CONFIABILIDADE E SEGURANÇA CIBERNÉTICA
(DACYS)
PL01
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**), Nuno Peralta* ()
{@isep.ipp.pt}

Exercise 1: Information Gathering

All assessments begin with understanding what is the attack surface. This can be what is exposed to the Internet such as devices and services. In this exercise choose a public Internet present institution to answer the following questions:

(a) What is Certificate Transparency (**CT** [1])?

  i) Using **CT**, enumerate all endpoints possible.

(b) Using different search engines such as **Google** [2], **Yandex** [3], and **Bing** [4] what public HTTP/FTP information can you gather on that same institution?

(c) Using the **RIPE** [5] database, what information can you gather?

  i) Using the same database, what information regarding the institution can you gather?

(d) What is **Shodan** [6] and what information can it provide to a company or malicious actor?

(e) What is **Censys.io** [7] and their business aim?

  i) Use **Censys.io** search to search for more information regarding the institution that you choose.

(f) Experiment with **DNS Dumpster** [8]. What information can you gather from it?

(g) Compile all the information gathered disclosing the endpoints (DNS, IP addresses, services, and service version) that you could gather.

(h) What are **vulnerability databases** and their purpose?

  i) Using **exploit-db** [9], **0day.today** [10], **packet storm** [11] and/or others, can you discover potentially vulnerable services? What are those services and how can you exploit them? (**DO NOT EXPLOIT THEM**).

Exercise 2: Replicating OSINT information

Open Source information is of great value to understanding security exposure, however, it is important to replicate that detection using tools already available aligned with the well-known perimeter of the enterprise. Gather some information on the following topic to better understand how can this be included in the company security posture assessment to detect leakages and exposures:

1. What is **amass** [12]?
2. What is **Nuclei** [13]?
3. What is **sublist3r** [14]?
4. What information can **SpiderFoot** [15] provide?
5. What are the inherent problems with using these tools without consent or authorization?
6. How can you use these vectors to protect your organization?
7. Define a plan to automate all this to detect exposures and risks to an organization.
8. If you are defending your organization how can you use these tools aligned with an inventory database (usually known as **CMDB** [16]) to better protect the organization and deliver to different teams the needed information to reduce the attack surface?

Exercise 3: Install a Kali Linux Virtual Machine

To test tools one should always have prepared a virtual disposable environment. This will help in an audit so we keep different clients segregated. It is also a great way to separate the offensive from the normal day-to-day use.

1. Investigate on HyperVisors such as **VMWare** [17] or **VirtualBox** [18].
2. Investigate containers such as **Docker** [19].
3. What is the difference between Virtual Machines and Containers?
4. Investigate about **Qubes-OS** [20]. What are the main security features? What is the main drawback of the solution?
5. Investigate on offensive Linux distributions such as **Kali Linux** [21] and/or **BlackArch** [22]. What is the main purpose of such distributions and why they should not be used daily?
6. Download the **Kali ISO** from the official Website and Install it on a HyperVisor of your choosing.

References

[1] G. Inc., "Certificate transparency: Working together to detect maliciously or mistakenly issued certificates." [Online]. Available: https://certificate.transparency.dev/

[2] Google, "Google." [Online]. Available: http://www.google.com/

[3] Yandex. [Online]. Available: https://yandex.com/

[4] Microsoft. [Online]. Available: https://www.bing.com/

[5] R. NCC, "Ripe network coordination centre." [Online]. Available: https://www.ripe.net/

[6] Shodan. [Online]. Available: https://www.shodan.io/

[7] Censys, "Industry-leading cloud and internet asset discovery solutions," Aug 2022. [Online]. Available: https://censys.io/

[8] HackerTarget, "Dnsdumpster - dns recon and research, find and lookup dns records." [Online]. Available: https://dnsdumpster.com/

[9] OffensiveSecurity, "Offensive security's exploit database archive." [Online]. Available: https://www.exploit-db.com/

[10] 0day Today Team, "0day.today - 0day.today exploit database : Vulnerability ..." [Online]. Available: https://0day.today/reg

[11] PacketStorm. [Online]. Available: https://packetstormsecurity.com/

[12] O. Owasp, "Owasp/amass: In-depth attack surface mapping and asset discovery." [Online]. Available: https://github.com/OWASP/Amass

[13] Projectdiscovery, "Projectdiscovery/nuclei: Fast and customizable vulnerability scanner based on simple yaml based dsl." [Online]. Available: https://github.com/projectdiscovery/nuclei

[14] aboul3la, "Aboul3la/sublist3r: Fast subdomains enumeration tool for penetration testers." [Online]. Available: https://github.com/aboul3la/Sublist3r

[15] Jul 2022. [Online]. Available: https://www.spiderfoot.net/

[16] "Configuration management database," Jun 2022. [Online]. Available: https://en.wikipedia.org/wiki/Configuration_management_database

[17] Sep 2022. [Online]. Available: https://www.vmware.com/

[18] "Virtualbox.org!" [Online]. Available: https://www.virtualbox.org/

[19] Sep 2022. [Online]. Available: https://www.docker.com/

[20] "Qubes-os - a reasonably secure operating system." [Online]. Available: https://www.qubes-os.org/

[21] “Kali linux - penetration testing and ethical hacking linux distribution,” Sep 2022. [Online]. Available: https://www.kali.org/

[22] “Blackarch.” [Online]. Available: https://www.blackarch.org/