**CYBER KILL CHAIN**

**Question** (Identify by Explaining Two Tools, as used for Defence and Attack in the cyber kill chain.)

**7 Phases of the Cyber Kill Chain**

1. **Reconnaissance**

( <https://www.jigsawacademy.com/blogs/cyber-security/reconnaissance-in-hacking/> )

*“A significant instrument as a starting point of numerous data hacking and for penetration testing. The cycle includes gathering data about the target machine that could be utilized to discover its blemishes, weaknesses, and security vulnerabilities.” (Link. Upadhyay)*

Security Engineer tends to become the private eye, gathering data and information to comprehend their victims. They focus on the security part of the innovation, study the shortcomings, and utilize any weakness for their potential benefit

***steps*** *= {*

*Accumulate inceptive data, decide the range of the network, recognize all active machines, get hold of the OS being used, uniquely mark the working framework, reveal services used on ports and understand the network map.*

*}*

1. **Attack: -**

The attacker acquires all necessary information about the target.

The use of either manual methods or automated scanners designed for mapping organizational structures, locating any security gaps and vulnerabilities which can be exploited.

OSINT tools are often use in this instance in order to access necessary information. (Open-source Intelligence)

* **HawkScan** < [**https://docs.stackhawk.com/hawkscan/**](https://docs.stackhawk.com/hawkscan/) :>) Open-source tool available on GitHub. HawkScan is based upon Open-Source Intelligence. Very similar to Metasploit 1 and Metasploit 2. HawkScan provides a command-line interface that you can run on Kali Linux. Used to get information about our target(domain) website and IP address.
* **Shodan.io** < [**https://www.shodan.io/**](https://www.shodan.io/) :>) Hackers can use Shodan to search for numerous servers with weak firewalls to set up backdoors and turn them into botnets for cyber attacks.
* **Nmap** <[**https://nmap.org/presentations/Shmoo06/shmoo-fyodor-011406.pdf**](https://nmap.org/presentations/Shmoo06/shmoo-fyodor-011406.pdf):>) When it comes to attacking devices on a network, you can’t hit what you can’t see. Nmap gives you the ability to explore any devices connected to a network, finding information like the operating system a device is running and which applications are listening on open ports.
* **The Harvester**< [**https://github.com/laramies/theHarvester**](https://github.com/laramies/theHarvester) :>)Gather information such as emails, subdomains, hosts, employee names, open ports and banners from different public sources.
* **Recon\_Dog**< [**https://github.com/s0md3v/ReconDog**](https://github.com/s0md3v/ReconDog) :>) This tool allows you to collect information about any website <technology used, subdomains

1. **Defence: -**

Detecting attempts to scan or gather information by an attacker.

* **Wireshark**< [**https://lifewire.com/wireshark-tutorial-4143298**](https://lifewire.com/wireshark-tutorial-4143298) :>) Network Traffic Sniffer, the go-to network packet capture tool. This tool lets you put your network traffic under a microscope, and then filter and drill down into it, zooming in on the root cause of problems.
* **p0f**< [**https://lcamtuf.coredump.cx/p0f3/**](https://lcamtuf.coredump.cx/p0f3/):>) Utilizes an array of sophisticated, purely passive traffic fingerprinting mechanisms to identify the players behind any incidental TCP/IP communications (often as little as a single normal SYN)

1. **Weaponization**: -
   1. **Attack: -** Attackers use the information gathered during the reconnaissance phase to create malware and ways to exploit found vulnerabilities.

* **Metasploit:** <[**https://www.metasploit.com/**](https://www.metasploit.com/):>) To create a word document with a malicious macro that when executed will connect back to the attacker system.
* **Msfvenom**: < [**https://www.offensive-security.com/metasploit-unleashed/Msfvenom/**](https://www.offensive-security.com/metasploit-unleashed/Msfvenom/):>) This tool was born from the need to generate in a simple and fast way payloads and exploits. msfvenom is a tool of the Metasploit Framework that generate viruses, bots, malware, spyware, Trojan, Worm, reverse shells and more.
  1. **Defence: -** Identification of vulnerabilities and methods of providing adequate security to key resources.

* **Endpoint Protection Tools-** A security solution that addresses endpoint security issues, securing and protecting endpoints against zero-day exploits, attacks, and inadvertent data leakage resulting from human error.
* **Red Hat Enterprise Linux 7-** Offers several ways for hardening the desktop against attacks and preventing unauthorized accesses.

1. **Delivery**: -

An adversary turns over the weapon to the victim.

1. **Attack:** -

Attackers attempt to deliver malware to organisations

* **Rubber Ducky-** A custom USB device emulates a USB keyboard to attack a workstation.
* **Social Platforms-** Adversary use a combination of tactics, including malicious applications, advertisements, plug-ins, and links on social media platforms
* **Mobile Devices-** vishing; the practice of eliciting information or attempting to influence action via the telephone.

1. **Defence:** -

To detect and prevent downloading malicious code.

* **Educating associates-** Getting informed on
* **Sandboxes-** Isolated environment on a network that mimics end-user operating environments. (Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.)
* **Anti-virus programs (Avast)-** A computer program used to detect, prevent and remove malware.
* **Firewalls-** Firewall is a network security system that monitors and controls incoming and outgoing network traffic.
* **Anti-spam mechanisms (Mail Washer)-** spam blocking tool.

1. **Exploitation:** - < <https://www.geeksforgeeks.org/kali-linux-exploitation-tools/> :>)

 A vulnerability is not that effective if it can not be exploited or it could not cause harm to the application.

1. **Attack:** -

Execute malicious code given the identified vulnerabilities

* **Metasploit: -** Exploits the website and validates vulnerabilities
* **BeEF: -** It also allows professional penetration tester using client-side attack vectors to assess the actual security posture of a target environment.

1. **Defence:** -

Preventing the execution of malicious software.

* **SIEM-** (Security Information and Event Management) software to investigate logs and perform analyses to identify suspicious activities,
* **EDR-** (endpoint detection & response)

1. **Installation:** -

Gaining Remote Access or other tools on the victim system allows the adversary to maintain persistence inside the environment.

1. **Attack:** -

Installing malware on a system to gain remote access to the environment.

* **Browser-**< <https://owasp.org/www-community/attacks/Man-in-the-browser_attack> :>)

Used to intercept and manipulate calls between the main application’s executable and its security mechanisms or libraries on-the-fly.

* **Applications-** Emails, social platforms and trojans could contain malicious files that could be download accidentally.

1. **Defence:** -

Detecting an attacker in order to prevent them from gaining access to managing operations.

* **HIPS- (**Host-based Intrusion Prevention System) a program employed to protect critical computer systems containing crucial data against viruses and other Internet malware by alerting or block a trial installation.
* **SCM tools-** (Software Configuration Management) Inspection of changes in the system’s configuration compared to the standard configuration. Determine what changed and who changed it.

1. **Command & Control:** -

<https://www.varonis.com/blog/what-is-c2/> (GRIMMICK, n.d.)

1. **Attack:** -

Adversary uses the C2 servers to remotely execute commands on the attacked computer to maintain and develop the attack.

* **Metasploit (**Poison Ivy**)-** Penetration testing and exploitation framework <<https://www.rapid7.com/db/modules/auxiliary/scanner/misc/poisonivy_control_scanner/> :>)
* **Empire** < <https://www.powershellempire.com/> :>) A tool used to perform file uploads and registry commands to establish remote access

1. **Defence:** - Detect and disrupt communication between the target and the attacker.

* **Rastrea2r("rastreador")-** Open-source command-based IoC (Indicators of Compromise) scanner tool
* **NIDS (**Network Intrusion Detection System**)**
* **Sagan-** Log analysis tool that can integrate reports generated on snort data, so it is a HIDS (Host-based Intrusion Detection System) with a bit of NIDS (Network-based Intrusion Detection System).
* **Zeek-** Network monitor and network-based intrusion prevention system.

1. **Actions on Objectives:** -
2. **Attack:** - Pursue the objectives of an attack, e.g., leaking data (violating data confidentiality), data modification (violating data integrity) or system encryption (violation of data availability).
3. **Defence:** - Stopping the attacker’s actions.

***Reference****: -)*

a. <http://gauss.ececs.uc.edu/Courses/c6056/pdf/kill-chain.pdf>

b. <https://seqred.pl/en/cyber-kill-chain-what-is-it-and-how-to-use-it-to-stop-advanced-methods-of-attack/>