Passive Reconnaissance

Module 8 | Activity 1

Introduction

In Module 8, you learned about the vulnerability risks within a computer system. Vulnerabilities in a computer allow hackers to take advantage of users. To check for possibility vulnerabilities, a penetration test can be done. The first step of a pen test is passive reconnaissance. This is the action of collecting as much public information about a target as possible. This is done in a way that is not suspicious and ensures no interaction with the target. Activity 1 will be guiding you through the steps of performing a passive reconnaissance.

Getting Started

First things first, the information collected in this activity should be collected in a **PASSIVE** manner. No scans or non-standard communication can be used. All information should be publically available with the help of a web browser or commands. Work with your team to collect as much information about the domain you choose. You will be using your VM and Google for this activity, so multiple teammates can login to use the webbrowser. This will make the activity go fast with more hands on deck. Feel free to work as a team or assign roles.

Data Collection

A. PICKING YOUR TEAM'S TARGET

Take a minute with your team to pick a domain name that you want to perform a passive reconnaissance on. This domain should be fairly large, so there is enough public information to gather. (Ex: GrubHub.com) No small businesses. Feel free to "shop around" to find a good domain to target that provides information.

Domain Name: _____

B. USING THE **whois** COMMAND TO FIND INFO ABOUT DNS DOMAIN

Similar to how we use the **whois** command in Module 4 Activity 2, we can use it to collect data about the domain you chose. We can use it to find information about registration data, expiration date, register, contact information (telephone number, address, email,etc.)

kernel.org

Updated 1 second ago

DOMAIN INFORMATION

Domain:	kernel.org
Registrar:	Gandi SAS
Registration Date:	1997-03-07
Expiration Date:	2019-03-08
Updated Date:	2017-03-11
Status:	clientTransferProhibited
Name Servers:	ns11.constellix.com ns21.constellix.com ns31.constellix.com ns41.constellix.net ns51.constellix.net ns61.constellix.net

REGISTRANT CONTACT

Name:	Jim Zemlin
Organization:	The Linux Foundation
Street:	1 Letterman Drive, Building D, Suite D4700 Suite 102
City:	San Francisco
Postal Code:	94129
Country:	US
Phone:	+1.4157239709
Fax:	+1.9712582363
Email:	admin@linux-foundation.org

ADMINISTRATIVE CONTACT

Name:	Jim Zemlin
Organization:	The Linux Foundation
Street:	1 Letterman Drive, Building D, Suite D4700 Suite 102
City:	San Francisco

Use the **whois** command to collect the following(Feel free to just add in screenshots):

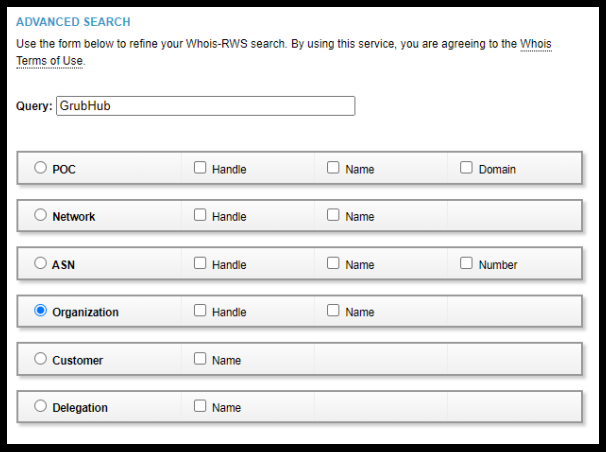
1. Domain owner information

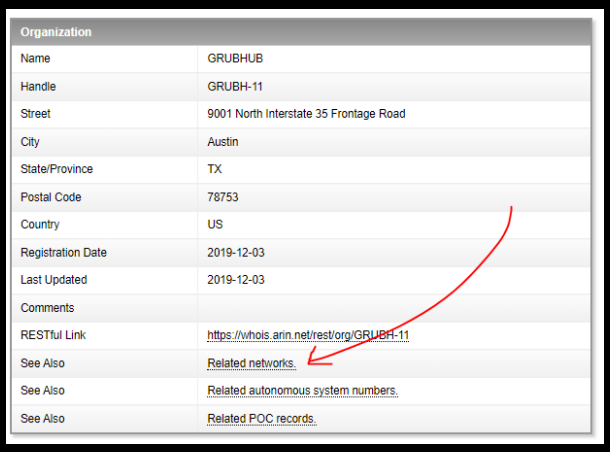
2. Domain registrant contact information

3. Administrative contact information

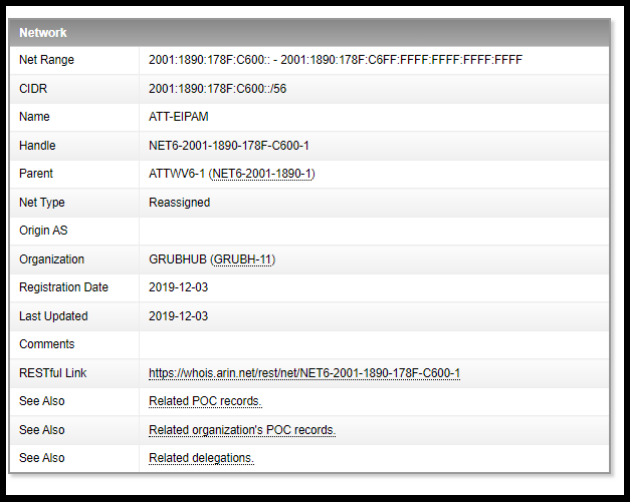
C. IP RANGE

Use The American Registry for Internet Numbers to find the IP Range of your domain. The IP Range tells you where the broadcast of the domain is located. Search your domain in the query search bar and select the appropriate category. I am going to use GrubHub as an example.





When you press submit, it will give you a list of organization links. Click on one, and you should see a link that says "Related Networks". Click on it. You will then reach the following page.

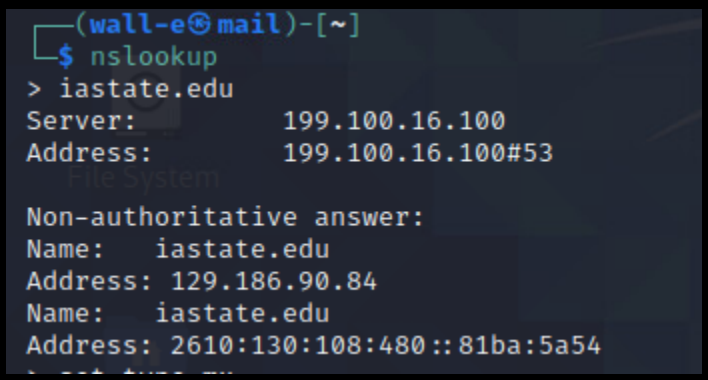


Click on the network research link to reach the final pages. Here you will find the network range labeled as CIDR. The CIDR tells you the domain broadcast address. Write it down below.

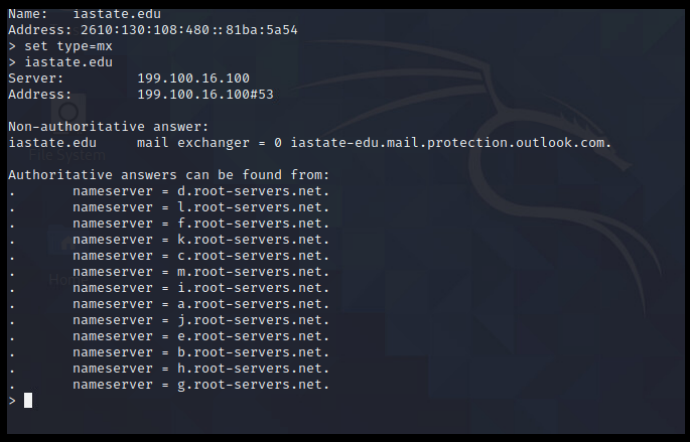
CIDR: _____

D. DNS Interrogation

Here we are going to use the **nslookup** to find other server records. Run the **nslookup** command. Then type in your domain server like the example below.



We are also able to find the mail server of the domain by running set type=mx and your domain server as shown below.



To find the DNS server, we can run set type=mx and your domain similar to the step above.

Find the following information about your domain.

1. Mail Server address_____

2. DNS server address_____

E. Network Path

This section will have you use the command traceroute to map out the network's path and find where the network is located. Run **traceroute <Your domain IP Address (199.100.16.100)>** to view the traceroutes. You can also use gsuite.tools/traceroute to see a visual traceroute of your domain.

1. Screenshot of traceroutes - include both a visual and/or textual

F. Geolocation

You may have heard of or used geolocation in the past for fun. Geolocation is the process of identifying the geographic location of a device through the internet, and it can be very useful for hackers. Sites like www.infosniper.net can be used to collect information about physical locations that can lead to physical attacks and social engineering.

Use the link above to collect the following data about your domain.

1. What country_____
2. Which ISP_____
3. Who is providing the hosting of the website?_____
4. Who is providing the target's DNS?_____

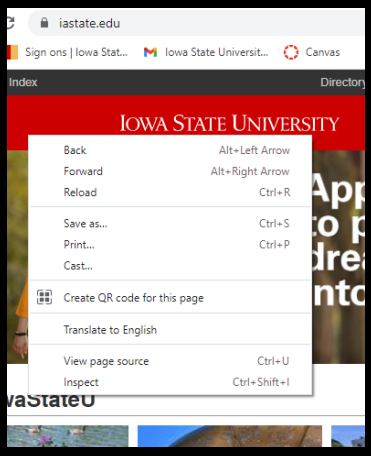
G. Google Searching!

At this point, you know that google is your best friend. Google is very valuable for searching and finding information about almost everything. As you probably guessed from the start, google is going to be used in many ways for this activity.

The first thing we can do with google is to simply do a search of the domain.

1. Find the employee list and information of the domain.

2. Look at the source code of the website to find information about the server. You can do this by right clicking anywhere on the website and clicking on "View page source".



Next, we will look on google to try and find Recent events involving the organization. Gossip can be very useful sometimes. Look to see if the company has merged with other organizations. If they have, you can then search that organization like we did above for valuable information.