**URG** - dane w pakietach są bardzo wazne i należy je natychmiast przesłać

**PSH**  - instruuje system wysyłający, by wysłać wszystkie zbuforowane dane natychmiastowo

**enumeracja**: proces wyciągnięcia informacji o targetowanym hoscie (nazwy userow, maszyn, serwisów, plików sharowanych itp).

**mac** 48 bitów / 3 bajty producent karty / reszta unikatowa (lub 6 bajtowy - 3 bajty producent karty, 3 pozostałe info).

**PED** - personal eletronic device

**TPM**—Trusted Platform Module. This is a hardware chip on the motherboard included on many newer laptops. A TPM includes a unique RSA asymmetric key, and it can generate and store other keys used for encryption, decryption, and authentication. TPM provides full disk encryption.

**Encrypting File System (EFS)** – system szyfrowania plików, wprowadzony dla systemu plików NTFS w wersji 3.0 przez firmę Microsoft dla systemów Windows. EFS umożliwia szyfrowanie plików z poziomu systemu aby zapewnić ochronę poufnych danych przed atakami osób, które mają fizyczny dostęp do komputera.

**CRL** - revoced certification - lista certyfikatów unieważnionych przez organ certyfikujący z różnych powodów. Dostępna offline!! (w razie awarii internetu)

**HVAC** - Temperature, and Humidity Controls

**SEH** - Structured Exception Handler - you can ensure that resources such as memory blocks and files are correctly if execution unexpectedly terminates.

**LEAP** - The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server).

**IEEE 802.1X –** standard IEEE kontroli dostępu do sieci przewodowych i bezprzewodowych. Umożliwia uwierzytelnianie urządzeń dołączonych do portów sieci lokalnej, ustanowienie połączenia punkt-punkt i nie zezwala na dostęp z określonego portu, jeśli uwierzytelnienie się nie powiedzie.

**CCMP** - CCMP, is the encryption mechanism that has replaced TKIP. Enkrypcja, która zastąpiła TKIP

**Baseline reporting** - ocena bezpieczeństwa w sieci

**Wildcard** - A wildcard certificate is a public key certificate that can be used with multiple subdomains of a domain. Publiczny klucz, który może byc użyty przez wiele subdomen w domenie.

**SCP** - Secure copy lub SCP – bezpieczny transfer plików pomiędzy lokalnym a zdalnym lub między zdalnymi komputerami, używając protokołu Secure Shell (SSH). Skrót SCP odnosi się do dwóch powiązanych ze sobą rzeczy: protokółu SSH oraz polecenia cp.

Ciphers types - do opracowania

**X-500** - jest zbiorem sieciowych standardów pokrywających usługi katalogowe (np. dap, później LDAP)

**3DES** - trzykrotne przetworzenie szyfrowania DES'em

**Stream cipher** - Szyfr strumieniowy (także: algorytm strumieniowy, algorytm potokowy) – algorytm symetryczny, który szyfruje oddzielnie każdy bit wiadomości.

**SHA** - verify data integrity

**RFID** (ang. Radio-frequency identification) – technika, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu (etykieta RFID) stanowiącego etykietę obiektu przez czytnik, w celu identyfikacji obiektu.

**EMI shielding -** Electromagnetic shielding is the practice of reducing the electromagnetic field in a space by blocking the field with barriers made of conductive or magnetic materials. Shielding is typically applied to enclosures to isolate electrical devices from their surroundings, and to cables to isolate wires from the environment through which the cable runs.

**RADIUS**—Remote Authentication Dial-In User Service. Provides central authentication for remote access clients. RADIUS encrypts the password packets and uses UDP. In contrast, TACACS+ encrypts the entire authentication process and uses TCP. Autentykacja dla zdalnych uzytkowników (wdzwanianie się), stosowana równiez w sieciach bezprzewodowych (w wersji enterprise). Pakiety są enkyptowane i przesłane przez UDP (TACACS działa przez TCP).

**Protokół Diffiego-Hellmana** – protokół uzgadniania kluczy szyfrujących, opracowany przez Witfielda Diffiego oraz Martina Hellmana w 1976 roku. Jego siła oparta jest na trudności obliczenia logarytmów dyskretnych w ciałach skończonych

**Warchalking** - to oznaczanie miejsc, w których dostępne są sieci bezprzewodowe.

**OCSP** - Online Certificate Status Protocol - standard opisujący protokół komunikacyjny pomiędzy systemem informatycznym odbiorcy usług certyfikacyjnych a serwerem usługowym.

**ESP** - Encapsulating Security Protocol. IPsec includes both AH and ESP. AH provides authentication and integrity, and ESP provides confidentiality, integrity, and authentication. ESP is identified with protocol ID number 50.

protokół bezpieczeństwa zapewniający:

* uwierzytelnianie źródła danych
* integralność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych)
* niezaprzeczalność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych)
* obsługuje unikanie duplikacji pakietów jak również ataku przez powtórzenie (zastosowanie numerów sekwencji)
* zapewnia poufność danych.

**Galois Message Authentication Code (GMAC)** is an authentication-only variant of the GCM which can be used as an incremental message authentication code. Both GCM and GMAC can accept initialization vectors of arbitrary length.

**Transitive Access -** relationships refer to trusts, such as between two servers. They allow the two servers to share data.

**MTTF** - Mean Time To Failure

**MTTR** - Mean Time to Repair

**MTBF** - Mean Time Between Failures

**ALE** - Annualized Loss Expectancy - SLE x ARO

**SLE** - Single loss expectancy - single cost

**ARO** - Annual rate of occurrence - how many times the loss will acure in a year

**Virus hoax** is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know. Zaleca skasowanie pliku np. systemowego, który uniemożliwia funkcjonowanie systemu.

**BCP**—Business continuity plan. A plan that helps an organization predict and plan for potential outages of critical services or functions.

**BIA**—Business impact analysis. The BIA identifies critical business or mission requirements and includes elements such as Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), but it doesn’t identify solutions. BIA identyfikuje krytyczne wymogi biznesowe włączając w to RTO czy RPO, ale nie zawiera dla nich rozwiązań.

**HMAC**—Hash-based Message Authentication Code. An HMAC is a fixed length string of bits similar to other hashing algorithms such as MD5 and SHA-1, but it also uses a secret key to add some randomness to the result.

**IKE**—Internet Key Exchange. Used with IPsec to create a secure channel over port 500 in a VPN tunnel.

**IPV6** - 128 bitów (8x4)

**MD5** - używa 128 bitów

**Saas** - brak zarządzania

**platform as service (paas)** - zarządzac aplikacją i danymi

**iaas**- wszystko co powyżej, a do tego os, oraz middleware

**PEAP** - tls

**PKI**—Public Key Infrastructure. Group of technologies used to request, create, manage, store, distribute, and revoke digital certificates. Certificates are an important part of asymmetric encryption. Certificates include public keys along with details on the owner of the certificate and on the CA that issued the certificate. Certificate owners share their public key by sharing a copy of their certificate.

**PSK**—Pre-shared key. A secret shared among different systems. Wireless networks support Personal Mode, where each device uses the same PSK. In contrast, Enterprise Mode uses an 802.1x or RADIUS server for authentication.

**RAID**—Redundant Array of Inexpensive (or Independent) Disks. Multiple disks added together to increase performance or provide protection against faults.

* **RAID-0**—Disk striping. RAID-0 improves performance but does not provide fault tolerance.
* **RAID-1**—Disk mirroring. RAID-1 uses two disks and provides fault tolerance.
* **RAID-5**—Disk striping with parity. RAID-5 uses three or more disks and provides fault tolerance.

**RPO**—Recovery Point Objective. A Recovery Point Objective identifies a point in time where data loss is acceptable. It is related to the RTO and the BIA often includes both RTOs and RPOs. RPO to punkt w czasie, w którym strata danych jest akceptowalna.

**RTO**—Recovery Time Objective. An RTO identifies the maximum amount of time it can take to restore a system after an outage. It is related to the RPO and the BIA often includes both RTOs and RPOs. RTO to maksymalny czas, który zajmuje przywrócenie systemu po awarii.

**SPOF**—Single point of failure. An SPOF is any component whose failure results in the failure of an entire system. Elements such as RAID, failover clustering, UPS, and generators remove many single points of failure.

**SSO**—Single sign-on. Authentication method where users can access multiple resources on a network using a single account. SSO can provide central authentication against a federated database for different operating systems.

**SCP**—Secure copy. Based on SSH, SCP allows users to copy encrypted files over a network. SCP uses port 22.

**SHA**—Secure Hash Algorithm. A hashing function used to provide integrity. SHA1 uses 160 bits, and SHA-256 uses 256 bits. Hashing algorithms always provide a fixed-size bit-string regardless of the size of the hashed data. By comparing the hashes at two different times, you can verify integrity of the data.

**TACACS**—Terminal Access Controller Access-Control System. An older remote authentication protocol that was commonly used in UNIX networks. TACACS+ is more commonly used.

**TACACS+**—Terminal Access Controller Access-Control System+. Provides central authentication for remote access clients and used as an alternative to RADIUS. TACACS+ uses TCP port 49, compared with TACACS, which uses UDP port 49. It encrypts the entire authentication process, compared with RADIUS, which only encrypts the password. It uses multiple challenges and responses.

**WAP**—Wireless access point, sometimes just called an access point (AP). Increasing the power level of a WAP increases the wireless coverage of the WAP. Decreasing the power levels, decreases the coverage. Coverage can also be manipulated by moving or positioning the wireless antenna.

**WPA2**—Wi-Fi Protected Access version 2. Newer security protocol used to protect wireless transmissions. It supports CCMP for encryption, which is based on AES and stronger than TKIP which was originally released with WPA. In Enterprise Mode, it can use RADIUS to support 802.1x authentication. In personal mode, it uses a preshared key (PSK).

**WTLS**—Wireless Transport Layer Security. Used to encrypt traffic for smaller wireless devices.

**WEP**—Wired Equivalent Privacy. Original wireless security protocol. Had significant security flaws and was replaced with WPA, and ultimately WPA2. WEP used RC4 incorrectly making it susceptible to IV attacks.

**XTACACS**—Extended Terminal Access Controller Access-Control System. An improvement over TACACS developed by Cisco Systems and proprietary to Cisco systems. TACACS+ is more commonly used.

**Validations** can be performed:

* on the server side, (walidacja przy pomocy php, asp).
* on the client side (**web browser – java, html, vbs**).

**Subject Alternative Name (SAN)** is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called Subject Alternative Names (SANs). Names include:

* Email addresses
* IP addresses
* URIs
* DNS names (this is usually also provided as the Common Name RDN within the Subject field of the main certificate.)
* directory names (alternative Distinguished Names to that given in the Subject)
* other names, given as a General Name: a registered object identifier followed by a value

**SRTP** is a Real-time Transport Protocol (RTP) profile, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both **unicast and multicast applications**. Like RTP, it is intended particularly for **VoIP** (Voice over IP) communications.

**Incident response** procedures involve: **Preparation**; **Incident identification**; **Escalation and notification; Mitigation steps; Lessons learned;** **Reporting**; **Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control.**

**Information classification** is done by confidentiality and comprises of three categories, namely:

* public use,
* internal use
* restricted use. T

hese categories make applying the appropriate policies and security controls practical.