COMMON CYBER THREATS AND ATTACKS

ΕΛΕΝΗ ΒΡΑΝΤΖΑ

M.SC.(HONS), M.SC., CYBEROPS ASSOCIATE, CCNA SECOPS, CCNA SECURITY, CCNA R&S, CCIE (R&S #10286), CCNP, CCDA, CCDP, WLANFE, WLANSE, ITIL FOUNDATION

CISCO ACADEMY ΤΟΥ ΚΕΔΙΒΙΜ ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΕΣΣΑΛΙΑΣ

email: evrantza@uth.gr

CISCO ACADEMY ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΕΣΣΑΛΙΑΣ

Η **Cisco Academy** του Π.Θ. ιδρύθηκε το **2005.**

Τα προγράμματα που υλοποιούνται είναι:

- **CCNA (Cisco Certified Network Associate)**
- **Cisco Certified CyberOps Associate – Κυβερνοασφάλεια**
- **Ταχύρρυθμο CCNA & Cisco Certified CyberOps Associate – Κυβερνοασφάλεια**
- **DevNet Associate (θα τρέξει σύντομα)**

CISCO CERTIFIED CYBEROPS ASSOCIATE – ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Το εκπαιδευτικό πρόγραμμα **«Cisco Certified CyberOps Associate – Κυβερνοασφάλεια»** του ΚΕΔΙΒΙΜ του Π.Θ. έχει διάρκεια **πέντε** (5) μήνες που αντιστοιχεί σε **112 ώρες** (60 διδακτικές ώρες και 52 ώρες επίβλεψη-διόρθωση εργαστηριακών ασκήσεων-πρακτική άσκηση).

Το πρόγραμμα **«Cisco Certified CyberOps Associate–Κυβερνοασφάλεια»** παρέχει βασικές δεξιότητες και γνώσεις απαραίτητες για να ξεκινήσει ο ενδιαφερόμενος την καριέρα του στις επιχειρήσεις κυβερνοασφάλειας.

Το πρόγραμμα προετοιμάζει τους εκπαιδευόμενους για θέσης συνεργάτη σε Κέντρα Επιχειρήσεων Ασφαλείας (Security Operations Center -SOC).

Στο πέρας του προγράμματος οι εκπαιδευόμενοι μπορούν να **προλαμβάνουν**, **ανιχνεύουν** και **υπερασπίζονται** τις απειλές στον κυβερνοχώρο και να έχουν τις απαιτούμενες γνώσεις για την επιτυχή συμμετοχή στην εξέταση πιστοποίησης **“Cisco Certified CyberOps Associate (200-201 CBROPS)”.**

COMMON CYBER THREATS AND ATTACKS

- Cyber Threats
- Types of Malware (lab: Anatomy of Malware)
- Network Attacks (lab: Attacking a mySQL Database)
- Evasion Methods
- Threat Actor Tools

THREAT, VULNERABILITY, EXPLOIT AND THREAT ACTORS

Threat is a potential danger to an asset such as data or the network itself.

Vulnerability is a weakness in a system or its design that could be exploited by a threat.

Exploit is the mechanism that is used to leverage a vulnerability to compromise an asset.

Threat actors are called the intruders who gain access by modifying software or exploiting software vulnerabilities.

TYPES OF THREATS

After the threat actor gains access to the network, four types of threats may arise.

- **Information theft** is breaking into a computer to obtain confidential information.
- **Data loss and manipulation** is breaking into a computer to destroy or alter data records.
- **Identity theft** is a form of information theft where personal information is stolen for the purpose of taking over the identity of someone.
- **Disruption of service** is preventing legitimate users from accessing services to which they are entitled.

TYPES OF MALWARE

Malware is short for **mal**icious soft**ware** or malicious code.

It is code or software that is specifically designed to **damage**, **disrupt**, **steal**, or generally inflict some other “bad” or illegitimate action on data, hosts, or networks.

The most common types of malware:

- Viruses
- Trojan Horses
- Worms
- Ransomware

VIRUSES

A virus is a type of malware that **spreads by inserting a copy of itself into another program**. After the program is run, viruses then spread from one computer to another, infecting the computers.

Most viruses **require human help** to spread.

VIRUSES

Viruses can lay dormant for an extended period and then activate at a specific time and date.

Viruses can be harmless, such as those that display a picture on the screen, or they can be destructive, such as those that modify or delete files on the hard drive. Viruses can also be programmed to mutate to avoid detection.

Most viruses are now spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

TROJAN HORSES

Trojan horse malware is software that **appears to be legitimate**, but it contains malicious code which exploits the privileges of the user that runs it. Often, Trojans are found attached to online games.

Users are commonly tricked into loading and executing the Trojan horse on their systems. While playing the game, the user will not notice a problem. In the background, the Trojan horse has been installed on the user's system. The malicious code from the Trojan horse continues operating even after the game has been closed.

TROJAN HORSES

The Trojan horse concept is flexible. It can cause immediate damage, provide remote access to the system, or access through a back door.

It can also perform actions as instructed remotely, such as "send me the password file once per week." This tendency of malware to send data back to the cybercriminal highlights the need to monitor outbound traffic for attack indicators.

Custom-written Trojan horses, such as those with a specific target, are difficult to detect.

TROJAN HORSE CLASSIFICATION

Type of Trojan Horse	Description
Remote-access	Enables unauthorized remote access.
Data-sending	Provides the threat actor with sensitive data, such as passwords.
Destructive	Corrupts or deletes files.
Proxy	Uses the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP	Enables unauthorized file transfer services on end devices.
Security software disabler	Stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Slows or halts network activity.
Keylogger	Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form.

WORMS

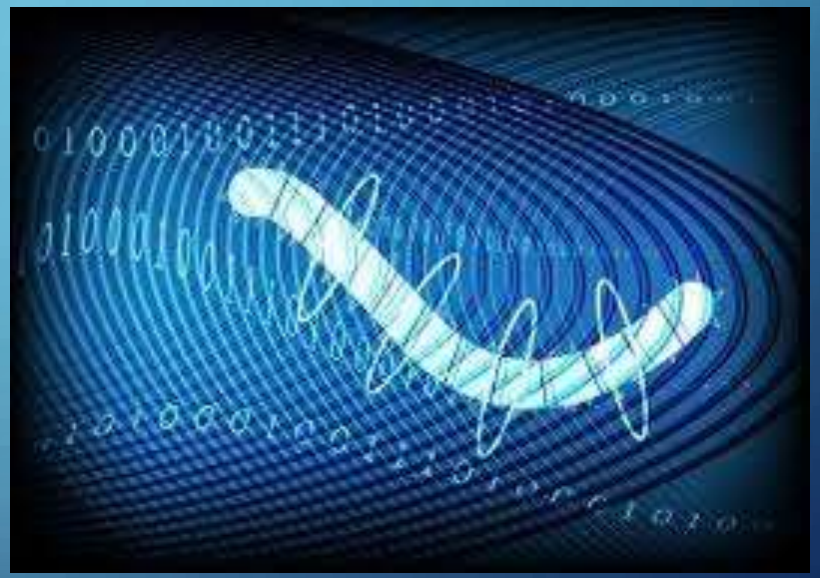
Computer worms are similar to viruses because they replicate and can cause the same type of damage. Specifically, worms **replicate themselves** by independently exploiting vulnerabilities in networks. Worms can slow down networks as they spread from system to system.

Whereas a virus requires a host program to run, **worms can run by themselves**. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network.

WORM COMPONENTS

Most worm attacks consist of three components:

- **Enabling vulnerability** - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
- **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload** - Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor access to the infected host or to create a DoS attack.



RANSOMWARE

- Ransomware typically denies a user access to their files by **encrypting the files** and then displaying a message demanding a **ransom for the decryption** key.
- Users without up-to-date backups must pay the ransom to decrypt their files.
- Payment is usually made using wire transfer or crypto currencies such as Bitcoin.

OTHER MALWARE

Type of Malware	Description
Spyware	Used to gather information about a user and send the information to another entity without the user's consent. Spyware can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
Adware	Displays annoying pop-ups to generate revenue for its author. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.
Scareware	Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. It is generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogus threat.
Rootkits	Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.

COMMON MALWARE BEHAVIORS

Computers infected with malware often exhibit one or more of the following symptoms:

- Appearance of strange files, programs, or desktop icons
- Antivirus and firewall programs are turning off or reconfiguring settings
- Computer screen is freezing or system is crashing
- Emails are spontaneously being sent without your knowledge to your contact list
- Files have been modified or deleted
- Increased CPU and/or memory usage
- Problems connecting to networks
- Slow computer or web browser speeds
- Unknown processes or services running
- Unknown TCP or UDP ports open
- Connections are made to hosts on the Internet without user action
- Strange computer behavior

TYPES OF NETWORK ATTACKS

There are three major categories:

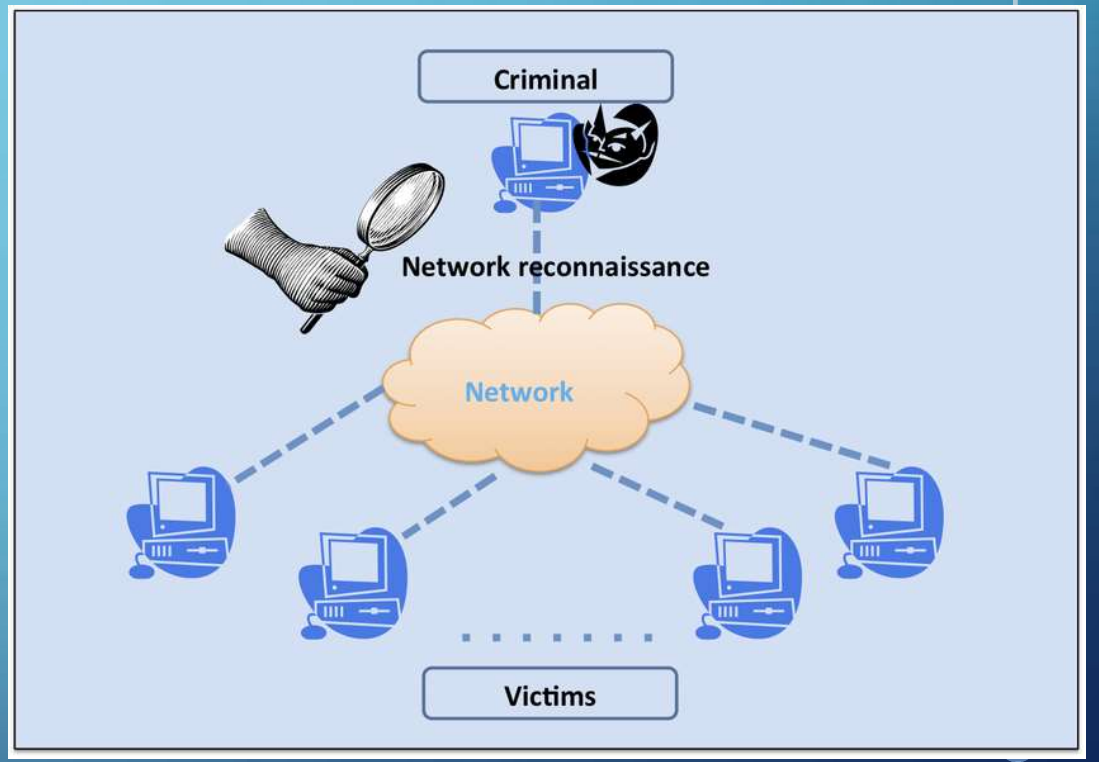
- Reconnaissance Attacks
- Access and Social Engineering Attacks
- DoS Attacks

RECONNAISSANCE ATTACKS

Reconnaissance is information gathering.

Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities.

Recon attacks precede access attacks or DoS attacks.



RECONNAISSANCE ATTACKS

Some of the **techniques** used by malicious threat actors to conduct reconnaissance attacks are:

Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

ACCESS ATTACKS

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of this type of attack is to **gain entry** to web accounts, confidential databases, and other sensitive information.

Threat actors use access attacks on network devices and computers to **retrieve data**, **gain access**, or to **escalate access privileges** to administrator status.

Password Attacks

In a password attack, the threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.

Spoofing Attacks

In spoofing attacks, the threat actor device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing.

ACCESS ATTACKS

Other Access attacks include:

- Trust exploitations
- Port redirections
- Man-in-the-middle attacks
- Buffer overflow attacks

SOCIAL ENGINEERING ATTACKS

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information.

Some social engineering techniques are performed in-person while others may use the telephone or internet.

Social engineers often rely on people's willingness to be helpful. They also prey on people's weaknesses. The threat actor could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

SOCIAL ENGINEERING ATTACKS

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.
Something for Something	Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.
Baiting	A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.
Impersonation	In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents.

DENIAL OF SERVICE (DOS) ATTACK

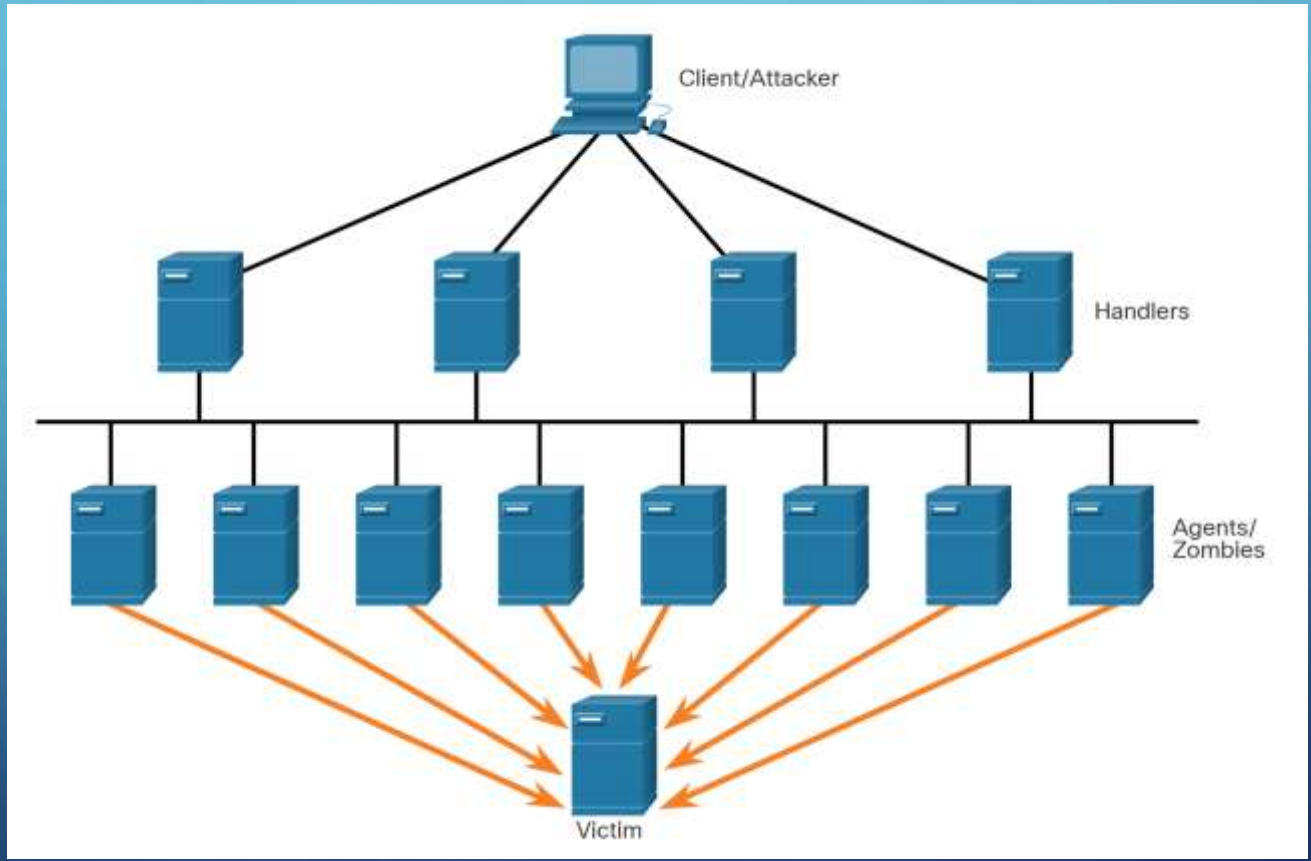
A Denial of Service (DoS) attack creates some sort of interruption of network services to users, devices, or applications.

There are two major types of DoS attacks:

- **Overwhelming Quantity of Traffic** - The threat actor sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes transmission and response times to slow down. It can also crash a device or service.
- **Maliciously Formatted Packets** - The threat actor sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. This causes the receiving device to run very slowly or crash.

DISTRIBUTED DOS ATTACK (DDOS)

A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources.



COMPONENTS OF A DDOS ATTACK

Component	Description
zombies	This refers to a group of compromised hosts (i.e., agents). These hosts run malicious code referred to as robots (i.e., bots). The zombie malware continually attempts to self-propagate like a worm.
bots	Bots are malware that is designed to infect a host and communicate with a handler system. Bots can also log keystrokes, gather passwords, capture and analyze packets, and more.
botnet	This refers to a group of zombies that have been infected using self-propagating malware (i.e., bots) and are controlled by handlers.
handlers	This refers to a master command-and-control (CnC or C2) server controlling groups of zombies. The originator of a botnet can use Internet Relay Chat (IRC) or a web server on the C2 server to remotely control the zombies.
botmaster	This is the threat actor who is in control of the botnet and handlers.

BUFFER OVERFLOW ATTACK

The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it. Exploiting the buffer memory by **overwhelming it with unexpected values** usually renders the system inoperable, creating a DoS attack.

For example, a threat actor enters input that is larger than expected by the application running on a server. The application accepts the large amount of input and stores it in memory. The result is that it may consume the associated memory buffer and potentially overwrite adjacent memory, eventually corrupting the system and causing it to crash.

An early example of using malformed packets was the **Ping of Death**.

It is estimated that one third of malicious attacks are the result of buffer overflows.

SQL INJECTION ATTACK

SQL injection is a code injection technique that is used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

SQL INJECTION ATTACK EXAMPLE

If an attacker with the username wiley enters the string "name' OR 'a'='a" for itemName, then the query becomes the following:

SELECT * FROM items

WHERE owner = 'wiley'

AND itemname = 'name' OR 'a'='a';

The addition of the OR 'a'='a' condition causes the where clause to always evaluate to **true**, so the query becomes logically equivalent to the much simpler query:

SELECT * FROM items;

This simplification of the query allows the attacker to bypass the requirement that the query only return items owned by the authenticated user; **the query now returns all entries stored in the items table, regardless of their specified owner.**

CROSS-SITE SCRIPTING (XSS) ATTACK

Cross site scripting attacks happen when user-submitted content that has not been sanitized is displayed to other users. The most obvious version of this exploit is where one user submits a comment that includes a script that performs a malicious action, and anyone who views the comments page has that script executed on their machine.

Cross-Site Scripting (XSS) is where web pages that are executed on the client-side, within their own web browser, are injected with malicious scripts. These scripts can be used by Visual Basic, JavaScript, and others to access a computer, collect sensitive information, or deploy more attacks and spread malware.

CROSS-SITE REQUEST FORGERY (CSRF) ATTACK

Cross Site Request Forgery (CSRF), sometimes pronounced “Sea Surf” is another type of attack that shares some aspects of XSS attacks. In both cases, the attacker intends for the user to execute the attacker’s code, usually without even knowing it.

The difference is that CSRF attacks are typically aimed not at the target site, but rather at a **different** site, one into which the user has already authenticated.

Here is an example. Let’s say the user logs into their bank website, **http://greatbank.example.com**. In another window, they are on a discussion page that includes an interesting looking link, and they click it.

Unfortunately, the link was for

http://greatbank.example.com/changeemail?new_email=attacker@example.com.

The browser thinks this is just a normal link, so it calls the URL, sending the cookies for greatbank.example.com, which, as you recall, include the user’s authentication credentials. As far as the bank is concerned, this request came from the user, and it executes the change. Now the attacker can go ahead and change the user’s password, then log into the bank and do whatever damage they want.

Note that even if the user is smart enough not to click on a strange link like that, if a site is vulnerable to XSS attacks, this attack can be carried out without the user having to do anything. A carefully crafted <img> tag can achieve the same result.

EVASION METHODS

Evasion Method	Description
Encryption and tunneling	This evasion technique uses tunneling to hide, or encryption to scramble, malware files. This makes it difficult for many security detection techniques to detect and identify the malware. Tunneling can mean hiding stolen data inside of legitimate packets.
Resource exhaustion	This evasion technique makes the target host too busy to properly use security detection techniques.
Traffic fragmentation	This evasion technique splits a malicious payload into smaller packets to bypass network security detection. After the fragmented packets bypass the security detection system, the malware is reassembled and may begin sending sensitive data out of the network.
Protocol-level misinterpretation	This evasion technique occurs when network defenses do not properly handle features of a PDU like a checksum or TTL value. This can trick a firewall into ignoring packets that it should check.
Traffic substitution	In this evasion technique, the threat actor attempts to trick an IPS by obfuscating the data in the payload. This is done by encoding it in a different format. For example, the threat actor could use encoded traffic in Unicode instead of ASCII. The IPS does not recognize the true meaning of the data, but the target end system can read the data.

EVASION METHODS (ΣΥΝΕΧΕΙΑ)

Evasion Method	Description
Traffic insertion	Similar to traffic substitution, but the threat actor inserts extra bytes of data in a malicious sequence of data. The IPS rules miss the malicious data, accepting the full sequence of data.
Pivoting	This technique assumes the threat actor has compromised an inside host and wants to expand their access further into the compromised network. An example is a threat actor who has gained access to the administrator password on a compromised host and is attempting to login to another host using the same credentials.
Rootkits	A rootkit is a complex attacker tool used by experienced threat actors. It integrates with the lowest levels of the operating system. When a program attempts to list files, processes, or network connections, the rootkit presents a sanitized version of the output, eliminating any incriminating output. The goal of the rootkit is to completely hide the activities of the attacker on the local system.
Proxies	Network traffic can be redirected through intermediate systems in order to hide the ultimate destination for stolen data. In this way, known command-and-control not be blocked by an enterprise because the proxy destination appears benign. Additionally, if data is being stolen, the destination for the stolen data can be distributed among many proxies, thus not drawing attention to the fact that a single unknown destination is serving as the destination for large amounts of network traffic.

EVOLUTION OF SECURITY TOOLS

Categories of Tools	Description
password crackers	Passwords are the most vulnerable security threat. Password cracking tools are often referred to as password recovery tools and can be used to crack or recover the password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password and access the system. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.
wireless hacking tools	Wireless networks are more susceptible to network security threats. Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.
network scanning and hacking tools	Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
packet crafting tools	Packet crafting tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples of such tools include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.
packet sniffers	Packet sniffers tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.
rootkit detectors	A rootkit detector is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.

EVOLUTION OF SECURITY TOOLS (ΣΥΝΕΧΕΙΑ)

Categories of Tools	Description
fuzzers to search vulnerabilities	Fuzzers are tools used by threat actors when attempting to discover a computer system's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.
forensic tools	White hat hackers use forensic tools to sniff out any trace of evidence existing in a particular computer system. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.
debuggers	Debugger tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.
hacking operating systems	Hacking operating systems are specially designed operating systems preloaded with tools and technologies optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, SELinux, Knoppix, Parrot OS, and BackBox Linux.
encryption tools	These tools safeguard the contents of an organization's data when it is stored or transmitted. Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Examples of these tools include VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN, and Stunnel.
vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit, and Netsparker.
vulnerability scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of these tools include Nipper, Securia PSI, Core Impact, Nessus, SAINT, and Open VAS.

ΕΥΧΑΡΙΣΤΩ

Cisco Academy of University of Thessaly

Ελένη Βράντζα (evrantza@uth.gr)

ΚΕΔΙΒΙΜ του Πανεπιστημίου Θεσσαλίας (https://learning.uth.gr/)


HR
klossner
" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."