Lab: Internet-wide Scanning

Jamie O'Hare

Edinburgh Napier University Security Society

2019

1. Overview

Aim: This lab looks to explore information gathering regarding Internet-wide scanning. Due to the nature of the means used in the lab, the tools and techniques employed would be classed as passive reconnaissance. Typically the first phase of information gathering in a black box security testing engagement. Importantly, this phase is performed prior to active reconnaissance to maximise the information gathered before corresponding with target systems, thereafter creating evidence through logs. However, this type of information gathering could also be used network administration.

Plan: A combination of regular Internet browsing, reconnaissance tools and publicly available Internet-wide scanners will be used.

For this lab, a web browser and a terminal on your host machine will be used.

Notes: A cheat sheet of filters can be found at Cheat Sheet.

A Shodan account will be required for this lab. These can be acquired for free when the account is created with an academic email.

To aid learning, answers and procedures where applicable, can be found at Solutions. These are provided upside down football programme quiz style to hinder thoughtless completion.

Additional passive reconnaissance materials can be found at References.

1.1 Cheat Sheet

In this exercise, there will come times in which filtering search results will be necessary. To ease this process, this cheat sheet below outlines some of the more useful filters. Further filters may be found in References.

Platform	Filter	Description
Shodan	city	City name
	country	2-letter country code
	hash	A numerical hash of the data property
	has_ipv6	Boolean
	has_screenshot	Boolean
	hostname	Hostname
	ip	Alias for net
	net	Network range (1.1.1.0/24)
	org	Organization assigned the address
	os	Operating system
	port	Port number
	product	Name of the software
	version	Version for the software
	vuln	CVE ID for a vulnerability
	http.component	Name of web technology
	http.html_hash	A numerical hash of the website HTML
	http.status	HTTP response status code (200, 404)
	ssl.version	Accepted sll version(s)
	ssl.cert.alg	Certificate algorithm used
	ssl.cert.expired	Boolean
	ssl.cert.pubkey.bits	Number of bits in the public key
	ssl.cipher.bits	Number of bits in the preferred cipher

Note: Shodan will try to find results matching all search terms. Meaning there is an implicit '+' between each search term. You can exclude results by using the '-' operator in front of filter.

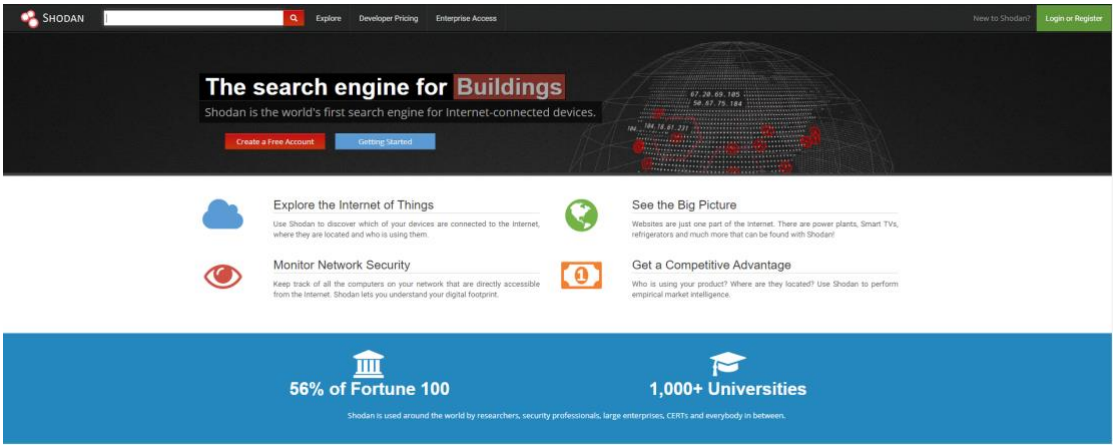
1.2 Activities

Split into multiple sections to show the potential use cases for Internet-wide scanning data. For each question, provide both the query used and the number of results where possible.

- Basic Usage
- Advanced Filtering
- Deep Web Funnies
- Specifying the Specifics
- Reflective Questions
- Further Reading
- Solutions

2.1.1 Basic Usage

Navigate to shodan.io, and register an account using your university email. This allows you to then use filters in the search bar.



Questions

Q1: What are the services are operating on 212.91.11.20?

Q2: What are the top 5 services operating on 134.0.0.0/8?

Q3: How many services are running on port 21 worldwide?

Q4: How many services are running on port 80 worldwide?

The next set of questions require the use of operators, make sure to read the cheat sheet footnote on how to do so!

Q5: How many services are running on port 21, 80 and 443 worldwide?

Q6: How many services are running on port 80 and 443 in Ireland?

Q7: How many services are running on port 80 and 443 in Ireland?

Q8: How many services are running on port 80 and 443 in Ireland with "hello world" in the banner?

Q9: What are the top 5 countries that Digital Ocean operate in?

Q10: What are the top 5 services that Digital Ocean are operating in India?

Congratulations, you can now do about as much Shodan as a B-tier tech journo!

2.1.2 Advanced Filtering

Obviously, you want to get to grips with what Shodan can really do. In this section, we will explore advanced filtering. Make sure to refer to your cheat sheet!

Questions

Q1: What are the top 5 services that Digital Ocean are operating in India?

Q2: How many services are running Splunk in Great Britain but not in London?

Q3: What country has the most web services which are blocked for legal reasons? (Hint: HTTP Status Codes)

Note: Click on an entry returned for the query used in Q3 and view the raw details for this service. This data can show you details about the crawler which collected them.

Questions

Q4: What are the top 5 services which accept sslv3 connections?

Q5: What service iss the most Heartbleed vulnerable ports other than 443?

Questions

Q6: How many apache services running default pages (It works!) are exposed on the Internet?

Q7: Attempt Q6 again, however, this time use the html.hash filter, is there any differences?

Q8: How many IMAP+TLS services are operating with expired certificates?

Q9: How many nginx services are using md5withrsaencryption in Great Britain but not in London?

Q10: What country has the most Heartbleed vulnerable services, accepting sslv3 connections on ports other than 443?

This only scratches the surface at what Shodan can be used for, if you are interested in finding out more perhaps look at the further reading section!

2.1.3 Deep Web Funnies

Shodan lets you explore the deep web, and although it doesn't contain as many lolcats as the regular web, there are still a few fun things you can find. This section tests your knowledge gained so far if you are struggling skip to the next segment specifying the specifics!

Questions

Q1: The famous IKEA house is located in which country?

Q2: How many cows are in the shed in Lockerbie?

Q3: How many games of Doom are being played right now?

Q4: How many MongoDB instances can you find in Mongolia?

Q5: How many iKettles are online?

Q6: Similarly, how many teapots are online?

If you managed all those questions you are now a qualified Shodan Safari guide!

2.1.4 Specifying the Specifics

The novelty of Shodan wears off fast if all you do is simple searches. In this section, we will begin to look at specific searches which could be used to scope out an organisation. In this example, we will be looking at **Edinburgh Napier University**.

From your host machine, using the command line, identify your current IP address.

Note: This lab presumes you are connected to Edinburgh Napier University's network. If you are not please skip to Q3.

Question

Q1: What is your IP address?

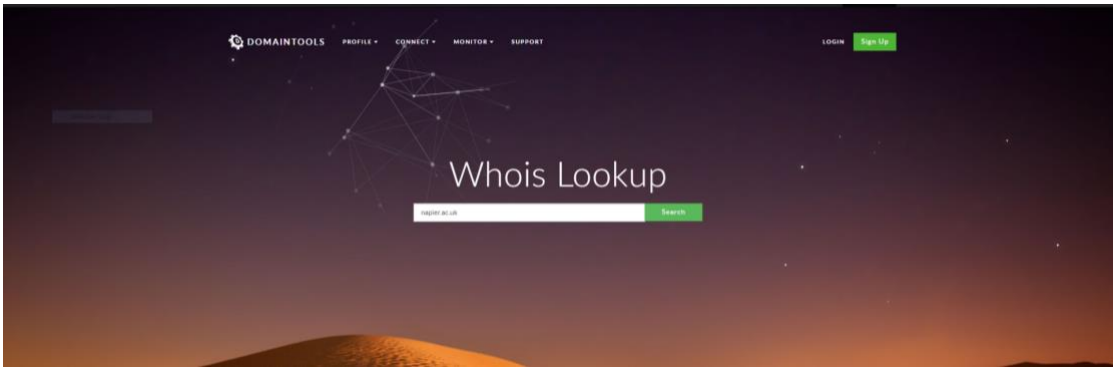
Note: If your IP address is 166.X.Y.Z, you have identified your IP address correctly however, due to ongoing network upgrades you have been given an IP from a different range. Skip to Q3.

Question

Q2: Perform a search for your IP, what do you see and why?

If your IP address does not return a result, we are yet to find an Internet-facing service. So we will have to try it the old fashion way, by finding the IP address of Edinburgh Napier's website. This can be achieved by using DNS.

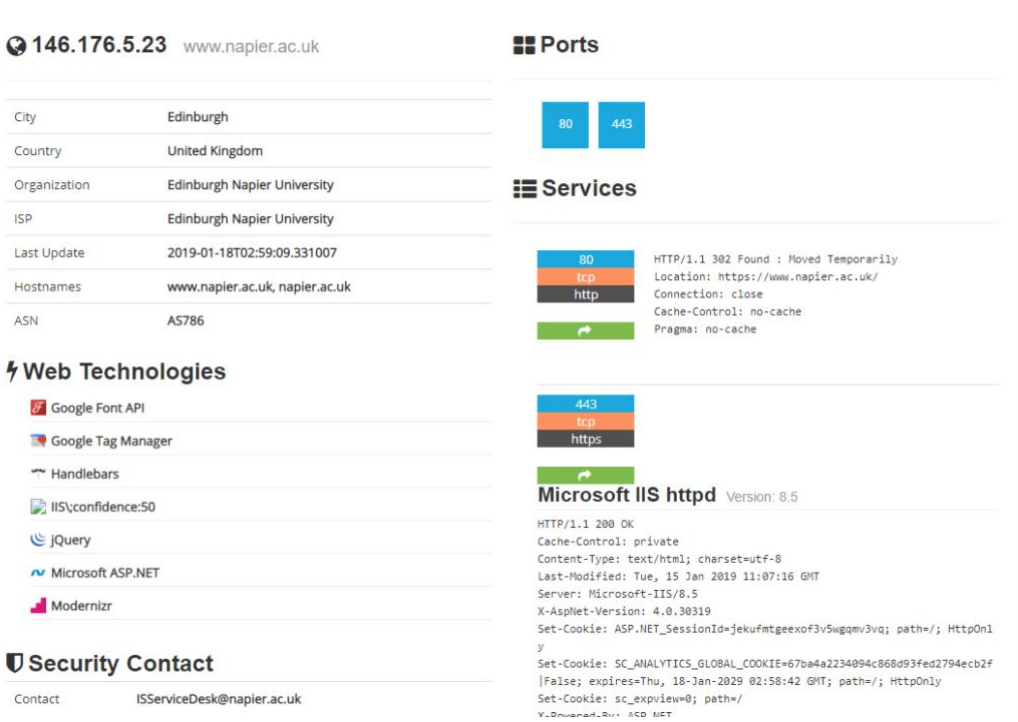
Domain name information can be retrieved through the use of whois or through several DNS web-apps. One such tool is **whois.domaintools.com**. Navigate to this page and search for **napier.ac.uk**.



Questions

Q3: What is the IP address tied to napier.ac.uk?

Q4: Search for this IP address on Shodan. What information can you find associated to this service? (Make note of the organisation and ASN)

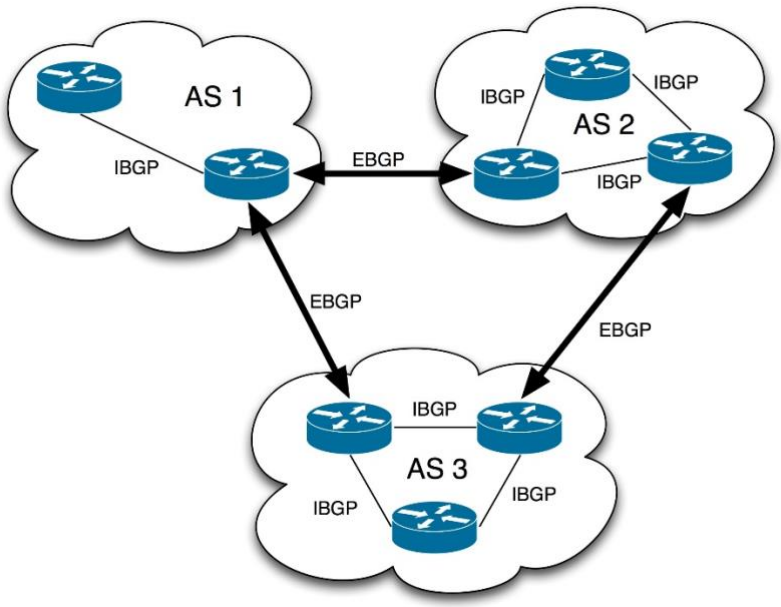


Your search for Edinburgh Napier's website on Shodan should look like this. A keen eye may be able to spot the fields specified in the cheat sheet! This section will try to demonstrate some.

Questions

Q5: Using the organisation filter search for Edinburgh Napier University, can you guess the Edinburgh Napier University IP address range from these results? (Hint: use "these")

The above question shows that you have to guess the IP address range from the organisation filter. However, using the handy ASN number found earlier, we can determine the IP range using a wee bit more reconnaissance. But first a quick AS 101!



Autonomous Systems (AS) are commonly referred to as the backbone of the Internet. An AS is an Internetwork owned and administrated by a single organisation, generally an ISP, which adheres to an individual and clearly defined routing policy. This policies complicates routing but allows for a preferred path across the Internet. In the current climate, this may be good to avoid surveillance, or perhaps to conduct surveillance! Each AS is identified by an AS number (ASN) which range from 1 to 65535.

Within an AS more classical routing protocols such as Open Short Path First (OSPF) and Routing Information Protocol (RIP) is used to exchange information. Whereas, to interconnect ASs Exterior Gateway Protocols (EGPs) are used. An example of this type of routing protocol is the Border Gateway Protocol (BGP). Unlike conventional protocols, BGP does not use metrics in determining next hop. Instead, the use of network policies and rules are applied.

One function within the BGP protocol is BGP neighbours, in which peers exchange information such as AS Path, Path Attributes, Route Prefix and most importantly for this lab, destinations within the AS. In the following questions we will investigate Edinburgh Napier University's AS to find their IP address range.

Similar to DNS, BGP information can be found through web-apps. Start off by navigating to **bgpview.io** and entering Edinburgh Napier University's ASN, like so!

Questions

Q4: Navigate to the Prefix tab and have a look at all the networks advertised. What is the IP address range for funnily named Goonhilly Earth Station?

Q5: Back to business, what is Edinburgh Napier University's IP address range?

Q6: Is this the same or close to what you guessed for Q3?

Q7: Now try using the net filter on Shodan to view Edinburgh Napier University's entire network, does this match the results seen when using the org filter?

Q7: How may this net/org searching be complicated if Edinburgh Napier University were to use a public cloud like Amazon Web Services or Digital Ocean?

Note: The answer to Q7 should be yes as Edinburgh Napier has only one entry on AS786, however, look for The Edinburgh University on BGPview…

Question

Q8: Conduct a thorough examination of the Edinburgh Napier University IP range using Shodan. What can you find?

2.1.5 Reflective Questions

This lab aimed to investigate the usage of Internet-wide Scanners for information gathering. Through the previous questions, we have explored how to use Shodan, including the nooks and crannies, along with a use case on Edinburgh Napier University. The following questions look to access your reflection on the lab as well as the accompanying lecture.

Questions

Q1: As a Network Administrator, what dangers may there be by having your services indexed by Shodan and what steps could you take to minimize these risks?

Q2**:** What advantages and disadvantages are there for a hacker attempting to use Shodan maliciously?

Q3: Discuss the potential legal and ethical issues for those behind Internet-wide scanners such as Shodan?

2.1.6 Further Reading

Shodan and Internet-wide scanning as a whole sits in a sweet spot between Academia and Industry. Below are recommended further reading if you wish to delve deeper in this area.

[1] J. Matherly, *Complete Guide to Shodan*. Leanpub, 2015.

[2] R. Bodenheim, and J. Butts, and S. Dunlap, and B. Mullins, Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices, International Journal of Critical Infrastructure Protection, volume 7, issue 2, 2014, pp.114–123.

[3] Z. Durumeric, and D. Adrian, and A. Mirian, and M. Bailey, and JA. Halderman, A search engine backed by Internet-Wide scanning, Proceedings of the 22nd ACM Conference on Computer and Communications, 2015, pp.542–553.

[4] E. Bou-Harb, and M. Debbabi, and C. Assi, Cyber scanning: a comprehensive survey, IEEE Communications Surveys & Tutorials, volume 16, issue 3, 2014, pp.1496–1519.

[5] J. O'Hare, Scout, 2018. [Online] Available: https://github.com/TheHairyJ/Scout.

2.1.7 Solutions

Hahahahaha, no answers for you yet! I will upload them later…