Komendy:

- Tracert (Windows) / traceroute (Linux) – route a packet takes to destination, takes advantages of ICMP TTL packets
- Nslookup (Windows, Linux)
- Dig (Linux)– Domain Information Groper
    - Like nslookup, but more advanced domain information
- Ipconfig (Windows) / ifconfig (Linux)
- Ping
    - Sends ICMP packages
- Pathping (Windows)
    - Combine ping and traceroute (Windows)
- Netstat
    - – a – show all active connections
    - – b – show binaries
    - – n – don't resolve names
    - –r – displays routing table
- Arp – a – view local ARP table (determine MAC addr based on IP)
- Route
    - Route print (Windows)
    - Netstat – r – Linux
    - View local routing table
- Curl – client URL, grab the raw data, transfer data from or to a server
    - tool used to download or upload data to a server via any of the supported protocols, such as FTP, HTTP, SMTP, IMAP, POP3, or LDAP
- Hping
    - Ping, that can send almost everything (ICMP, TCP, UDP)
    - Used for security auditing and testing of firewalls and networks
- Nmap
    - NSE – Nmap Scripting Engine
- The Harvester
    - OSINT tool, get email and subdomains from public sources
- Sn1per
    - Combine many reconessance tools into single framework: dnsenum, metasploit, nmap, Harvester
- Scanless
    - Port scan proxy
    - Your IP is hidden
- Dnsenum
    - Enumerate DNS information, find host names in Google, view host information from DNS servers
- Nessus
- Cuckoo – sandbox for malware (virtualized environment)
- Netcat
    - Hacking tool that can read from and write to network connections (TCP and UDP)

Bardziej linuxowe komendy (ale I Windowsowe):

- Cat – wyświetlanie lub łącznie plików
- Head – pierwsze 5 linii pliku
- Tail
- Grep
- Chmod
    - U – user, g –group, o – other
    - –rwx rwx rwx, pierwszy symbol oznacza plik lub jeśli jest d to directory
    - Chmod a-w file.txt – all users no writing permissions to file.txtx
- Logger – add entries to systemlog (syslog)
- Powershell - .ps1 file extension, uses cmdlets
- Openssl – build certificates, manage TLS/SSL, message digests, encryption&decryption
- Wireshark
- Tcpdump – capture packets, commandline tool
- Tcpreplay – suite of packet replay utilities, replay and edit packet captures, send hundrets or thousands flows per second

Komendy z obszaru forensics:

- Dd
    - Create bit-by-bit **copy of a drive**
    - Create a disk image dd if=/dev/sda of= /tmp/sda-image.img
    - Clone disks, partitions and files, erase disks
- Memdump
    - Copy information in system memory to the standard output stream
    - **Dump physical or kernel memory**
- WinHex
    - Universal hex editor, edit disks, files, RAM
    - Secure wipe, disk cloning
    - **Examine files, recover files, search for specific type**
- FTK imager
    - Acquiring **disk images**
- Autopsy
    - Acquiring **disk images**
    - Perform digital forensics **of hard drives, smartphones**

Zbiór pojęć I informacji:

- Exploitation frameworks (metasploit, SET – Social Engineering Tool)
- **Pamiętaj:** Lockhead martin cyber kill chain – atakujący nie wycofa się
- Tabletop exercises – incident response exercises
- data sanitization = dod standard
- Stakeholder management – keeping good relationships with customers
- DRC – Disaster Recovery Plan
- BCP – Business Contuinity Plan
- COOP – Continuity Of Operations Planning
- MITRE ATT&CK
- Diamond Modelstake
    - methodology framework for intrusion analysis developed by U.S. government intelligence community

- Cyber Kill Chain
    - Recon, Weponization, Delivery, Exploit, Installation, C&C, Actions
    - 7-step military model adopted by Lockheed Martin to identify the phases of a cyberattack
- NVD – National Vuln Database
- SIEM – Security Information and Event Management
- Logi
    - Event Viewer / Application Log (Windows)
    - /var/log (Linux)
- Syslog
    - Standard for message logging, often integrated into SIEM, each log entry labeled
- Journalctl (Linux)
    - Method for quering the system journal
- NetFlow
    - Probe network communication
- IPFIX – IP Flow Information Export
    - Newer NetFlow
    - IETF specification that defines how IP flow information is to be formatted and transferred from an exporter to a collector
- sFlow – Sampled Flow
    - portion of actual network traffic
- runbook
    - linear
- playbook
    - conditional steps to follow
- legal hold
- ESI – Electronically Stored Information
- Different filesystems store timestamps different
    - FAT – time in local time
    - NTFS – time in GMT
- Swap / pagefile
    - A place to store RAM whgen memory is depleted
    - Transfer pages of RAM to a storage
- Snapshot
    - Image of VMs
    - Incremental between snapshot
- Artifacts
- E-discovery
    - Gathering data required by the legal process
- MAC – Message Authentication Code
    - 2 parties verify non-repudiation
- Digital signature
    - Non-repudiation can be publicly verified
- Strategic intelligence
- Counterintelligence (offensive)
    - Chronimy nas samych przeciwko szpiegostwu itp.

- Chain of custody – przekazywanie materiały dowodowego między osobami i dokumentacja tych poczynań
- Hashing – integrity + authenticity
- Checksum – integrity
- SIP – Session Initiation Protocol (wykorzystywany w VoIP)
- Banner grabbing - The practice of connecting to an open port on a remote host to gather more information about its configuration
- Sensivity labels - SIEM dashboard configuration setting provides a countermeasure against false positive/negative errors
- Siem dashboard - A correlation engine used for processing various types of log data into an actionable information
- utilities that enable logging of data from different types of systems in a central repository include
    - NXlog (cross-platform log-managing tool)
    - Wszystkie inne syslogi

Ulotność danych

1. CPU register, CPU cache
2. Router table, ARP cache, process table, kernel stats, memory
3. Temporary file systems / swap space
4. Disk
5. Remote logging and monitoring
6. Physical configuration / network topology
7. Archival media

Cache memory -> RAM -> Swap/Pagefile -> Temporary files -> Disk files -> Archival media

Czyszczenie dysków

Data sanitization - przypadki:

- CE - cryptographic erase - effective for encrypted devices (mostly SED)

The encryption key itself is destroyed during the erasing operation. CE is a feature of self-encrypting drives (SED) and is often used with solid-state devices. Cryptographic erase can be used with hard drives, as well.

- zero-fill - is not effective on SSDs or hybrid drives

- SE – secure erase – dysk musi mieć SE utility (flash-based devices)

Data sanitization - techniki:

- physical destruction - nie ma nośnika, nie ma problemu

- destroying data - uniemożliwienie odzyskania informacji, ale także uniemożliwienie ponownego wykorzystania samego nośnika

- purging - trwałe zniszczenie danych, ale bez zniszczenia nośnika. Nawet w laboratorium nie odzyska się, przykłady: degaussing, cryptographic erase, other non-destructive techniques

Some generic magnetic storage devices can be reused after the degaussing process has finished, such as VHS tapes and some older backup tapes. For this reason, though, the technique of degaussing is classified as purging and not destruction, even though hard drives are rendered unusable after being degaussed.

- clearing data - usunięcie danych, ale w laboratorium je odzyskasz, nadpisywanie danych raz lub kilka razy

- Erasing or deleting - usuń, do kosza wyrzuć, łatwe do cofnięcia, dane można odzyskać

Podsumowanie: Destroying > degaussing / purging > clearing > erasing

Syslogi

- Syslog – 1980, only UDP
- Syslog-ng – 1998, added TCP and TLS encryption
- Rsyslog – added buffer operations

Netflow	**sFlow**
Cisco	HP
Only collect IP traffic	Traffic for OSI 2-7
No packet sampling	packet sampling (only portion of the actual network traffic)
Exporter / cache(analyzer)	Agent / collector

Netflow does not capture the full packet capture of data as it crosses the network sensor but instead captures metadata and statistics about the network traffic.

This metadata can highlight trends and patterns in the traffic generated by the malicious user, such as the volume of data sent and received.