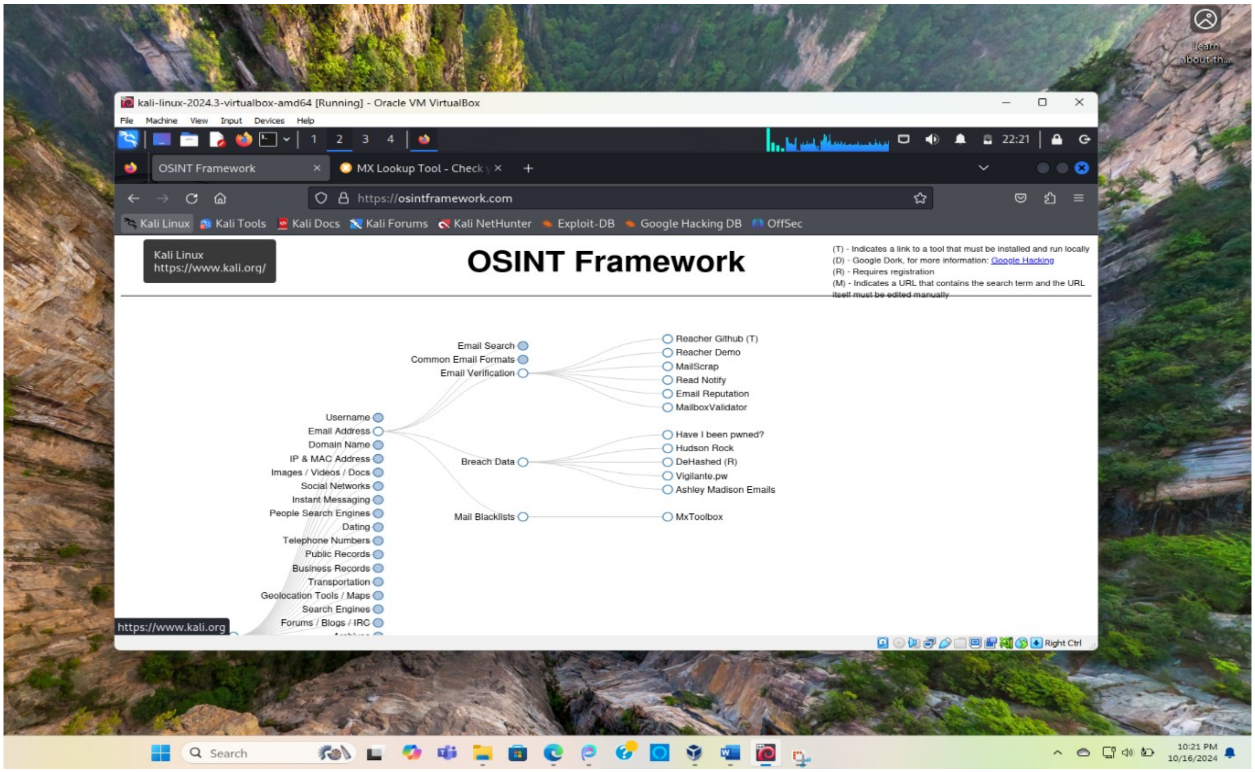
Three email addresses were found for Ryan Aniol



Output - Transform Output

```
[10/16/24, 7:47 PM] INFO Transform To Person [PGP] done (from entity "target.com")
[10/16/24, 7:47 PM] INFO Running transform To Email Addresses [PGP] on 1 entities (from entity "Ryan Ani
[10/16/24, 7:47 PM] INFO Transform To Email Addresses [PGP] returned with 3 entities (from entity "Ryan
[10/16/24, 7:47 PM] INFO Transform To Email Addresses [PGP] done (from entity "Ryan Aniol")
```

The OSINT framework was used to look up the desired email address

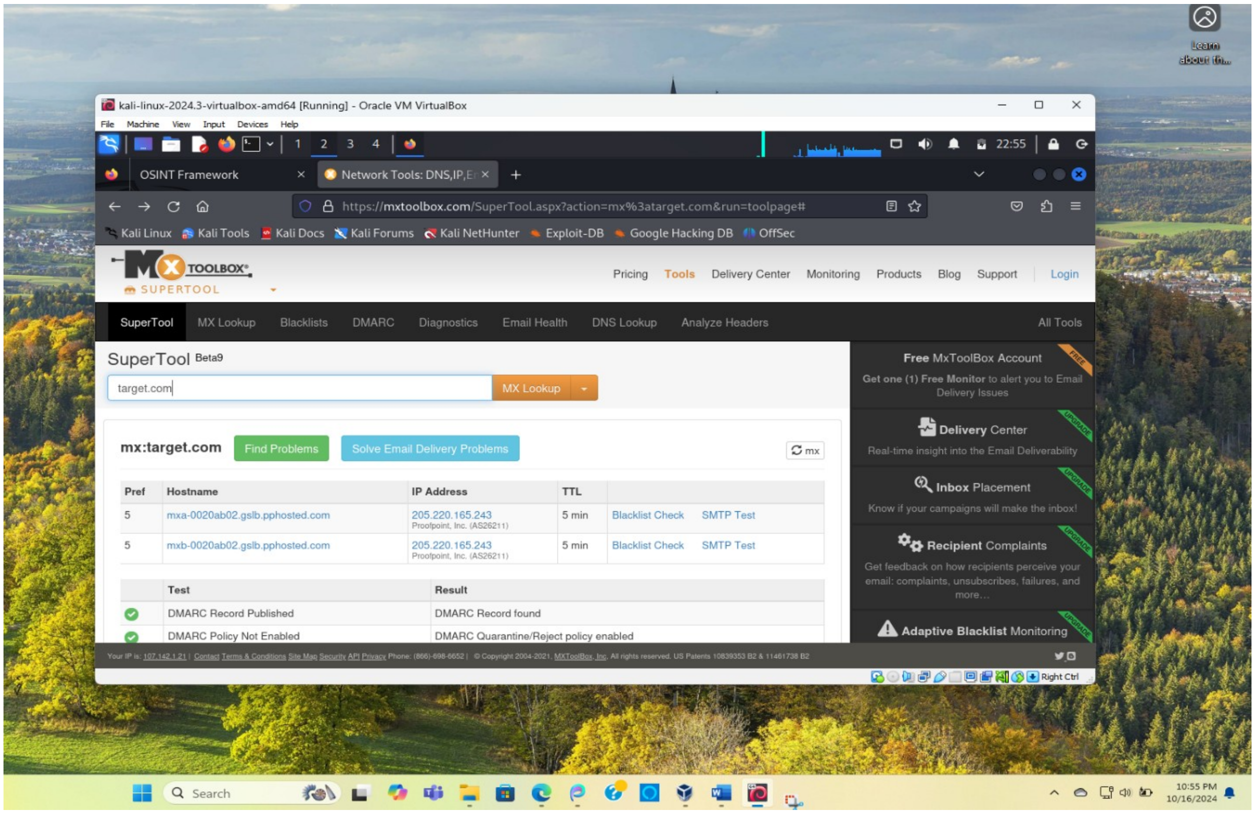


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

https://osintframework.com

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

Mx Toolbox was used to do a further search of the email address



kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

https://mxtoolbox.com/SuperTool.aspx?action=mx%3atarget.com&run=toolpage#

SuperTool Beta9

target.com

mx:target.com

Pref	Hostname	IP Address	TTL		
5	mxa-0020ab02.gslb.pphosted.com	205.220.165.243 Proofpoint, Inc. (AS26211)	5 min	Blacklist Check	SMTP Test
5	mxb-0020ab02.gslb.pphosted.com	205.220.165.243 Proofpoint, Inc. (AS26211)	5 min	Blacklist Check	SMTP Test

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

Your IP is: 107.142.1.21 | Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

Spear Phishing Email

October 16th, 2024

Subject: Urgent: Action Required for Upcoming Board Meeting

From: ceo.johndoe@target.com

To: assistant.ryan@target.com

Hello Ryan,

I hope you're doing well! Can you help me with a small but urgent task before the board meeting next week? I'm attaching the confidential meeting agenda and some sensitive data that needs your immediate review. Please open the document and make any necessary corrections before forwarding it to the rest of the team.

[malicious link disguised as a trusted service].

Let me know once you've reviewed it. Thank you so much for your help!

Best regards,
John Doe
CEO, Target Inc.

Legal authorities and ethical consideration from a Christian perspective

From a Christian ethical standpoint, you must act with integrity and respect while performing penetration testing. Ensure you have written permission from the company to perform penetration testing, including social engineering attacks like phishing. Follow legal frameworks such as the Computer Fraud and Abuse Act (CFAA), ensuring no unauthorized access is obtained. It is important to show respect for others. Although phishing is allowed during pen testing, it’s important to avoid excessively intrusive behavior or harming the dignity of individuals. Educate clients on how to secure their systems, not simply expose flaws. Your role is to prevent malicious attacks by simulating one. Lastly, transparency and accountability go a long way. Your testing should reflect honesty and good intentions, helping organizations without causing unnecessary harm. Proverbs 11:3, states that "The integrity of the upright guides them, but the unfaithful are destroyed by their duplicity."

References

Bible Gateway. (n.d.). *Proverbs 11:3, New International Version*. https://www.biblegateway.com/passage/?search=Proverbs%2011:3&version=NIV#:~:text=Proverbs%2011%3A3%20New%20International%20Version%203%20The%20integrity,but%20the%20unfaithful%20are%20destroyed%20by%20their%20duplicity.

GeeksforGeeks. (2021, January 6). *Maltego tool in Kali Linux*. https://www.geeksforgeeks.org/maltego-tool-in-kali-linux/

Kumar, M. (2020). *The basics of hacking and penetration testing* (2nd ed.). Syngress.

Maltego. (2024, October 8). *What is Maltego?* https://docs.maltego.com/support/solutions/articles/15000019166-what-ismaltegofrom