Sonpo

INFORMATION GATHERING

Nowadays, the Internet serves as a vast source of information about any organisation. Some information can be misused to launch a cyber attack if an attacker exploits it to his advantage to the detriment of the security of an organisation. Traceable data from publicly available sources pose a digital footprint risk for you.

The **Information Gathering (IG)** service is a comprehensive initial information analysis of your organisation, which is created on top of publicly available information from freely accessible sources on the Internet (including the darknet, social networks, ...). Such an initial information analysis provides an overview of information about you and your organisation that is freely "roaming" the Internet and thus helps to identify critical areas that may be the target of a cyber-attack. A sensitive information leak can be a major risk these days, putting your company's reputation and security at risk.

You will see for yourself what information potential attackers (hackers) are able to find out about you very quickly, what weaknesses they are able to identify and easily exploit to launch a cyber attack. The results of this information analysis will identify targets for improving cybersecurity and help your organisation choose the right tools to secure target systems and networks.

We mainly use OSINT (Open-Source Intelligence) tools in the provision of IG services:

- Automated tools that can perform global scans in minutes.
- Customisable tools that can filter out irrelevant results using search criteria.
- Systems that can query data from individual devices (IT, OT, IoT)
- Investigative tools that discover relevant information related to the subject of interest.
- Tools known to be used by hackers.
- Tools that are used in cybersecurity.

WE DIVIDE THE ACTUAL PROVISION OF IG SERVICES INTO 5 STEPS:

1. **IDENTIFICATION OF THE OBJECTIVE OR OBJECTIVES**
   The first step is to analyse the organisation. For larger organisations, there is the possibility of focusing only on agreed objectives or parts.

2. **IDENTIFICATION OF INFORMATION SOURCES AND DATA COLLECTION**
   The second step is to identify the different tools and techniques that will be used to collect information about the objective. This step allows the attackers to obtain as much information about the objective as possible.

3. **DATA FILTERING**
   The third step helps to filter the data and convert it into meaningful and actionable information.

4. **ANALYSIS**
   The fourth step combines information from multiple sources.

5. **REPORT**
   The fifth step is reporting to the client. Information detailing risks and mitigations.

INFORMATION GATHERING SERVICES

The primary function of testing is to help IT teams discover publicly accessible assets and map what information could easily become the target of a potential attack.

The tests are then used to analyse where individual vulnerabilities exist in applications, servers, infrastructure, etc.

AS PART OF OUR IG SERVICES, WE FOCUS ON THE FOLLOWING CORE AREAS:

TECHNICAL INFORMATION

- Site
- IP addresses
- Domains and subdomains
- Servers
- Services and applications
- Certificates
- MTA configurations
- DNS zones
- Google hacking

HUMAN RESOURCES

- Employees
- Emails
- Passwords
- Identities
- Social networks

IMPORTANT INFORMATION

- Data leaks
- Dark web

OUR SERVICES AND SOLUTIONS

- Security audits, analyses and consultations
- Penetration tests
- Configuration audits
- Regular health checks
- Expert consultations on ransomware protection
- Analysis of compliance with international authorities *(CISA)*
- Training of administrators and users
- Solutions of emergency situations in cyber incidents

Sonpo

SONPO, a.s. | Prague | Czech Republic
www.sonpo.eu | sales@sonpo.eu