Social engineering:

- Elicitation – wydobywanie informacji od ludzi nie powodując u nich przekonania że są przesłuchiwani
- Flattery – dawanie komplementów
- Bracketing – próba oszacowania jakiejś wartości
- Confidential bait – przekazanie komuś poufnej informacji licząć że ten się odwdzięczy

Pojęcia:

- Typosquatting – literówki w urlu
    - URL hijcaking
- Prepending – dodawanie czegoś do czegoś, na przykład w urlu dodawanie tej samej literki: zamiast facebook.com to ffacebook.com
    - Inna definicja tyczy się oznaczania ludzi w social mediach
- Pretexting – tworzenie pretekstu w phishingu
- Pharming – docieranie do szerokiej grupy odbiorców poprzez przekierowania sieciowe
    - Redirect traffic to poisoned website, DNS poisoning)
    - Credential harvesting
- Phishing
- Vishing
- Smishing
- Spoofing – czyli podszywanie się pod coś, na przykład MAC spoofing, IP spoofing
- Spearphishing – skupianie się na danej osobie lub szczególnej grupie osób
- Whaling – skupianie się na „grubej rybie”
- Impersonation – podszywanie się pod jakąś osobę
- Identity fraud
- Dumpster diving
- Shoulder surfing
- Privacy filter
- Hoax – wiadomości łańcuszkowe, prośby żeby przekazać dalej
- Watering hole attack – atak skierowany na szeroką grupę odbiorców, wiemy na przykład że dane strony np. KNFu są odwiedzane przez pracowników banku więc próbujemy wrzucać malware na te strony
- Defense-in-depth
- rDNS – reverse DNS – taki koncept że walidujemy adresy lub emaile poprzez sprawdzenie adresów IP, z którymi są w DNS powiązane żeby sprawdzić, czy pochodzą z legitnych źródeł
- tarpitting – spowalnianie konwersacji jako sposób bronienia się przed atakującym
- tailgating
- invoice scam
- credential harvesting
- cloning - making an unauthorized copy of a payment card

Sposoby wpływania na ludzi w social engineering:

- authority – władza połączona z takim poszanowaniem a.k.a twój szef lub policjant w ładnym mundurze
    - knowledge of systems, technical jargon
- Intimidation – zastraszenie

- Consensus / Social proof – dużo osób Ci coś radzi
- Scarcity – mało czegoś, ale nie tylko w kontekście czasu, coś może być np. tanie lub na promocji
- Urgency
- Familiarity/Liking – mutual friends
- Trust

Wirusy i inne złe rzeczy:

- Malware
- Virus
    - Requires user interaction
- fileless virus
    - operates in memory
- worm
- SMBv1 – Ethernal Blue – DoublePulsar – WannaCry
- Ransomware
- Crypto-malware
- Trojan horse
- Rootkit – silny malware, może być bardzo nisko zakorzeniony, przed bootowaniem systemu może się odpalać
    - Installs itself at the OS or kernel level to avoid detection, loads before OS loads, can disable anti-virus
- Secure Boot = UEFI
- Adware
- Spyware
- Bot, botnet
- Logic bomb

Ataki i podatności:

- Collision – te same hasze produkują inne ciągi znaków, niedobrze
- Spraying attack – różne hasła i loginy i bawimy się
    - bypasses account-lockout policies
- Dictionary attack – jest jakiś zestaw słów
- Rainbow table – tablica ze skrótami haszy
- Skimming – kopiowanie zawartości paska magnetycznego karty płatniczej
- Birthday attack – liczymy na to, że są kolizje
- Downgrade attack
- Horizontal privilege escalation – na inne konta, urządzenia
- Data Execution Prevention
- Stored XSS
- Buffer overflow – dostanie się do innych miejsc w pamięci niż te przeznaczone na działanie aplikacji
- Replay attack
- Network tap – zbiera ruch sieciowy
- ARP poisoning – zatrucie tablicy ARP w switchu i wtedy on zmienia się w HUBa, albo można mu własne jakieś wpisy zrobić

- Pas the hash
- Session hijacking (sidejacking)
- XSRF, CSRF, sea-surf
    - Exploiting a website's trust
    - Server perform an action
- XSS
    - The browser runs malicious code
- SSRF – Server Side Request Forgery
- Driver
- Shimming – jakaś przestrzeń, luka do wypełnienia
    - Shimming is a cyberattack technique that allows attacker to insert malicious code into a legitimate process or app
- Metamorphic malware
- SSL stripping
- SSL 3.0 POODLE attack
- Race condition
- Memory leak – pamięć nie jest w ogóle zwracana przez aplikację w wyniku czego się w końcu wyczerpuje
- NULL pointer dereference – skieruj program na puste miejsce w pamięci i może zwróci jakiś ciekawy błąd
- Integer overflow
    - When a result of an arithmetic operation exceeds the maximum size of int type used to store it
- Directory traversal
- Resource exhaustion – one device can also do it
- ZIP bomb
- DHCP starvation – kończą się adresy IP w sieci/podsieci
- Rouge access point – access point, którego nie powinno być u nas, ktoś np. włączył thethering, hotspot mobilny
- Evil twin – to samo SSID, ktoś podszywa się pod prawdziwy Access Point
- Bluejacking – wysyłanie unsolicited messages via BlueTooth
- Bluesnarfing – access to data
- Disassociation attack
- RF (Radio Frequency) jamming – zakłócanie sygnału innym
- Reactive jamming – zakłócanie, ale gdy ktoś próbuje się do sieci podłączać
- Fox hunting – szukamy skąd zakłócenia

Inne pojęcia dalej:

- Crypto nonce
- IV – Initialization Vector
- On path attack – MITM
- ARP – masz IP daj MAC
- On path browser attack – MITB
- MAC budowa:
    - 48 bitów, czyli 6 bajtów
    - Pierwsze 3 bajty to manufactorer (OUI)

    - Kolejne 3 bajty to serial number (NIC)
    - LAN switch bazuje na MAC addr
- MAC flooding – tablica MAC w switchu pomieści ograniczoną ilość adresów MAC, switch zmienia się w HUB
- MAC spoofing / cloning
- DNS poisoning
- Domain hijacking – przejęcie domeny po prostu
- URL hijacking – rejestrowanie podobnie brzmiących domen
- Outright misspelling – e na o się zmienia w urlu na przykład
- Different top-level domain
- Layer 2 loop without STP
- DDOS amplification – uses protocols like NTP, DNS, ICMP
- Downtime – przestój
- Ps1 – powershell
- Shadow IT
- Hacker on a chip – malicious USB, po podłączeniu staje się klawiaturą
- Firmware = BIOS
- Syslog – standard for message logging
- Passive footprinting – zbieranie informacji z open source
- Wardriving / warflying – szukanie hotspotów w różnych lokalizacjach
- Active footprint – „trying the doors”, port, ping scans
- Purple team – połączenie red team I blue team
    - The purple team is made up of both the blue and red teams to work together to maximize their cyber capabilities through continuous feedback and knowledge transfer between attackers and defenders
- White team – manages interactions between red and blue team, enforces the rules, determines score, results
    - The white team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission
- Privacy screen – mitigation to shoulder surfing
- Smurf attack – DDOS using ICMP and spoofing IP
- pfSense – firewall bazujący na systemie operacyjnym FreeBsd
- darkweb – is a tiny portion of deepweb
- I2P – Invisible Internet Protocol – pozwala na połączenia do deepweb
- BitBucket – taki github dla przedsiębiorstw
- Tribal knowledge – older platforms may have fewer people who are subjcet matter experts
- Bounce rate – wskaźnik jaki procent użytkowników opuszcza stronę zaraz po wejściu zamiast zostać
- .bat – batch file, script file for Windows

Różne postaci jako atakujący:

- Insiders
- Nation state
- Hacktivist

- Script kiddie
- Organized crime
- Hackers
- Competitors

Różne grupy jako atakujący:

- Black hat – zły hacker ze złymi intencjami
- Gray hat – ktoś kto nielegalnie testuje zabezpieczenia ale bez złych intencji
- Blue hat – outside security consulting team employed to bug test
- Criminal syndicates – chcą kasy za włamanie

Skrótowce :

- SPIM – Spam Over Instant Messages
- PUP – Potentially Unwanted Program
  - A type of computer program not explicitly classified as malware by AV software
  - An application downloaded and installed with the user's consent (legal app)
- RAT – Remote Access Trojan
- HID – Human Interface Device – wpinasz pendrive znaleziony na ulicy a on zaczyna pisać
- TOC TOU – Time Of Check to Time Of Use
- RFID – Radio Frequency Identification
  - ARPT – Active Reader Passive Tag
  - ARAT – Active Reader Active Tag
- NFC – Near Filed Communication
- OT – Operational Technology
- VBA – Visual Basic for Application, kojarzyć z officem
- APT – Advanced Persistent Treat
- RFC – Request For Comments
- TTP – Tactics Technics Procedures
- SOAR – Security Orchestration, Automation and event Response
- OSINT – Open Source Intelligence
- RoE – Rules of Engagement
  - What activities are allowed during pentest (white team)
- IoC – Indicator of Compromise
- KPA – Known Plaintext Attack – atak bazujący na znajomości plaintextu i ciphertextu i w ten sposób można łamać klucze krypto
- GHDB – Google Hacking Database
- NVD – National Vuln Database
- ISAC – Information Sharing and Analysis Center
- NCCIC – National CyberSec and Communication Integration Center
- I2P – Invisible Internet Protocol – pozwala na połączenia do deepweb
- AIS – Automated Indicator Sharing
  - Free sharing service, shares indicators between government and private entities
- STIX – Structured Threat Information Expression (format)
- TAXII – Trusted Automated Exchange of Indicator Information (transport protocol that allows sharing info over HTTPS)
- CRL – Certificate Revocation List

- BPC – Business Process Compromise
    - Manipulacja procesami
- CCPA – California Consumer Privacy Act
- GDPR
- TI analyst – Threat Intelligence analyst
- CISO – Chief Information Security Officer
    - Risk management
- CVE – Common Vulnerabilities and Exposures
    - Maintained by MITRE
- CVSS – Common Vulnerability Scoring System (od 0 do 10)
- SDK – Software Development Kit
    - A set of software tools or programs provided by hardware and software vendors that developers can use to build apps
- WTLS – Wireless Transport Layer Security
    - Security level for WAP
- PED – Portable Electronic Device – device used in a debit, credit, smartcard based transactions to enrypt cardholder's personal number
- IRM – Information Rights Management
- SPIT – Spam over Internet Telephony

Wiedza rozszerzana w kolejnych domenach:

- 802.1X Network Access Control
- 802.11 wireless, no security
- 802.11w – secure version
- 802.11 ac – also secure
- WPA2 podatne na KRACK (Key Reinstallation Attack)
- WEP, WPA – starsze protokoły względem WPA2, podatne
- MD5 – funkcja haszująca przestarzała, tylko SHA256
- Które protokoły wysyłają w plaintext:
    - Znam: Telnet, FTP, http
    - Nie znam: IMAP, POP, SMTP
- CVSS – Common Vulnerability Scoring System (od 0 do 10)

Standard (protocol)	Method
WEP	RC 4 stream
WPA	TKIP
WPA2	AES CCMP

Słabe protokoły krypto:

- RC4
- 3DES

Angielskie słówka:

- Fusing the data – łączenie danych
- Tainted – skażone
- Countermeasure – środek zaradczy

- Motherboard – płyta główna
- Auxliary – pomocniczy
- Explicitly – wyraźnie
- Facilitate – ułatwiać
- Digest – skrót
- Malfunction – niesprawność
- trust a website has in the user's web browser – zaufanie, którym strona internetowa darzy przeglądarkę użytkownika
- ATM machine – bankomat
- Espionage – szpiegostwo
- USB stick – pendrive
- Vetting process – proces weryfikacyjny
- Proprietary – prawnie zastrzeżony
- Enterprise - przedsiębiorstwo
- Acquision – nabytek
- Covertly – potajemnie
- Liability – odpowiedzialność
- Firmware – oprogramowanie sprzętowe
- Forged packets – sfałszowane pakiety
- Derivative content – treści pochodne – new contect that is created from existing content by reusing it in different forms
- Cross-platform – wieloplatformowe
- Disgruntled – niezadowolone
- Semi-authorized – częściowo uprawnione
- Divulge - ujawniać