1. Vysvětlete korelaci událostí, co je detekce anomálií, referenční model
2. Hlavní součásti protokolu IPsec, základní účely, co obsahuje SA a SAD
3. Popiště síťové útoky - rozdělení, principy, techniky MiTM, SSL strip
4. Pen testování WEB aplikací- OWASP, co obsahuje průzkum prostředí, mapování aplikace, testování vstupů, závěrečný report
5. Pojmy - aktiva, hrozba, ochrana, bezpečnost, zranitelnost, riziko, incident, dopad
6. Rozdělení DDoS útoků - principy skupin, aspoň jeden příklad
7. WPA autentizace PSK

---

1. Korelace událostí a její druhy
2. Referenční model(popsat + cyklus)
3. WPA - 4-way hand shake, diskuze na zabezpečení bedzrátové sítě
4. pojmy
5. Penetrační testování
6. TLS
7. Druhy síťových útoků(MitM, SSL strip)

---

1. jak funguje 4WH u WPA PSK, problém s bezpečností u bezdrátu, rozdíly s WPA2 2)Popsat referenční model, co to je, jak to funguje, životní cyklus
2. pojmy
3. IPsec
4. Penetrační testování: napsat všechny ty rozdělení a jaké má kroky (nebylo psáno že web appky takže obyč)
5. Logování
6. Firewally, DMZ, druhy, zapojení s DMZ, FW load balancing, nastavení

Pojmy

- Aktiva: cokoliv, co je majitelem považováno za cenné
- Hrozba: možnost ztráty aktiv, popsána:
    - nositelem hrozby (konkurenční firma)
    - objektem hrozby (zákaznická db)
    - mechanismem hrozby (krádež db, kopírování dat)
- Ochrana: opatření snižující četnost nebo velikost ztrát aktiv různý charakter (administrativní, organizační, personální, technické opatření)
- Bezpečnost: stav, kdy ztráta aktiv nepřekračuje stanovenou míru nemůže být absolutní (nelze ochránit před všemi hrozbami)
- Zabezpečení: ucelený systém ochran - komplexní, systematická a efektivní
- Slabina: zranitelné místo
- Riziko: pravděpodobnost využití zranitelného místa
- Incident: jakákoliv realizace hrozby
- Průnik: dopad pokud při incidentu došlo ke ztrátě aktiv, rozsah škod, důsledek útoku
- Počítačová síť: technické prostředky realizující spojení, výměnu informací mezi PC a umožňují uživatelům komunikaci

- Bezpečnost sítě: neustálý proces (není to stav), kterým má být dosaženo uspokojivého zabezpečení sítě a toto zabezpečení udrženo
- k zajištění užíváme bezpečnostní služby (CIA):
    - autentizace - ověření identity
    - řízení přístupu - autorizace
    - důvěrnost přenášených dat
    - integrita
    - nepopiratelnost - ochrana proti odmítnutí původu

Korelace událostí a její druhy

Korelace je spojení podobných i zcela odlišných událostí ve znalost o větší probíhající události.

Na zaklade pravidel - detekce signatur

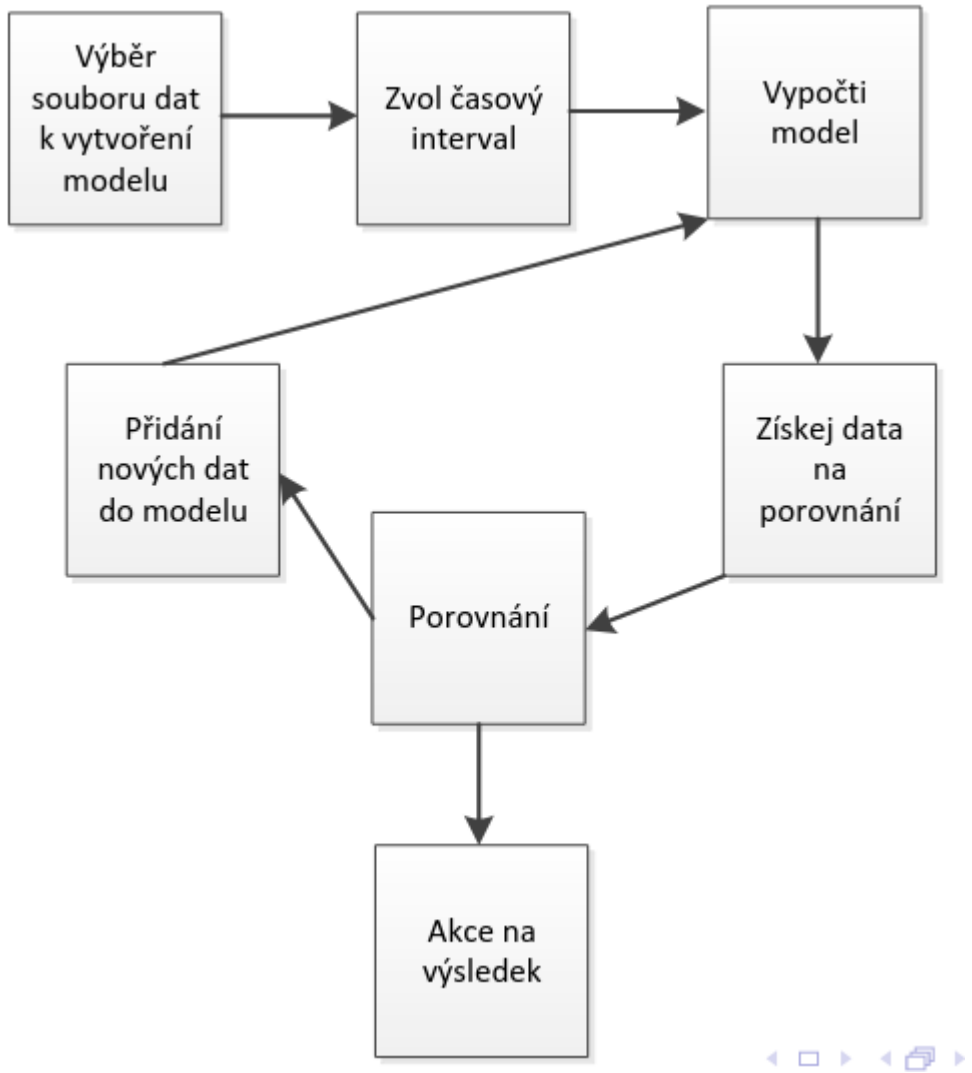
Tato korelace muze byt realizovana vytvorenım pravidla (vzoru utoku) v nejakem programovacım jazyce

Na zaklade modelu - detekce anomalii

Frekvenční model počítá výskyty definovaného jevu za pevně daný okamžik.

Referenční model porovnáva model „normálního“ chování a sleduje, zda se sledované jevy pohybují v povolených odchylkách - data jsou sbírána a porovnávána s modelem. Přesnost je velmi závislá na množství

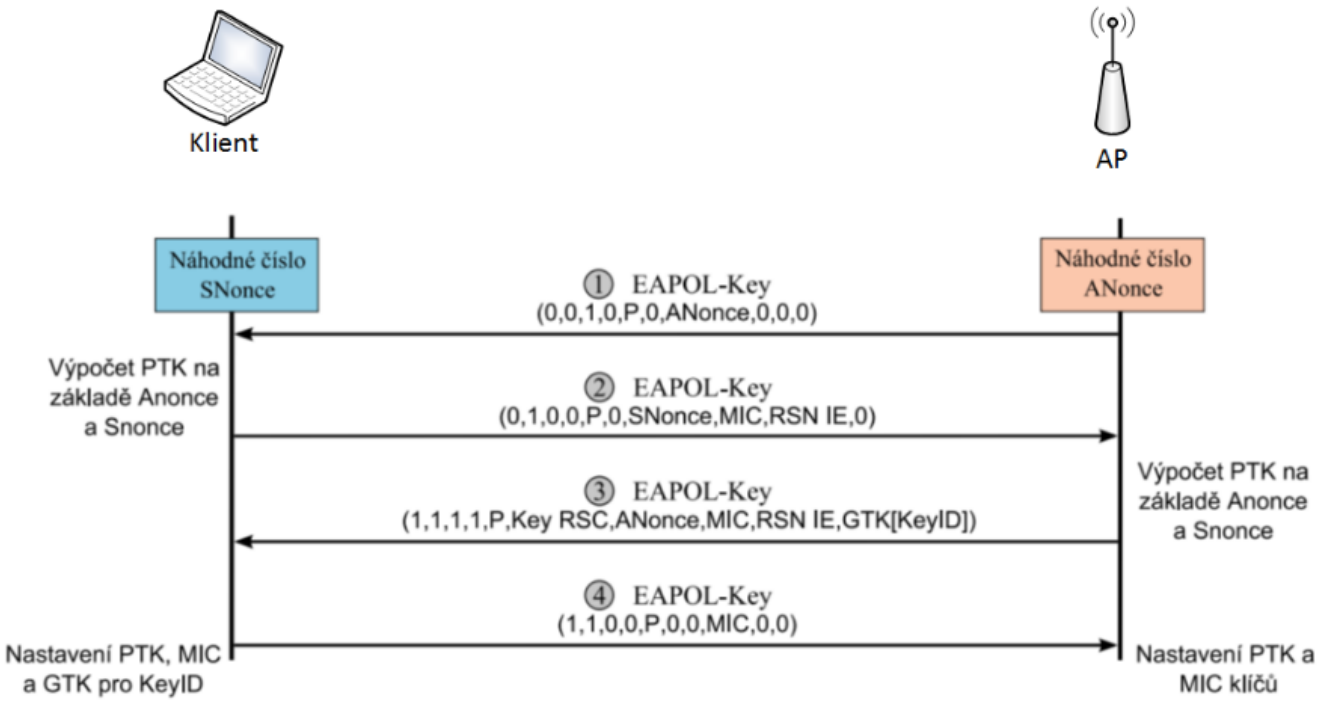
a kvalitě dat ze kterých byl model vytvořen. Nastavenie je vytvorene expertom.



Model strojového učení klasifikuje vstupní data do tříd a shlukuje je do skupin s posobnými vlastnostmi. Anomáliemi mohou být nadměrný provoz, změna chování síťového prvku, přihlášení pomocí VPN mimo pracovní hodiny, opakovaná neúspěšná přihlášení, přihlášení z více IP během krátké doby. . .

WPA, 4WH

4WH



1. AP vygeneruje náhodné číslo ANonce, otevřeně odesláno uživateli
2. uživatel generuje náhodné SNonce, vypočítá PSK-PTK, odvodí dočasné klíče, s využitím KCK posílá AP zprávu obsahující SNonce a MIC otevřeně, AP přijme zprávu, pomocí SNonce vypočítá PTK s dočasnými klíči, vypočte MIC a ověří shodu (autentizace uživatele, passphrase)
3. AP zašle klientovi zprávu s GTK, zašifrované pomocí KEK, uživatel ověří MIC (autentizace AP)
4. závěrečná zpráva od uživatele k AP potvrzuje dokončení 4WH

WPA2

1. PTK kratšie ako pri WPA
2. RC4 nahradené AES
3. autentizace pomocí IEEE 802.1x nebo PSK (Pre-Shared Key)
4. důvěrnost pomocí TKIP (Temporal Key Integrity Protocol)
5. integrita - MIC nahradený CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
6. kompatibilita se stávajícími zařízeními - upgrade firmware
7. pracovní režimy: firemní vs osobní řesení

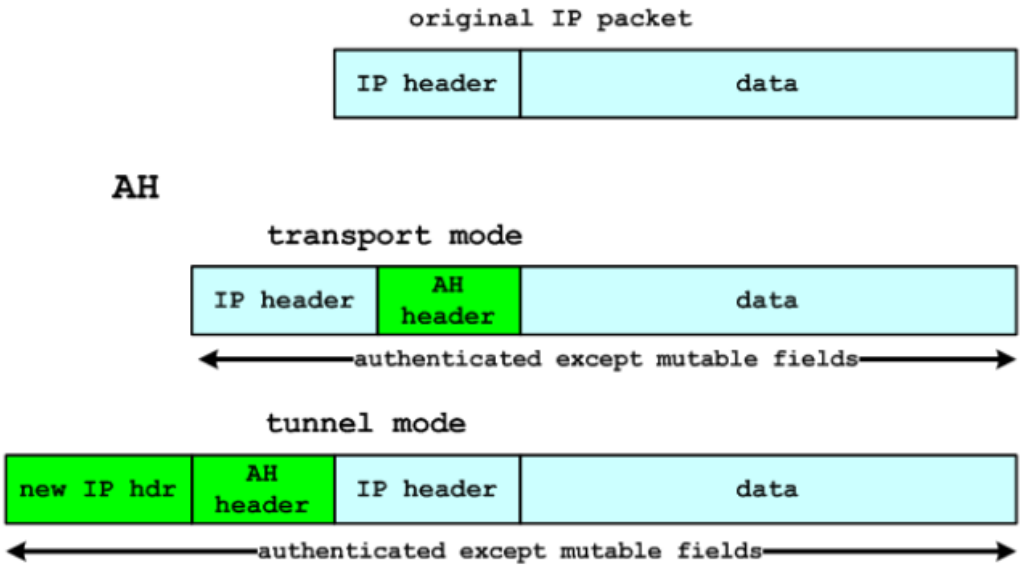
Režim	Wi-Fi Protected Access 2 – WPA2	
	Autentizace	**Šifrování**
Enterprise Mode (firemní mód)	802.1x / EAP	CCMP – AES
Personal Mode (osobní mód)	PSK	CCMP – AES

IPsec

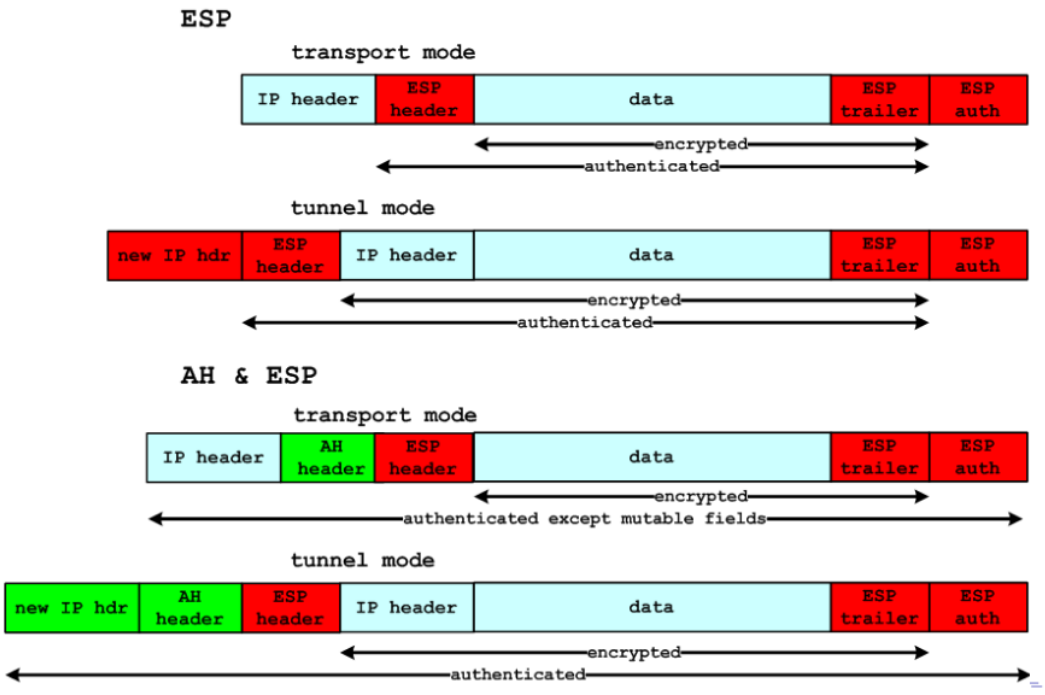
- end-to-end bezpečnost
- šifrování a autentizace na úrovni síťové vrstvy = zabezpečení síťové vrstvy

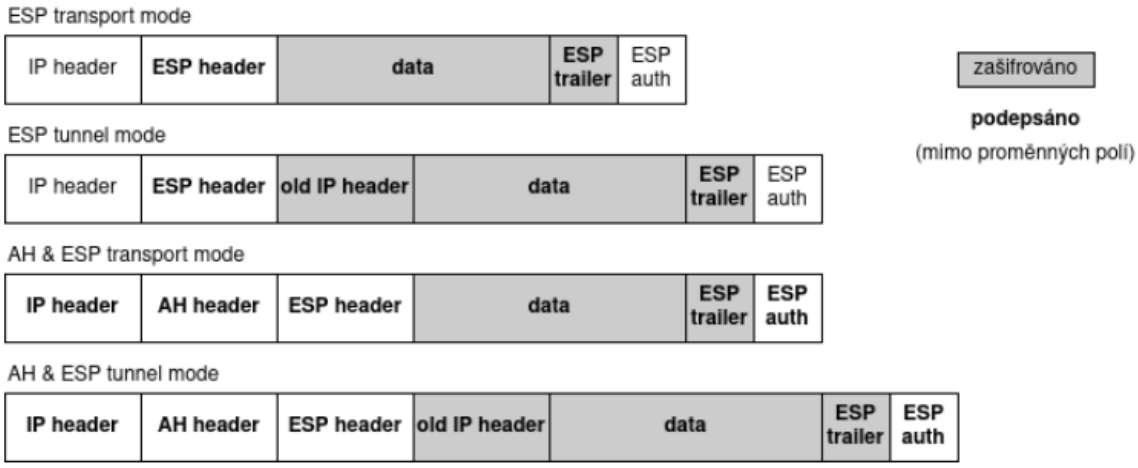
Součásti

- authentication header protocol (AH)
  - integrita a autentičnost IP paketů (MAC funkce)
  - sekvenční číslo, ochrana proti replay attacks



- encapsulating security payloads protocol (ESP)
  - důvěrnost dat pomocí šifrování
  - autentizace pouze ESP částí a dat, ne IP hlavičky





- security association (SA)
  - formálně popisuje spojení mezi dvěma stranami a parametry použité pro zabezpečení
  - aktivní spojení v db SAD (security association db)
  - SA management a pravidla jsou uložena v SPD (security policy db)
  - SA parametry v SAD - sekvenční čísla, AH informace, ESP informace, životnost SA, IPsec protokol mód, max velikost paketu, security parameter index (SPI, 32b)

Módy

- transportní mód: ochrana payloadu paketu, IP není šifrovaná, mezi hosty
- tunelující mód: ochrana celého paketu (IP hlavička a data), paket se stane payloadem v novém paketu s novou hlavičkou, mezi hosty, bránami (překlad IP)

Ustanovení klíče (symetrické klíče)

- PSK
- IKE1 a IKE2
  - Internet Key Exchange (sada autentizačních schémat včetně certifikátů)
  - implementace pomocí knihoven Strongswan, Libreswan, Openswan
- Kerberos

TLS

- chová se jako bezpečné TCP, lze zabezpečit protokoly nad TCP
- zabezpečení transportní vrstvy

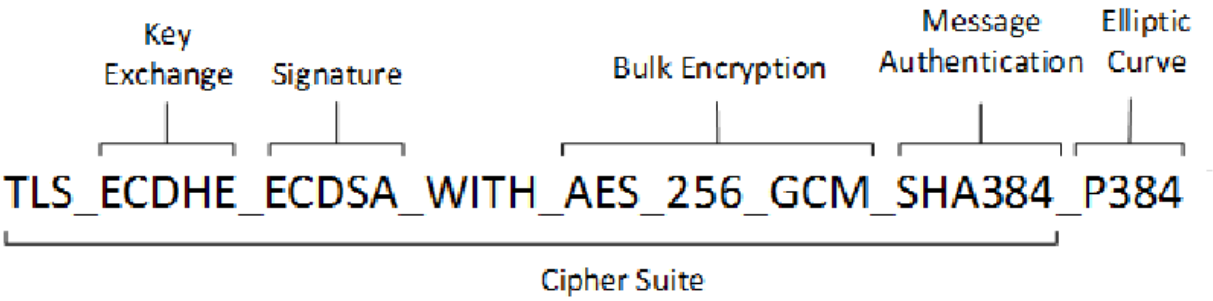
Součásti

- handshake protocol (inicializace, autentizace stran, ustanovení klíče)
- record protocol (datový přenos šifrovaných data MAC autentizace)
- alert protocol (notifikace chyb a varování)

CipherSuite

- ustanovení klíče s dočasnými klíči (ECDHE, DHE)
- bezpečný podpis (RSA, DSS, ECDSA)

- bezpečné šifrování a mód (AES-GCM)
- bezpečná hashovací funkce (SHA-256, 384)



DDoS

záplavové/volumetrické (flooding attacks)

- vytížení komunikační, paměťové, výpočetní kapacity
- TCP flood, UDP flood, HTTP flood, ICMP flood
- ARP flood:
  - falešné dotazy ARP
- reset flood:
  - pakety s falešnou src IP, příznak RST - resetuje spojení
  - skutečná komunikace je neoprávněně ukončena
- syn flood:
  - otevření několika polootevřených spojení a čekání na potvrzující zprávu, která od útočníka nepřijde
- HTTP flood:
  - ze zombie klientů, zaslání legitimních požadavků http GET nebo POST
  - jsou náročnější
- UDP flood:
  - velký počet IP paketů s UDP datagramy
- PingSweep:
  - ICMP echo s podvrženou src IP
- Smurf:
  - ICMP se spoofovanou adresou oběti zaslány na broadcast

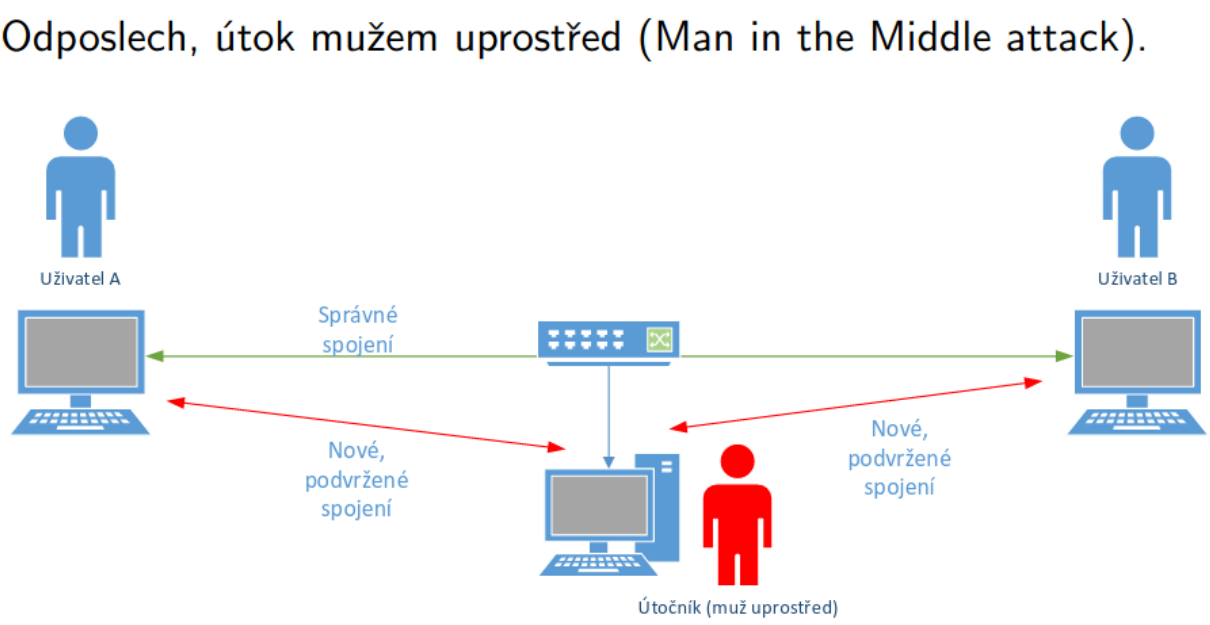
logické útoky (logical attacks)

- útok na slabinu v programu/protokolu/OS
- protokolové
- aplikační
- ping of death, land attack, Slowloris, R-U-Dead-Yet (RUDY), Apache Range Header attack
- Teardrop:
  - fragmenty paketů přesahující falešně nastavený offset jsou zasílány cíli
  - cíl nezvládne sestavit paket nazpět a spadne
- Land:
  - TCP-SYN jsou podvrženy, stejná src i dest IP, nekonečná smyčka

- Ping of death:
  - Ping o velikosti vyšší než 65 535 B
- Regular expression Dos (ReDoS):
  - Zatížení procesu zpracování výrazů (dlouhé divné username a heslo)
- RandomUnreachableHost:
  - poslání ICMP host unreachable na náhodné IP adresy, přerušení některých spojení v síti
- UnreachableHost:
  - ukončení legitimních spojení pomocí ICMP host unreachable
- Slowloris:
  - generuje a opakovaně posílá částečné http požadavky, ale neukončí je
  - cíl otevírá další a další spojení
- XMasTree:
  - generování paketů, kde jsou příznaky FIN, URG, PSH v TCP hlavičce a jsou náročné na zpracováni

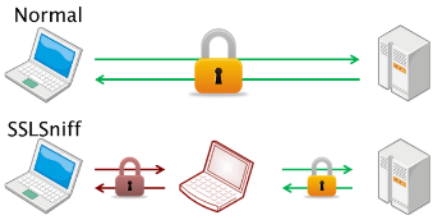
Útoky v sieti

- na přenos (odposlech dat, MITM, replay, ARP spoof, routing útoky, SSL strip)



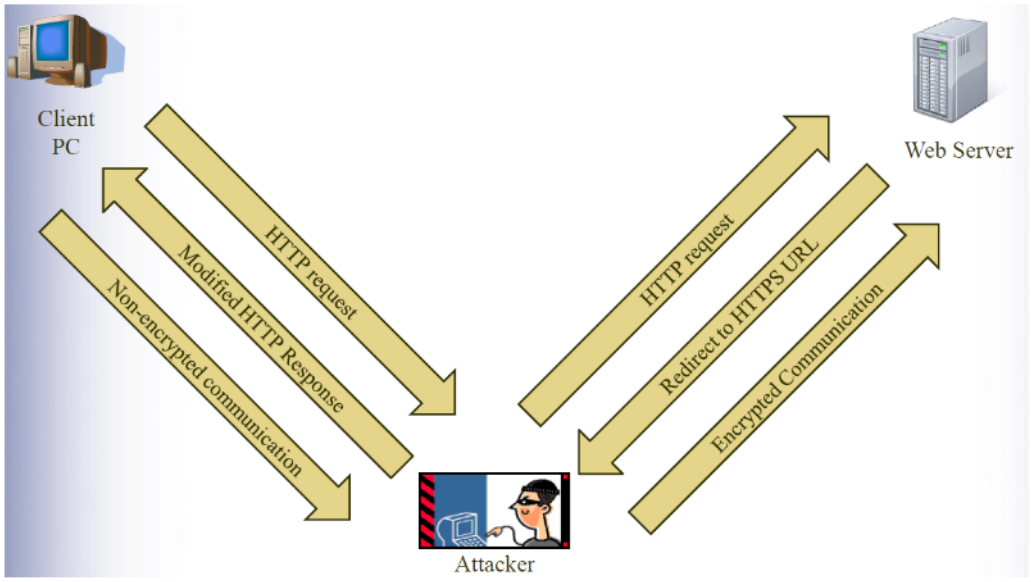
Síťové útoky - MitM pomocí podvrhnutí certifikátu - SSL Snif

Přeposlání zašifrované zprávy přes útočníka, dvojí SSL pomocí falešného certifikátu (podobný název certifikátu jako pravý).



Síťové útoky - SSL Strip

Změna hlavičky z https na http (druh MitM).



- na koncové prvky (pomocí malware)
- na síť (nepovolené průniky do sítě)
- odepření služeb (DoS, DDoS)
- zneužití fyz. osob (social engineering, phishing)

Obrana

- bezpečná konfigurace
- aktivní prvky
- sestavení a dodržování pravidel
- zabezpečení koncových prvků
- nasazení správné kryptografie, obran a protokolů
- testování obecných zranitelností
- celkový audit
- školení uživatelů a dohled

Pentest (obecne)

- penetrační test: posouzení úrovně bezpečnosti metodou pokusu o průnik technická forma, zkušenosti, inteligence, při nalezení zranitelnosti je napravena nutnost povolení majitele systému
- zranitelnost: slabé místo systému
- exploit: využití zranitelnosti, exploit nese payload
- payload: náklad, umožní kontrolu nad systémem (Metasploit - Meterpreter)
- vulnerability assessment: není penetrační test samotný, pouze odhaluje zranitelnosti, čistě mechanická a strojová záležitost nesoucí false-positives neobnáší demonstraci nalezených slabin
- bezpečnostní audit: zhodnocení stavu vůči normě

Attack vector

- externí testy: vnější hrozby, útok crackera z internetu
- interní testy: z vnitřní strany, potenciální útočník, co získal přístup do vnitřní sítě či neloajální zaměstnanec

Znalosť systému

- black-box testy:
  - jsou známy pouze vstupy a výstupy systému, není známa vnitřní struktura
- white-box testy:
  - jsou k dispozici všechny možné informace o systému
  - topologie, zařízení, údaje, zdrojové kódy atd.
- grey-box testy:
  - medzistav medzi black, white

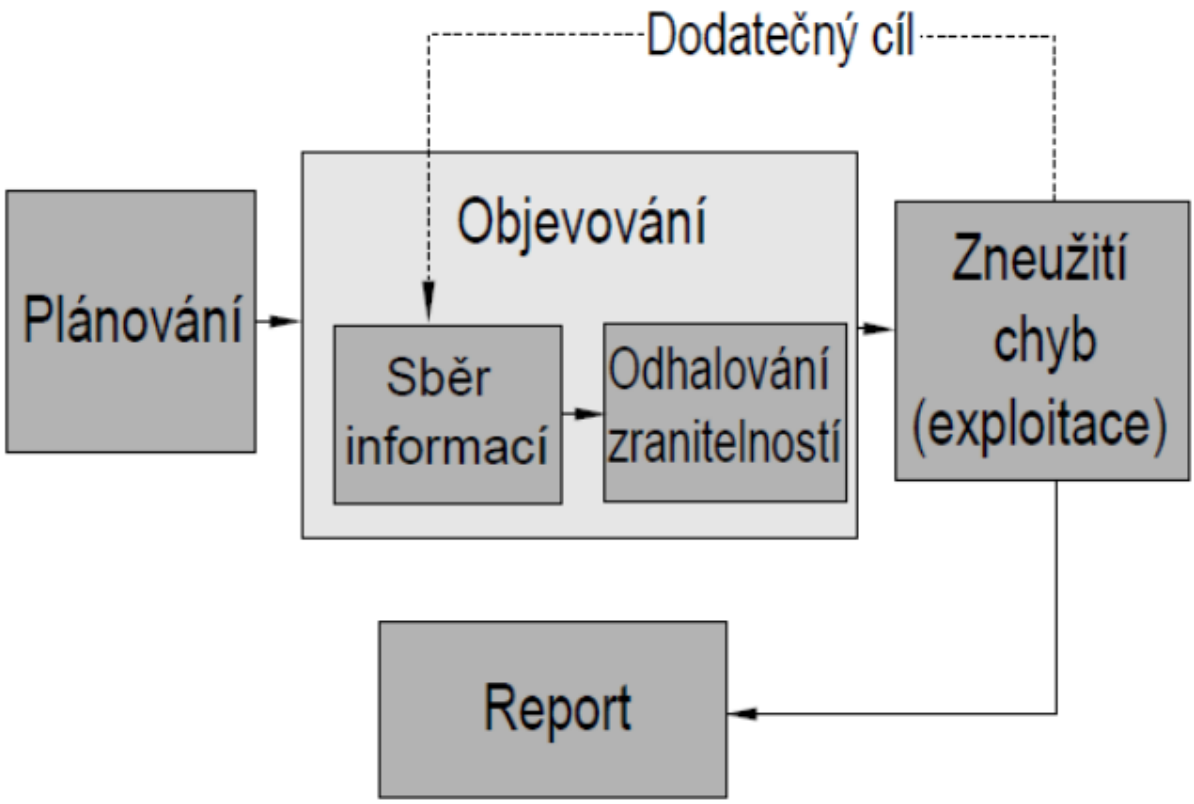
Automatizácia

- manuální (testy na míru pro specifické podmínky, nutné mít rozsáhlé znalosti)
- automatizované (nelze jimi otestovat úplně všechno)
- semiautomatizované (kombinují výhody obou způsobů)

Metódy testu

- plánování: počáteční fáze, časový plán a sestavení týmu, stanovení detailních cílů
- sběr informací: co nejvíce info o cílové síti/systému, rozsahy IP, otevřené porty, služby
  - nmap, zenmap
  - odhalování zranitelností: síťové služby, porovnání verzí s db zranitelností, chybné konfigurace, specializované nástroje
  - Nessus
  - Security Focus
  - ExploitDB
  - OpenVas
- zneužití chyb (exploitace): využití nalezených zranitelností, už existuje řada exploitů možnost otevření nové služby či cesty, postup začne od začátku
  - Metasploit Framework
  - výběr a konfig exploitu

    - kontrola zranitelnosti cíle
    - kontrola a konfig payloadu
    - volba šifrovací techniky (obcházení IPS)
    - execution
    - Armitage
    - Rapid7
- report: předání výsledků penetračních testů nalezené zranitelnosti včetně řešení výsledky min. do 6 měsíců (jinak ztratí vypovídací hodnotu) zaslat šifrovaně, psát neutrálne



Metodiky, štandardy, guides

- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTMM)
- Application Security Verification Standard (ASVS)
- OWASP Web Security Testing Guide (WSTG)
- OWASP Mobile Application Security Verification Standard (MASVS)
- OWASP Mobile Security Testing Guide (MSTG)

Firewally

- DMZ (demilitarizovaná zóna)
    - část sítě na perimetru mezi vnější a vnitřní sítí
    - bezpečnější umístění serverů a služeb poskytovaných do Internetu
    - pro FW rozhraní se stupněm důvěrnosti mezi vnitřní a vnější sítí
- honeypot

    - falešná návnada
    - systém nebo SW na serveru vypadá zranitelně a má přitahovat útoky
    - součástí IDS často

Packetový fw

- paketové filtry (IP a porty): 3. a 4. vrstva ISO/OSI
- zkoumají IP adresu, hlavičku, porty
- využití acl
- rychlost, jednoduchost, nízká cena
- nižší úroveň zabezpečení, nechrání proti spoofu, ...

Stavový packetový fw

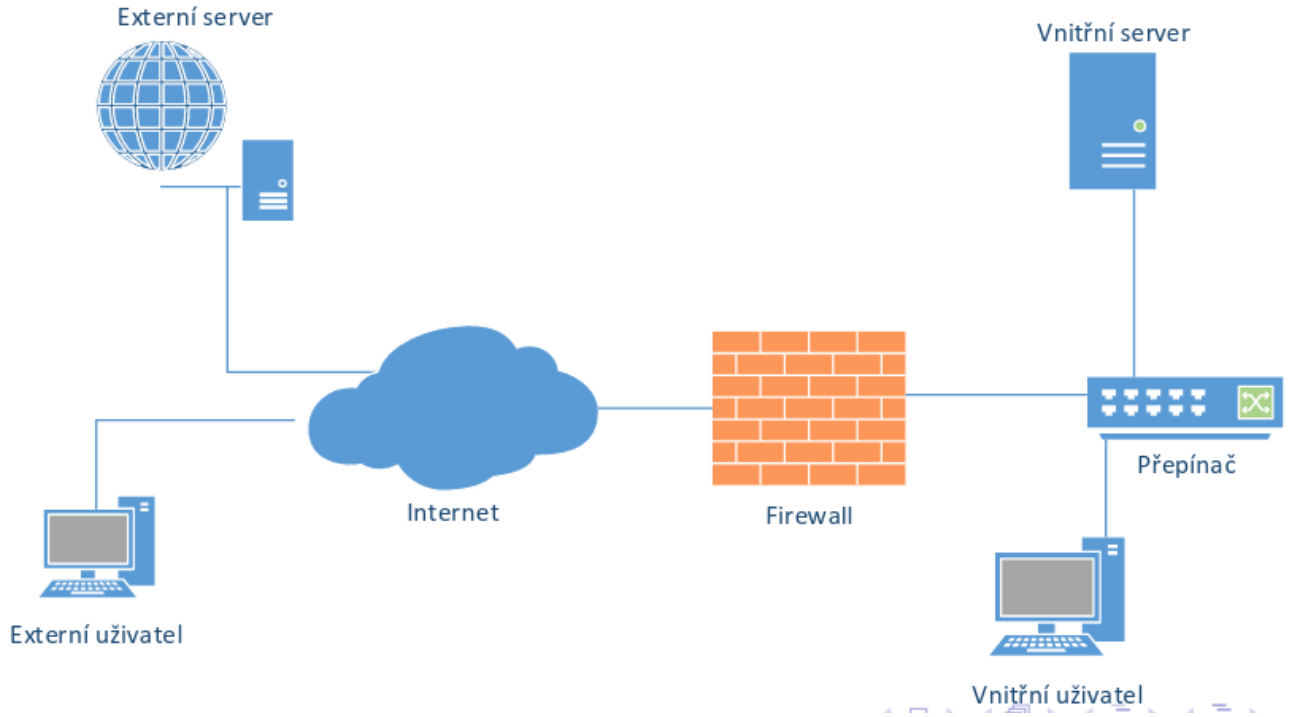
- stavové paketové filtry, stavová inspekce (stateful packet inspection): 3. a 4. vrstva
- jako paketový fw, ale rozhoduje se ještě podle stavu (nové spojení, existující)
- ukládá info o stavu jednotlivých spojení do paměti, např. povolit jen odpovědi, atd.
- ukládá info o socketech (src IP, dest IP, src port, dest port, TCP/UDP)
- rychlost, jednoduchost, vyšší bezpečnost než paketový fw
- nižší zabezpečení než aplikační filtry, nechrání proti některým útokům a je náchylný na DDoS

Application fw

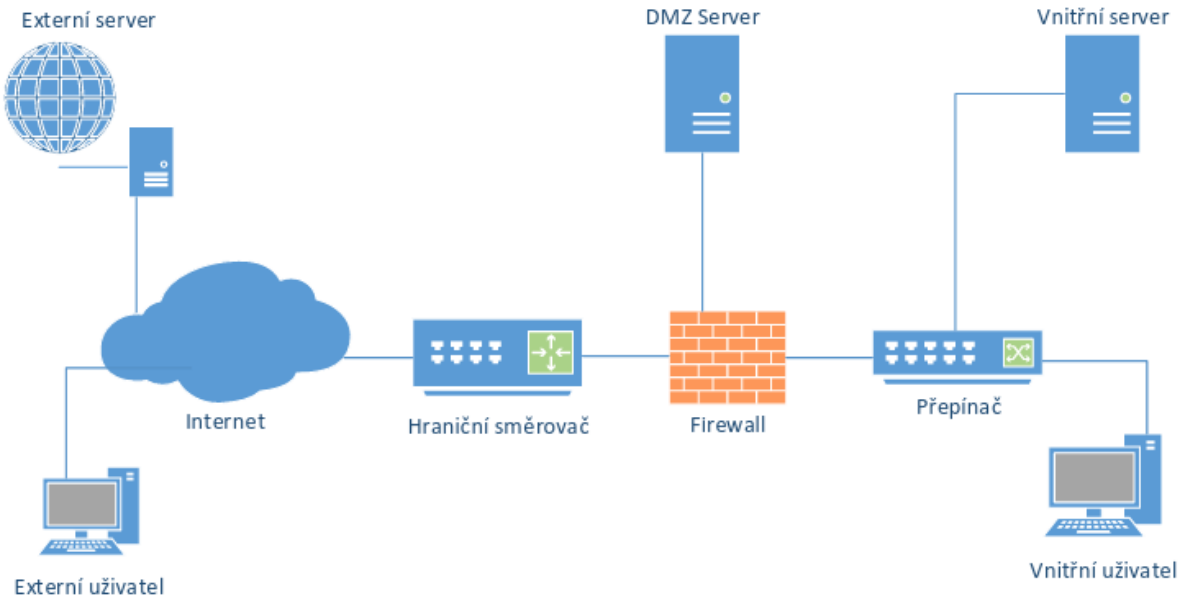
- aplikační brány/proxy firewally: 3., 4. a 7. vrstva
- aplikační firewall
    - Next Generation FW (NGFW) s deep packet inspection
    - vyšší bezpečnost, prevence proti červům, trojanům, mitigace DDoS
    - vyšší zpoždění, výpočetní náročnost, periodický update a revize, složitost může způsobit vznik chyby či zranitelnosti
- virtuální firewall
    - provoz mezi virtuálními stroji
- osobní firewall
    - v OS na 2. až 7. vrstvě
    - součástí OS + IPS/IDS
- proxy server
    - prostředník v komunikaci, sám vystupuje jako klient

Umiestnenie

- Mezi vnitřní (intranet) a vnější sítí (Internet), často jako součást směrovače nebo jako samostatné zařízení.



- Ve vnitřní síti u hraničního směrovače.
- Mezi vnitřní sítí, vnější sítí a **demilitarizovanou zónou** (DMZ), FW s min. 3 rozhraními.



Pentestování WEB aplikací - OWASP, co obsahuje průzkum prostředí, mapování aplikace, testování vstupů, závěrečný report OWASP

- projekt zaměřen na bezpečnost webových aplikací – všechny nástroje dokumenty
- jsou volně dostupné, důležitá je standardizace bezpečnostního testování web a mobil aplikací
- Známý dokument OWASP top ten – vychází každé 3 roky, popisuje největší webové
- zranitelnosti – 2021 – Broken access control - cryptography failures -injection – insecure design – sec. Misconfig ...

Metódika

- Průzkum prostředí: identifikace OS, web serveru, použitého prog. Jazyka, autora aplikace, ostatních technologií
- Mapování: nalezení subdomén, vhostů, součástí aplikace
- Testování vstupů: v rámci celé aplikace, testování formulářů, session management
- Report: Shrnutí a předání výsledků pen testu, cílem je prezentovat zprávu, která vede ke zlepšení zabezpečení – nalezené exploity s řešením

Logování

- Záznamy reprezentující popis konkrétních událostí ve sledovaném systému:
  - Informační
  - ladící
  - varovné
  - chybové
  - pohotovostní kategorie
- Otázky: kdo bude logy vytvářet, kde se budou vytvářet, jaké události se budou logovat, co budou logy obsahovat

Manuální analýza

- vhodná pro small scale operace

Automatická analýza

- Agregace: stahování logů na jedno místo – logovací server – nutno zajistit bezpečný přenos
- Filtrace: analýza dat, rozhodnutí která jsou důležitá
- Normalizace: úprava na společný formát
- Korelace : spojení podobných nebo naprosto rozdílných události ve znalost o větší probíhající událost, kritický blok problematiky logování