FOUNDATIONS IN IT SECURITY: INVESTIGATING AN IP ADDRESS

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

TODAY ….

Today we will overview how to perform a simple investigation of an IP Address.

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: OVERVIEW

GORDON | REYNOLDS (2018)

OVERVIEW

- Whenever a computer or device connects to an internet or local network, it needs to have a unique IP address assigned to it in that network.
- The IP address assignment is performed automatically in the background by either your Internet Service Provider if you're connecting to the Internet, or by an internal DHCP service enabled on a server or a router if connecting to a local network.
- It acts as an identifier on a network and can be traced back to the device based on the date, time and IP address.

GORDON | REYNOLDS (2018)

OVERVIEW

- A connection made to any service will expose your IP address to the target.
  - For example, visiting a website using your web browser will initiate a connection from your computer to the web server that is hosting the website.
  - Your IP address will usually be logged by the web server which can be used for analytics traffic reports or even to track abusive behaviour such as brute force or DoS attacks.

GORDON | REYNOLDS (2018)

OVERVIEW

- An IP address isn't just 4 sets of numbers separated by 3 dotted decimal points.
  - For example, 185.23.47.32
- Using the right tools and online services, you can actually find a lot of information about an IP address which can help you to report the attacks to the proper service provider for them to take the necessary actions, such as temporarily suspending the service to prevent further attacks on other targets.

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: IP ADDRESS INFORMATION

GORDON | REYNOLDS (2018)

#1: IP ADDRESS LOCATION

- The most basic information that you can easily get from an IP address is the location.
- An IP address doesn't actually contain any information at all, but yet the location can be revealed by querying a large IP geolocation database that is maintained by different companies, each with different rates of accuracy.
- There is a free online demo version of MaxMind's Geo2IP City database that includes not only country, but also more detailed information such as subdivisions, city, postal code, latitude and longitude.

GORDON | REYNOLDS (2018)

#2: IP PROXY

- Another piece of important information that you can get from an IP address is by checking if it is running a proxy service.
- An open proxy is capable of hiding the real user's IP address.
- Therefore, if the attacker's IP address found in your firewall log is detected as proxy, then there is no need to investigate any further.
  - http://getipintel.net/index.php#web
  - For a given IP, the website assigns a score between 0 and 1.
    - A score of 1 implies a proxy address which is explicitly banned

GORDON | REYNOLDS (2018)

#3: DETECT WEBSITES HOSTED ON AN IP ADDRESS

- If the computer is running an HTTP web server, the IP address of the server can also reveal the type of websites that it is hosting.
- A single IP address can actually be configured to host multiple domains which is a method commonly used in shared web hosting.
- This method relies on checking a database containing domains resolved to IP addresses and the system simply matches the domains that resolve to the same IP address.

GORDON | REYNOLDS (2018)

#3: DETECT WEBSITES HOSTED ON AN IP ADDRESS

- This method is known as "Reverse IP Lookup" or "IP neighbor". There are a number of such services available on the Internet offered for free.
  - https://majestic.com/reports/neighbourhood-checker
  - Free sign-up

GORDON | REYNOLDS (2018)

#4: CHECK AN IP ADDRESS FOR BLACKLIST

- When it comes to checking for blacklists, it is commonly split into two different categories:
  - Spam
  - Malware.
- You can check the IP address on both categories to find out if it has been used to send spam or host malware.
  http://multirbl.valli.org/lookup/

GORDON | REYNOLDS (2018)

#5: REPORT ABUSIVE IP ADDRESSES

- After you've done all the investigation on the abusive IP address, the last step is to report the malicious activity to the proper authority.
- You will need to send the firewall log file showing the attack to the abuse email address which can be found by performing a WHOIS on the IP address.
- One of the most reliable services that can perform a Whois Lookup on an IP address is by DomainTools.
- Simply type in the IP address and click the Search button which will return a small list of contact information.
  - http://whois.domaintools.com/

GORDON | REYNOLDS (2018)

IP LOOKUP

- A useful tool is IPVOID as it can perform multiple test from a single interface (webpage).
  - https://www.ipvoid.com/
- In addition, you can also check the reputation of an IP address using tools such as Symantec's IP reputation checker.
  - https://ipremoval.sms.symantec.com/

GORDON | REYNOLDS (2018)

SUMMARY ….

Today we overviewed how to perform a simple investigation of an IP Address.

GORDON | REYNOLDS (2019)