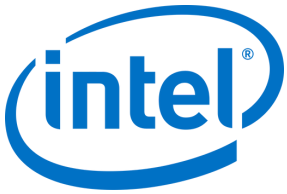


OSINT Report

Passive reconnaissance on intel.com

Feb' 2024

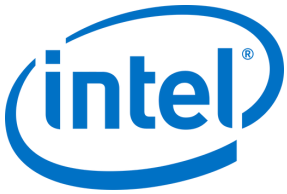
Prepared by :

Gopi Gor

FDIN: A21370441

ggg@fordham.edu

Executive Summary



This report discusses the passive reconnaisance method to find information on a company. Open-Source Intelligence methods are used to find information on one of the Fortune 500 companies - we focused on **intel.com.**

Over the course of the report, we will be discussing the information that we obtained, such as sub-domains, IP addresses, server details, hosts, open ports and services.
We will also analyze these results to present findings, draw conclusions, and make recommendations.

The key findings of this report are:

1. The IP address of all servers and subdomains.
2. The DMARC policy compliance.
3. The hosts discovered.
4. Port services and their versions

Apart from this, we had some smaller findings which we will discuss in a different section.

Background Information

Headquarted in Santa Clara, California, Intel is known to be a global technology company, mainly in semiconductors and computing technology. It made the first microprocessor in 1971 and has been raising the bar with new influential products.

A number of noteworthy turning points have shaped Intel's influence on the technology scene. It has operations worldwide, with teams scattered all across the globe.

Intel has experienced difficulties recently, such as production setbacks and increased market competitors. The business's resolve to overcome challenges is reflected in improvements to leadership and strategy.

Apart from this, Intel has had many relevant events like conferences and discussions regarding AI, and multiple events for cloud, IOT and upcoming technologies. Intel makes sure at every step that they are the leading brand in microprocessors and semiconductors.

Methodology

The methodology used in this OSINT research was done mainly for intel.com. The tools, techniques and commands have been listed below.

1. **whois** - *whois intel.com*
2. **nslookup** - *nslookup intel.com*
3. **dig** - *dig intel.com*
4. **MXToolbox** - *intel.com*
5. **Recon-ng** - *recon-ng -> workplaces create intel.com -> modules load google_site_web -> options set SOURCE intel.com -> run*
6. **The Harvester** - *theHarvester -d intel.com -b dnsdumpster*
7. **Shodan** - shodan domain intel.com -> shodan host [IP address]
8. **Google Hacking** - *site:intel.com filetype:pdf "Threats"*

A lot of these tools revealed lots of information about the source and while some gave out almost coinciding information, some tools stood out in the outputs we got.

Findings

The findings revealed a lot of detail about the source and we used a mix of different tools to gather that information. The screenshots in the appendices will depict the findings but they are explained in this section.

- With the whois command, we found registrar details such as email, contact, expiry date, and domain status. We also found 4 name servers of the company and their respective IP addresses.
- With the nslookup command, we found the domain IP of DNS server and IP address of the server. **IP: 13.91.95.74**
- With the dig command, we found the same domain IP address and DNS server IP details. **IP: 150.108.2.11**
- When we looked at MXToolbox for **intel.com** we could find the email subdomains and their IP address, along with their email tests where we found that the DMARC policy was not enabled, and SOA length was not good.
- When we used the recon-ng tool, we found multiple hosts related to intel.com. Some of them also revealed IP address, longitude, latitude, countries and regions.
- When we used theHarvester tool, we found no IP addresses or emails, but we found **109** hosts.
- Finally, with the shodan tool, first we found the multiple domains linked to shodan along with their IP address, then we found the specific details of an IP, which showed us open ports, city, country, services running etc.

Analysis

The above findings provide a lot of entry points for intruders to get into the network through the various domains.

For example, if someone knew the registrar details, they could phish the company about expiration dates and get access to the network. Furthermore, in many tests conducted above, we could find the domain, IP address, subdomains and their IP addresses. This raises a concern because an adversary can look for each IP in detail to look for vulnerabilities, source code and open ports for entry.

From the MX Toolbox we also saw that the DMARC policy was not enabled. This shows that the domain could be phished of spoofed since they don't have this email authentication policy enabled. Also the email domains found could be exploited further to find more detailed information about users in that domain.

The tools which revealed IP address along with locations and geographic details allows a complete analysis to be made about the locations where the company has locations, and this could also be used to try physical methods of breaching.

Recommendations

As per the report and OSINT research done on **intel.com**, there are a few recommendations I can provide to avoid having so much information easily accessible to everyone.

1. Setting up of IDS/IPS systems.
2. Using of private IP spaces instead of public IP's.
3. Minimizing the revealing of information on websites, blogs.
4. Implementing a NAT network for outside communications.
5. Constant OSINT research to understand open points and rectify as needed.
6. Encryption of communication channels via secure methods.
7. Implementation of incident response plans incase there is an entry of an intruder via different hosts or IP address.
8. Keeping in contact with threat intelligence agencies to understand potential threats to the organization.

Appendix

This appendix provides evidence into the findings of the OSINT Research.

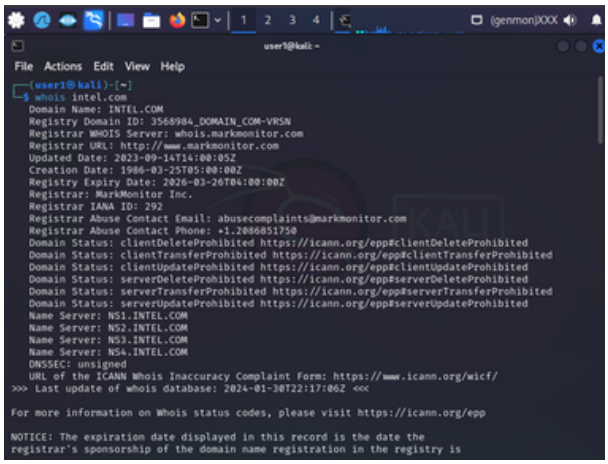


Fig. 1: whois

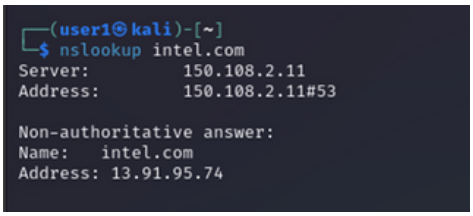


Fig. 2: nslookup

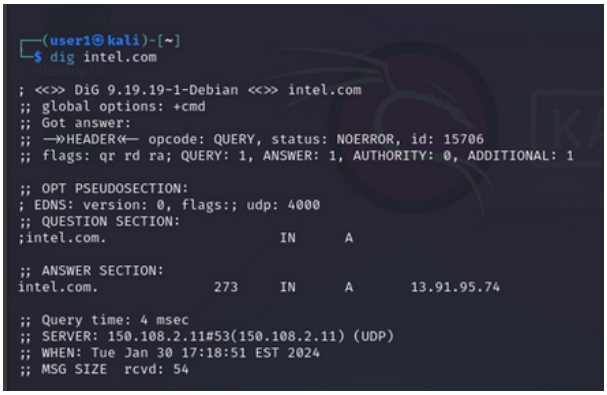


Fig. 3: dig

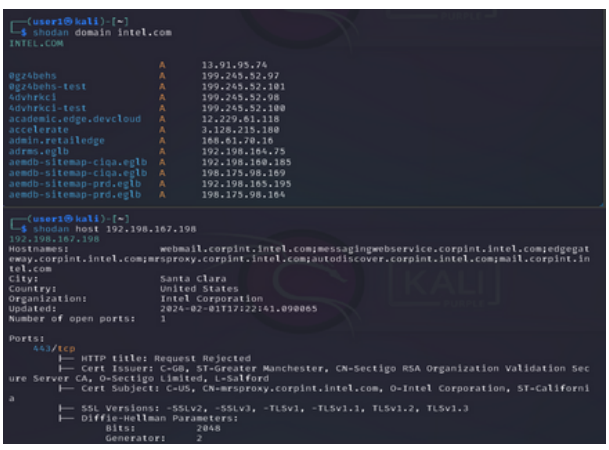


Fig. 4: shodan

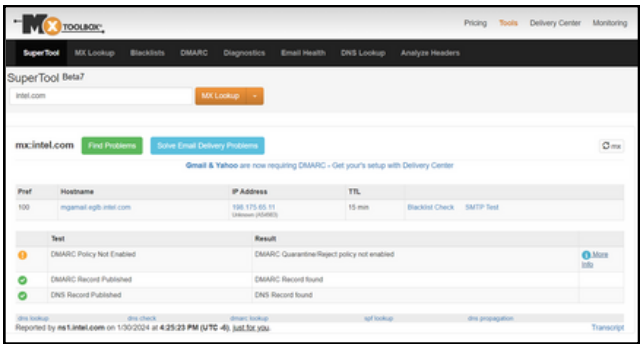


Fig. 5: MX Toolbox

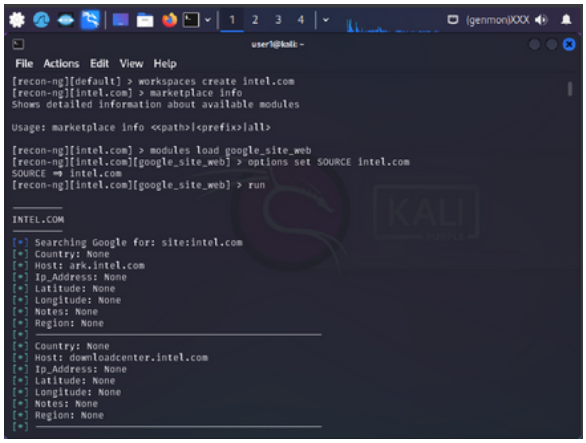


Fig. 6: Recon-ng

Fig. 7: theHarvester

References

1. https://www.mxtoolbox.com/
2. https://hackertarget.com/recon-ng-tutorial
3. https://www.kali.org/tools/theharvester/
4. https://www.researchgate.net/publication/352390324_Prevention_to_Sensitive_Information_Disclosure_via_OSINT
5. https://traversals.com/blog/osint-investigations/