OSINT OPEN-SOURCE INTELLIGENCE OSINT

Offensive OSINT

OWASP
The Open Web Application Security Project

Whoami

OWASP
The Open Web Application Security Project

- **Adam Nurudini**

  CEH, ITIL V3, CCNA, CCNP, CASP, PCI-DSS, BSC-IT

  Lead Security Researcher @ Netwatch Technologies
  Project Consultant, Information Security Architects Ltd
  Member, Cybersecurity Resilience Service Team
  Web Application Penetration Tester
  President – GIMPA School Of Technology Student Association

NETWATCH TECHNOLOGIES

CSRT Cybersecurity Resilience Services Team
MEMBER | www.csrt.org.gh

DISCLAIMER

Any Views or opinions presented in this presentation are solely mine and do not necessarily represent my employer.

- I am not a lawyer or giving you legal advice
- I am not giving you permission or authorizing you to do anything ever.
- In fact don't do anything ever .

osint
open source intelligence

TakeAways

- What is OSINT
- Collect data indirectly without knowing other information
- Collect data about servers, location, operating systems, etc.
- Threat intelligence for your organization
- Data gathering that could protect you and your company
- Skills of GHDB
- Shodan methods and operations
- OSINT using free tools only

OSINT

Open-Source Intelligence (OSINT) is **intelligence** collected from public available sources

“**Open**” refers overt, public available sources (as opposed to covert sources)
Its not related to **open-source software** or **public intelligence**

This information comes from a variety of sources, including the social media pages of your company and staff. These can be a goldmine of information, revealing information such as the design of ID badges, layout of the buildings and software used on internal systems.

Source: https://en.wikipedia.org/wiki/Open-source_intelligence

Open-Source Intelligence (OSINT)

Fields and Sectors where OSINT is mostly required.

Government, Finance, Telecom, Critical Infrastructure, Cyber Security Advisory Firms, Cyber Threat Intelligence Teams, Law, Cyber Forensic Teams and etc.

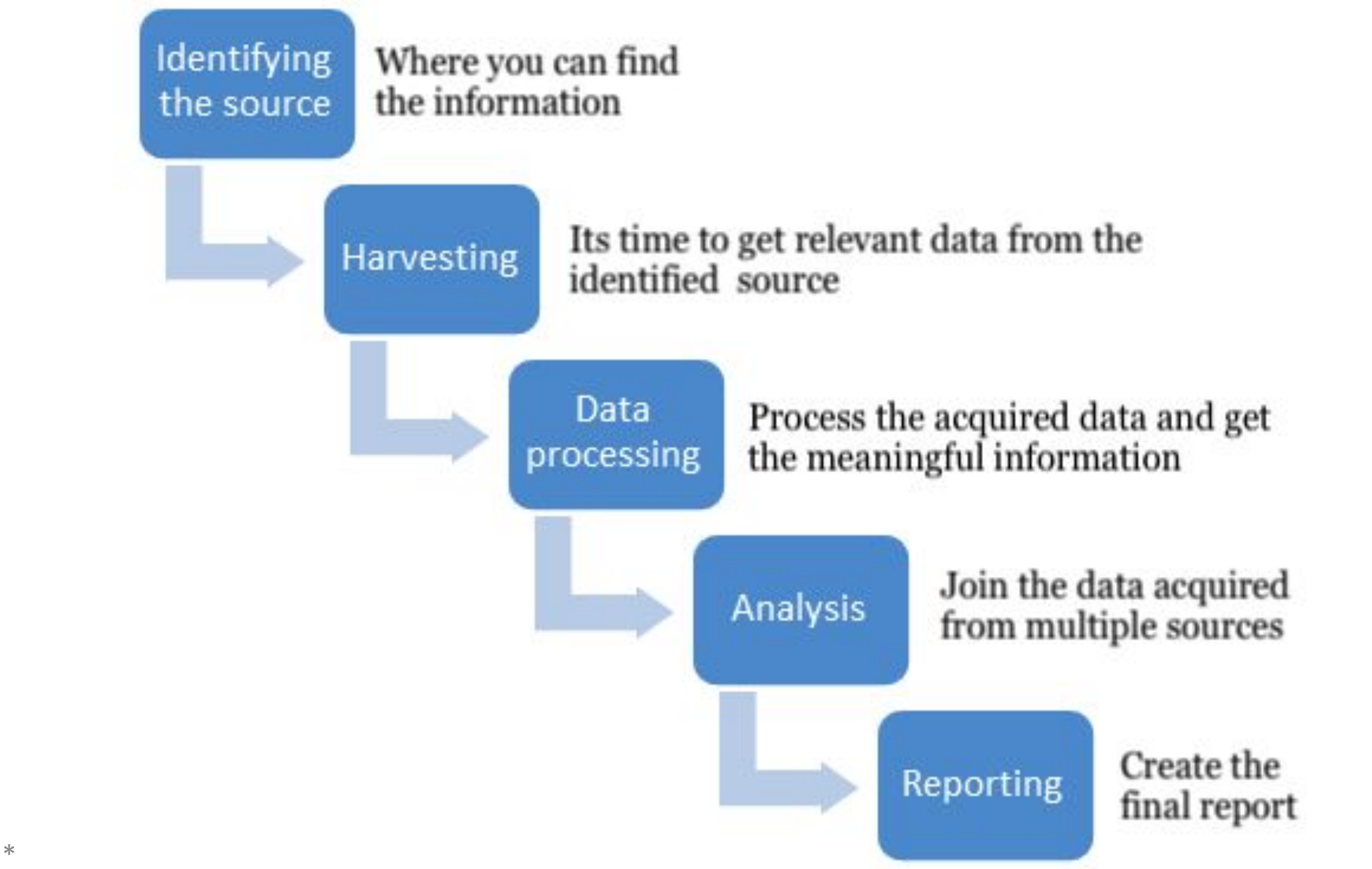
TYPES OF OSINT

From Security perspective we can separate OSINT into:

- Offensive: Gathering information before an attack
- Defensive: Learning about attacks against the company.

The OSINT gives opportunities to both the defender and attacker; you can learn the weakness of a company and fix it while at the same time the weakness could be exploited.

The OSINT Process



Identifying the source — Where you can find the information

Harvesting — Its time to get relevant data from the identified source

Data processing — Process the acquired data and get the meaningful information

Analysis — Join the data acquired from multiple sources

Reporting — Create the final report

OSINT - What information to look

1. Technology infrastructure

IP, Hostname, Services, Networks, Software / hardware versions and OS information, Geo-location and Network diagrams.

2. Database

Documents, papers, presentations, spreadsheets and configuration files

3. Metadata

Email and employee search (name and other personal information)

Offensive OSINT – End goals

The information above can lead to the following cyber attacks:

1. Social Engineering
2. Denial of Service
3. Password brute force attacks
4. Target infiltration
5. User accounts take over
6. Identity theft
7. Data theft

Open Source Intelligence Reconnaissance Surveillance Report

OSINT
Investigations

Brace your self demo is starting

Everybody is interested in something

Offensive OSINT – Resources and tools

1. OSINT Search Engines

Attackers rely on these OSINT search engines to conduct passive reconnaissance.

- Google - https://google.com
- Shodan - https://shodan.io
- Censys - https://censys.io
- Fofa - https://fofa.so
- Dogpile - http://www.dogpile.com
- Archives - https://archive.org/

Offensive OSINT – Resources and tools

2. Email Harvesting

Harvesting email address is an OSINT technique that gives attackers more information to conduct attacks such as password stuffing and social engineering attacks.

Theharvester
https://github.com/laramies/theHarvester

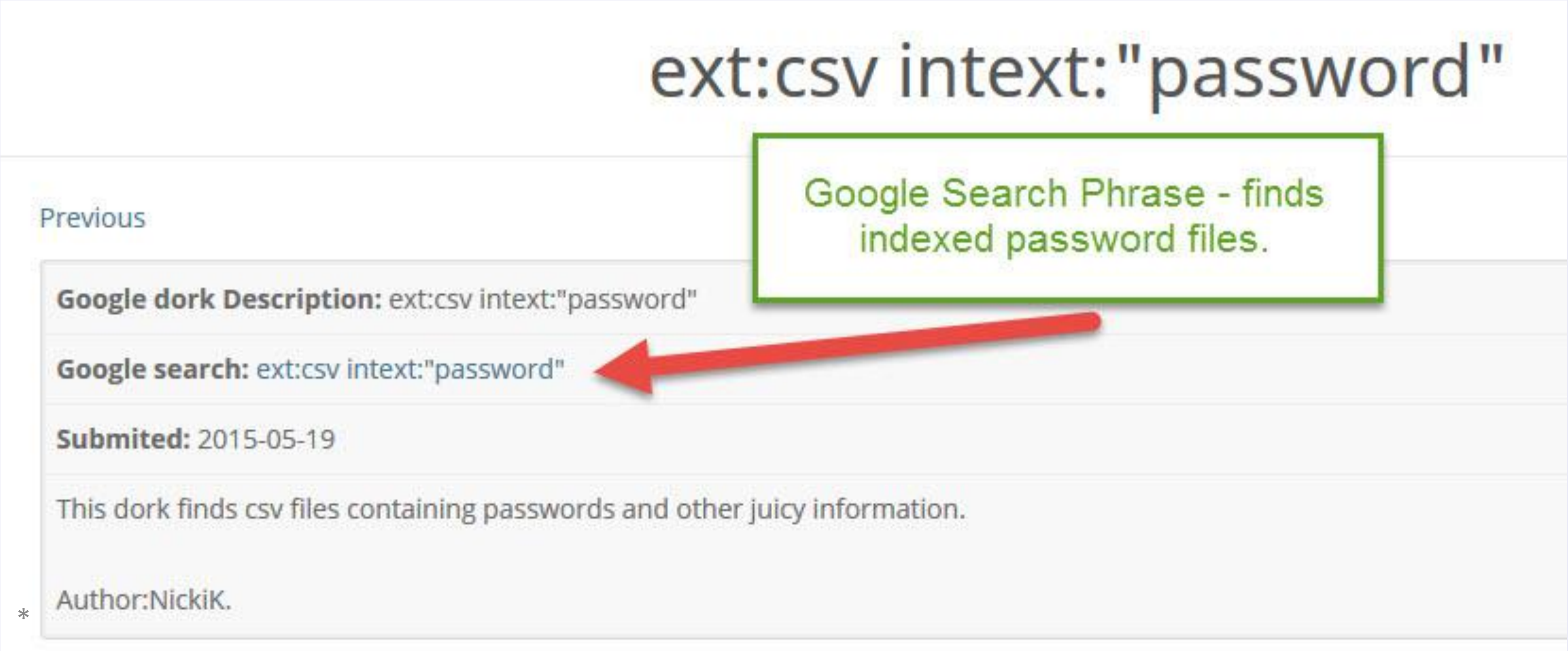
Prowl
https://github.com/nettitude/prowl

Haveibeenpawned -
https://haveibeenpwned.com/

Offensive OSINT – Resources and tools

3. Google Hacking Database (GHDB)

The GHDB is an index of search queries (we call them dorks) used to find publicly available information. Dorks - https://www.exploit-db.com



ext:csv intext:"password"

Google Search Phrase - finds indexed password files.

Previous

Google dork Description: ext:csv intext:"password"

Google search: ext:csv intext:"password"

Submited: 2015-05-19

This dork finds csv files containing passwords and other juicy information.

Author:NickiK.

Offensive OSINT – Resources and tools

3. DNS / Subdomain Enumeration

Subdomain enumeration is the process of finding valid (resolvable) subdomains for one or more domain(s).

Having unsecured subdomain can lead to serious risk to your business.

Tools for subdomain enumeration

Aquatone	- https://github.com/michenriksen/aquatone
Sublister	- https://github.com/aboul3la/Sublist3r
DNS dumpster	- https://dnsdumpster.com/
Facebook	- https://developers.facebook.com/tools/ct

OSINT is important and still gets overlooked by attackers and defenders

I hope that you found this talk useful

References

https://www.slideshare.net
https://resources.infosecinstitute.com
https://google.com
https://www.exploit-db.com
https://www.wikipedia.org/

Thank You

Questions & Answers

Lets connect
Twitter: @Bra__Qwesi
Email: adam.nurudini@st.gimpa.edu.gh