BPC-IC2

Bezpečnost ICT 2

Otázky ke státnicím

Bakalářský obor Informační bezpečnost, FEKT VUT

https://github.com/VUT-FEKT-IBE/BPC-IBE-SZZ

Text: kámen u cesty
Korektura: czechbol

28. května 2023

Obsah

1 Definujte a vysvětlete základní pojmy (aktiva, hrozba, ochrana, bezpečnost, zranitelnost, riziko, incident a dopad).

aktiva	cokoliv cenného: data, služby, hardware, software, ...
hrozba	možnost ztráty aktiv
ochrana	opatření ke snížení rizika, četnosti nebo velikosti ztrát
bezpečnost	stav, kdy riziko ztráty aktiv nepřesahuje určitou míru
zranitelnost	místo bez dostatečné ochrany
riziko	**pravděpodobnost** využití zranitelného místa
incident	realizace hrozby
dopad	důsledek útoku, rozsah škod

2 Bezpečná konfigurace přepínače a směrovače (základní postupy konfigurace, bezpečnostní funkce, útoky, Port Security, port Fast, hardening).

L1: rozbočovač (hub) a opakovač (repeater), L2: most (bridge) a přepínač (switch), L3: směrovač (router), přepínač (switch) a brána (gateway), L4-L7: sondy, brány, firewally, ...

2.1 Konfigurace

Jako v případě veškerého síťového hardware je třeba **fyzicky zabezpečit přístup** k přepínači (klíče, kódy, biometrie), připojit UPS, nepoužívané fyzické porty umístit do „mrtvé“ VLAN (aby nebylo možné jen tak připojit nové zařízení). Je nutné zkontrolovat **požadavky na síťový přístup** (HTTPS, dostatečné SSH klíče, logování přístupů a manipulace, ACL), **vypnout služby a porty** které nejsou využívány, **zapnout bezpečnostní funkce** (DHCP Snooping, MAC filtering/Port Security, AAA, IPS, VPN). Také je třeba **zálohovat** konfigurace, nastavení testovat a ověřovat, **aktualizovat** software i firmware.

Manuálně / přes management protokoly (SNMP), One Step Lockdown, Autosecure, Port security...

2.2 Zabezpečení přepínače

Port Security je omezení počtu MAC adres na port/ochrana před MAC útoky. **PortFast** nastavení porty na forwarding state ihned po zapojení (připojení stanic a serverů), je to součást STP protokolu. **BPDU Guard** chrání síť před zasíláním BPDU zpráv (Spanning Tree) na porty, které by takové zprávy v normálním provozu z těchto portů nedostaly. **Root Guard** zabraňuje nahrazení Root Bridge *spoofovanou* zprávou od útočníka, nastaví všechny root porty pro STP.

Mezi útoky patří **MAC address spoofing** (příjem cizích dat pomocí nelegitimní změny směrovacích tabulek), **ARP Poisoning** (úprava ARP cache vede k MitM), **Rough DHCP Server Spoofing** (falešný DHCP server odpovídá rychleji → MitM, DoS), **DHCP Starvation** (DHCP je zaplaven velkým množstvím dotazů s cílem vyčerpání paměti IP adres), **STP Manipulation** (útočník jako Root Bridge pro příjem provozu v síti), **MAC address table overflow** (vyčerpá se MAC tabulka adres na přepínači, který se přepne na HUB a data posílá všemi porty), **LAN storm** (přepínače přeposílají broadcast všemi porty, čímž se přetíží CPU a dojde k DoS).

2.3 Zabezpečení směrovače

Bezpečná konfigurace je popsána výše v podkapitole 2.1.

Mezi typické útoky na směrovače patří pokusy o **průnik do nastavení** (zneužití výchozích hesel), **Routing Table Poisoning** (*spoofování* routovacích protokolů a vyvolání nežádoucích změn ve směrovacích tabulkách), **Hit and Run** (posílání škodlivých paketů v náhodných intervalech), **(D)DoS** (vytížení CPU/RAM velkým množstvím paketů, logické útoky typu Christmas tree packet attack).

Hardening znamená zvyšování odolnosti proti útokům. Jedná se o vypínání nepotřebných protokolů, omezování oprávnění na minimální nutná, zapínání ochranných funkcí a šifrování komunikace při správě zařízení.

3 Problematika logování, hlavní cíle a rozdělení (definice logu, základní kategorie, formát, obsah logu, struktura záznamu, ochrana logů).

Log, záznamová data, logovací zpráva je soubor nebo sada souborů obsahujících záznamy reprezentující popis konkrétní události, která nastala ve sledovaném systému.

3.1 Úrovně

– **ladící** (`DEBUG`): využívané při vývoji a hledání problémů,
– **informační** (`INFO`): popisují stavy a události,
– **varovné** (`WARNING`): chybějící funkce nebo součást systému,
– **chybové** (`ERROR`): chyby ohrožující funkčnost systému,
– **pohotovostní** (`CRITICAL`): událost spojená s bezpečností nebo stav, ve kterém sytém již dále nedokáže pracovat.

3.2 Formát

Textový formát má výhodu ve skutečnosti, že ho lze otevřít v jakémkoliv textovém editoru. Jeho vytváření je nenáročné na systémové prostředky, existuje společná syntaxe pro mnoho aplikací.
Binární formát lze číst pouze k tomu určeným programem. Binární logy bývají menší než textové (data lze ukládat efektivnější), lépe se ukládají do databáze a mají lepší optimalizaci využíti prostředků. Binární logování využívá například OS Windows nebo Systemd.

3.3 Obsah

Každý záznam musí mít časové razítko, aby bylo v případě problémů lehké zjistit posloupnost událostí. Také by měl obsahovat zdroj, který záleží na typu logu: aplikační log by měl ukládat soubor či funkci, systémový program a uživatele, síťový konkrétní stroj a jeho adresu. Nesmí dojít k ukládání hesel nebo klíčů.

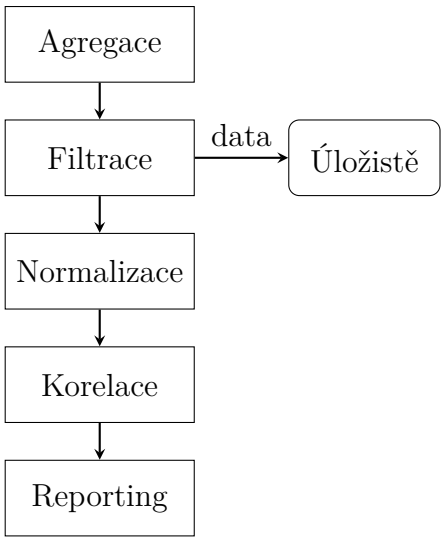
Každému záznamu je také přiřazena úroveň pro účely filtrace a oddělení informačních údajů od těch, kterým je potřeba věnovat zvýšenou pozornost. A také musí být obsažena informace samotná, včetně informace o chybě (*traceback*), je-li k dispozici.

3.4 Ochrana a manipulace

Administrátor systému by měl mít přehled o souborech, do kterých logy zapisují klíčové programy a démony (přihlašování, změna nastavení systému). Tyto logy by měly být zálohovány a chráněny – v případě existence centrálního logovacího serveru je potřeba zajistit jejich bezpečnost i při přenosu po síti.

4 Definice operací nutných k aplikaci automatické analýzy logů (blokové schéma včetně popisu funkce jednotlivých bloků). Jakým způsobem je realizován blok korelace při detekci známých a neznámých událostí.

Při **agregaci** začíná proces stahování záznamů na jedno centrální místo. **Filtrace** je analýza surových dat a rozhodování, která data jsou potřebná. **Normalizace** je úprava záznamů na společný formát (který využívá databáze a analytické systémy). **Korelace** je spojení podobných i zcela odlišných událostí ve znalost o větší probíhající události. Představuje nejproblematičtější blok. Výsledná data jsou posílána e-mailem, zobrazena graficky odlišeným způsobem nebo jsou nějakou formou předložena lidskému operátorovi, který vykoná další akce.



V případě incidentu, nebo i při pravidelné kontrole, lze využívat filtraci i další programy, které hlídají zaznamenané události. Při ruční analýze lze využít základní nástroje jako `tail`, `cat`, `grep` nebo Event Viewer.

4.1 Detekce signatur (známých událostí)

Shromažďovaná data jsou analyzována a sledována. V případě aktivace pravidla je realizována akce – upozornění, obrana. Automatické SIEM (*Security Information and Event Management*) systémy nepokrývají všechny potřeby organizace a velkou část korelací událostí je nutné doprogramovat.

4.2 Detekce anomálií (neznámých událostí)

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. **Model strojového učení** klasifikuje vstupní data do tříd a shlukuje je do skupin s posobnými vlastnostmi.

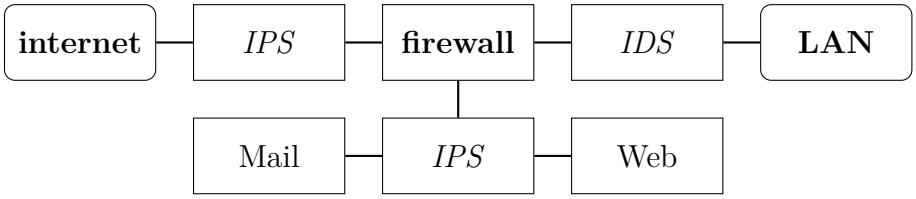
Anomáliemi mohou být nadměrný provoz, změna chování síťového prvku, přihlášení pomocí VPN mimo pracovní hodiny, opakovaná neúspěšná přihlášení, přihlášení z více IP během krátké doby, ...

klasifikovaná data	NOP	NPP	FWA	VPNM	LF	**odhadnutý výsledek**
brute force			ano		ano	—
DDoS		ano	ano			—
data loss	ano		ano	ano		—
—	ano		ano		ano	brute force
—	ano		ano	ano		data loss

5 Detekce nepříznivých událostí na základě signatur a anomálií, systémy IDS/IPS (vzájemný vztah, efektivita a ladění, umístění, základní architektura, zástupci, referenční model).

Intrusion Detection Systems odchytávají pakety a provádí jejich analýzu, *Intrusion Prevention Systems* k tomu umí vytvářet vlastní aktivitu v potlačování nevhodné aktivity.

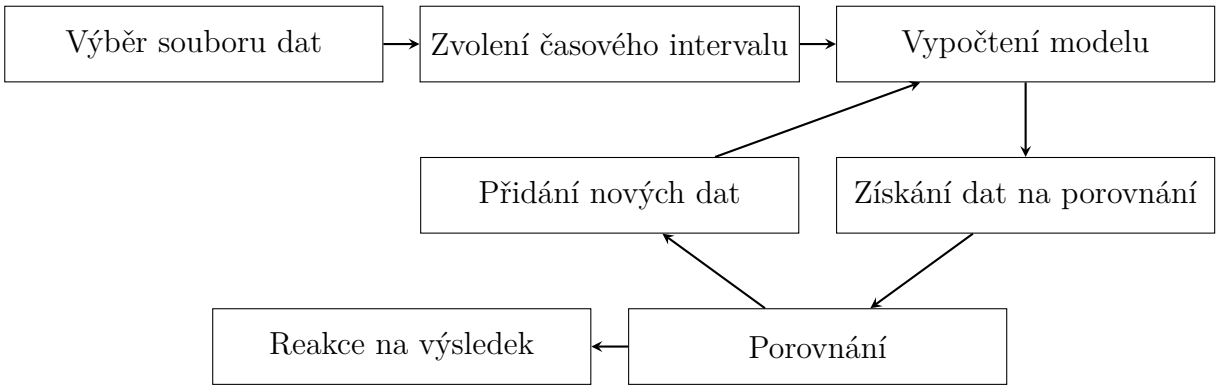
Typicky jsou nasazeny „inline“ jako síťové firewally. Umístění je rozhodující pro jejich správnou funkčnost, často to bývá mezi komponetnami síťové infrastruktury.



IDS/IPS existují ve třech variantách: **komplexní** zařízení je hardware a software vytvořený k efektivnímu odchytávání a analýze provozu, **softwarová** zařízení jsou speciální programy nainstalované na server (Snort, Suricata), **cloudová** jsou dostupná od ISP (Radware, F5).

V **jednovrstvé** architektuře je IPS/IDS tvořen jedinou komponentou, která obstarává všechny funkce. Ve **vícevrstvé** architektuře (zpravidla třívrstvé) existuje jeden manažer (analyzuje hlášení a realizuje opatření), kterému náleží agenti (analyzují protokoly a služby), kteří využívají senzory (monitorující provoz a předávající data).

5.1 Referenční model IPS



6 Dělení penetračních testů (dle znalosti, způsobu realizace a cíle), metodologie testování (pět kroků testování). Penetrační testování webových aplikací (OWASP, průzkum prostředí, závěrečný report).

Penetrační testování je posouzení bezpečnosti pomocí pokusu o průnik do testovaného systému. Umožňuje komplexní prozkoušení nově nasazených aplikací, bezpečnostních systémů, firewallů, IPS/IDS apod. Nutností je mít souhlas majitele systému.[1]

6.1 Dělení penetračních testů

Dle znalosti:

- **Black Box**: tester zná jen vstupy a potenciální výstupy systému, neví nic o vnitřním uspořádání, tj. je v pozici běžného uživatele. U tohoto typu testování se vyžaduje především dobrá znalost skenovacích technik a mapování sítě/systému. *Nevýhodou* může být, že pokud nedojde k proniknutí do sítě, nebude otestována interní bezpečnost.
- **White Box**: k dispozici má topologii sítě, přístupové údaje, dokumentaci, tj. je v pozici vývojáře/technika. Dopadem tohoto velkého množství informací je fakt, že testeři stráví hodně času studií a pochopením systému, oproti samotnému testování. Často se využívají techniky jak statické, tak dynamické analýzy kódu. *Nevýhodou* může být, že testeři nepřemýšlejí jako skutečný útočník.
- **Grey Box**: kombinace dvou předchozích, k dispozici jsou pouze základní znalosti o systému. *Výhodou* je, že testeři se mohou soustředit na testování zranitelné části systému, namísto prohledávání systému od nuly.

Dle realizace:

- **Automatizované testy** využívají specializovaných nástrojů schopných detekce vlastností a chyb zkoumaného systému. Výhodou je rychlost či velké pokrytí *attack surface*, tester však musí znát limitace aplikace a možnosti jejího nastavení.
- **Manuální testy** se provádí ručně a jsou tedy časově mnohem náročnější a od testera vyžadují hlubokou znalost oblasti, umožní však testování na míru a pokrytí detailů, které automatizované testy nepokryjí. Tyto dvě formy se v praxi kombinují.

[1] *Pozor!* Posouzení zranitelnosti není to stejné jako penetrační test. *Penetrační test* je komplexní činností, kde se hledají, identifikují a následně zneužívají (v omezeném rozsahu) zranitelnosti. Oproti tomu *posouzení zranitelností* je především automatizovanou činností, která zranitelnosti hledá, ale nedemonstruje jejich zneužití.

Dle cíle:

Síťová infrastruktura. Webové aplikace. Programy. Telefonní aplikace. IoT zařízení. Fyzický pentest.[2]

6.2 Metodologie

plánování	určují se detailní cíle a časový plán, vymezují se priority
sběr informací	zjištění informací o síti/systému: IP rozsahy, porty, služby
odhalování	zjištění typu a verzí služeb běžících za otevřenými porty
zneužití	využívání nalezených zranitelností
report	předání výsledků, které povedou ke zvýšení bezpečnosti

6.3 Testování webových aplikací

OWASP (Open Web Application Security Project) je nezisková organizace zaměřená na zlepšování bezpečnosti software. Jejím cílem je neomezený přístup jednotlivců i organizací k informacím o bezpečnostních hrozbách. Mezi jejich neznámější publikace patří: OWASP top 10, ASVS (Application Security Verification Standard), OWASP Web Security Testing Guide

6.3.1 OWASP Top 10

Publikace shrnující aktuálních deset nejhorších zranitelností. Vychází z domluvy firem z odvětví a OWASP, nemusí tedy nutně znamenat, že se vyskytují nejčastěji. Postupně se jedná o zranitelnosti (2021):

1. Chybná kontrola přístupu (chyba v ACL)
2. Kryptografické chyby (např. nezabezpečená komunikace aplikace jako HTTP/FTP)
3. Injekce (SQL injection, Code injection)[3]
4. Nezabezpečený design (chyba vzniklá už při plánování projektu)
5. Špatná konfigurace bezpečnostních politik (nenastavení lockout mechanismu po určitém počtu neúspěšných přihlášení)[4]
6. Užívání komponent se známou zranitelností
7. Nekorektní funkce autentizace a identifikace (obecné chyby autentizačních mechanismů)
8. Chyby integrity dat a software[5]
9. Chyby bezpečného loggingu a monitoringu
10. Server-Side Request Forgery (vykonávání requestu jménem serveru)

[2]Penetrační testy lze dále rozdělit na externí a interní. Záleží na počáteční pozici testera, tj. mimo/uvnitř sítě.

[3]XSS: https://www.youtube.com/watch?v=EoaDgUgS6QA.

[4]I XML External Entities – XXE: https://www.youtube.com/watch?v=gjm6VHZa_8s.

[5]Nebezpečná deserializace: https://www.youtube.com/watch?v=HaW15aMzBUM.

6.3.2 OWASP Testing Guide

Rozděluje penetrační test na dvě fáze: **Pasivní fáze** a **Aktivní fáze**.

V pasivní fázi dochází k tzv. *fingerprintingu* (tj. k průzkumu prostředí). Na konci této fáze by útočník měl mít základní znalosti o prostředí webu, jako přístupové body, funkcionality a obsah. Jedna ze základních metod je využití veřejně dostupných informací z vyhledávačů jako Google, DuckDuckGo apod. (tzv. Google Dorking) Dále lze využívat HTTP proxy (jako BurpSuite) pro prozkoumání zaslaných HTTP žádostí za účelem identifikace OS serveru nebo typu serveru (Apache, Microsoft, Apache Tomcat, ...).

V aktivní fázi už dochází k interpetaci dat získaných z fingerprintingu a pokusy o exploitaci. Všechny zranitelnosti, payloady a nevydařené útoky by měly být řádně zapsány. To umožní později sepsat koherentní a komplexní report.

6.3.3 Report

V **OWASP Web Security Testing Guide** je uvedeno že dobrý report je základ penetračního testu. Bez něj nelze prezentovat výsledky a zajistit, že chyby budou opraveny. Rozděluje report na čtyři části:

Úvod	prostor pro obsah, jména členů týmu, limity testování, časové rozmezí testu
Shrnutí	cíl testu, shrnutí dopadů z ekonomického a compliance hlediska, návrhy pro budoucí zlepšení
Nálezy	výpis všech nalezených zranitelností, všechny zranitelnosti by měly obsahovat co nejvíce detailní informace
Dodatky	použité metody, nástroje, vysvětlení závažnosti, relevantní výstupy nástrojů, ...

Více např. https://owasp.org/www-project-web-security-testing-guide/v42/5-Reporting/README.html.

7 (D)DoS útoky (princip, rozdělení, popis základních útoků: SYN Flood, HTTP Flood, DNS reflection, Ping of Death, Slow-Loris). Zátěžové testování (typy testů, nejznámější nástroje).

DDoS (*Distributed Denial of Services*) je DoS útok realizovaný z více uzlů, které s hlavním útočníkem spolupracují a napadají cílový uzel.
Botnet je skupina uzlů (až statisíce), které zpravidla bez vědomí svých majitelů útočí na cíle na internetu. Svému majiteli vytváří zpravidla zisk nebo jiné prostředky (exploit, trojan, pronájem, těžba kryptoměn, krádež dat).

7.1 Typy útoků

7.1.1 Záplavové útoky

ARP flood: ARP dotazy
RST flood: pakety obsahují falešné IP adresy s parametrem RST, který resetuje spojení
SYN flood: otevření spojení bez následného potvrzení[6]
HTTP flood: legitimní, ale náročné GET a POST dotazy
UDP flood: legitimní UDP datagramy
PingSweep: zprávy od uzlů požadují odpovědi od cílového systému[7]
Smurf: ICMP pakety se *spoofovanou* adresou oběti jsou posílány na broadcast adresu
Reflection attack: malý dotaz se zdrojovou adresou oběti: DNS/NTP amplifikace[8]

7.1.2 Logické útoky

Teardrop: fragmenty paketů se špatně nastaveným offsetem: cíl není schopen správně sestavit celý packet
Land: TCP-SYN mají cílovou IP adresu i port shodné se zdrojovou adresou
Ping of Death: ICMP ping s velikostí nad 65kB
ReDoS: extrémní zátěž pomocí regulérních výrazů
XMasTree: TCP paket má v hlavičce nastaveny příznaky FIN, URG, PST
Slow-Loris: nekompletní pomalý GET dotaz

[6] https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/
[7] https://www.netscout.com/what-is-ddos/icmp-flood
[8] https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/

7.2 Detekce a mitigace

Detekce signatur a anomálií. Robustní a bezpečná síťová infrastruktura; firewally, IDS, honeypoty, redundantní linky a servery; vysokorychlostní DDoS filtry; blacklisting & whitelisting; *tarpit* (udržení příchozích spojení v open-state, snížení TCP window na nulu); rate limiting na směrovačích; filtrace na základě reputace zdroje (IP rozsah, geolokace, služba).

7.3 Zátěžové testování

Lze testovat sítě jako celek, síťová zařízení (servery, routery, firewally), koncové stanice (počítače, telefony) nebo aplikační vrstvu (webové služby, operační systémy, aplikace).

Postup testování: **definice** (specifikace cíle, požadavků a běžného provozu), **příprava** (nastavení sítě a testeru), **realizace** (monitoring, opakování), **vyhodnocení** (dokumentace).

Hlídanými **parametry** jsou: doba, počet dotazů, čas na dotaz, dotazy za čas, přenesená data, distribuční rozložení odpovědí, ...

Performance test je zatížení systému definovanou zátěží pro změření chování. **Stress test** je postupné zatěžování narůstajícím počtem paralelních spojení. **Soak test** je dlouhodobé testování. **Failover test** je ověření chování systému v případě selhání. **Targeted infrastructure test** slouží k detekci nejslabších míst. **Volume test** je ověření chování při zvýšeném objemu dat.

Je vhodné testovat mimo běžnou špičku, aby nebyla ohrožena finanční (služby zákazníkům) nebo bezpečnostná strana sítě.

7.4 Software testery

Avalanche (hardware, do 40Gbps), Apache jMeter, LOIC.

8 Netechnické typy útoků (sociální inženýrství, phising; používané techniky), útoky MitM (ARP spoofing, DNS spoofing, SSL strip, SSL sniff).

sociální inženýrství: psychická manipulace s lidmi za účelem zisku informací, přístupu ke službě nebo provedení podvodu
phishing: kontaktování uživatelů s cílem získání citlivých informaci pro škodlivé účely
spear phishing: phishing mířený na konkrétní osoby
whale phishing: cílení na vlivné představitele firm či organizací nebo na veřejné osoby
cloning: vytvoření phishing zprávy z původně legitimní
baiting: zanechání malware na médiu, které má oběť objevit a připojit ke svému sytému
tailgating: průnik do chráněných prostor s nevědomou pomocí legitimního uživatele
insider threats: hrozby od vnitřního uživatele
vydávání se za jinou profesi (technická podpora, údržba)

Phishing

Vektory bývají e-mail, sociální sítě, webové portály nebo instant messaging. **Cílem** bývá přístup k bankovnictví, webovým portálům, sociálním sítím nebo IT službám. **Obranou** je legislativa, školení uživatelů, veřejná informovanost, technická opatření (e-mail filtering, vynucení 2FA).

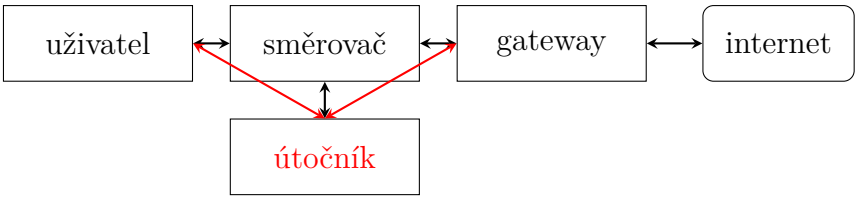
Využívá se **manipulace s odkazy** (modifikace URL, rozdíl mezi obsahem a cílem `<a>` tagu pomocí JS), **obcházení filtrace** (využití obrázků či videa místo textu), **website tampering** (podvržení webových stránek) nebo **covert redirect** (přesměrování odkazů na phishing stránky s XSS/falešným přihlášením).

8.1 MitM

8.1.1 ARP spoofing

Také *ARP Cache Poisoning* nebo *ARP Poison Routing*. Jde o způsob podvrhnutí ARP zpráv na lokální síti; cílem je asociovat útočníkovu MAC adresu s IP adresou jiného síťového prvku (brána) a routovat veškerou komunikaci místo něj. Útočník může způsobit DoS (zahazováním některých paketů) nebo MitM (úpravou dat).

Při překladu lokální IP adresy na MAC dochází k zaslání broadcast paketu, na který zařízení s požadovanou IP adresou pošle odpověď. Tyto zprávy nejsou nijak autentizované, ARP je stateless protokol a všechna zařízení na síti automaticky *cachují* ARP odpovědi bez ohledu na to, jestli o ně požádaly.



Síť pod ARP spoof útokem

Ochranou může být integrace s DHCP serverem nebo monitoring ARP provozu.

8.1.2 DNS spoofing

Způsob podvrhnutí DNS zpráv a otrávení DNS cache s účelem směrovat některé DNS záznamy na falešné IP adresy. V normálním prostředí plní roli neautoritativního DNS serveru lokální směrovač, který směrovací data získává od dalšího DNS serveru (síť, ISP, autoritativní DNS server).

DNSSEC zaručuje bezpečnost komunikace s DNS servery. Všechny odpovědi z DNSSEC zón jsou podepsány. Krom `A`/`AAAA` záznamů lze chránit i `TXT`, `MX` a další: SSHFP (SSH klíče vázané na hostname) nebo IPSec klíče. Zajišťuje pouze autentizaci, ne důvěrnost.

8.1.3 SSL strip

Degradace HTTPS spojení na HTTP. Tři roky po jeho „objevení“ v roce 2009 bylo vydáno RFC 6797: HTTP Strict Transport Security (HSTS), zavádějící HTTP hlavičku `Strict-Transport-Security`. Klienti podporující HSTS musí upgradovat na HTTPS *před* připojením k webu, a pokud není možné TLS spojení navázat (nedůvěryhodný certifikát), spojení by mělo být ukončeno a na web by neměl být povolen přístup.[9]

8.1.4 SSL sniff

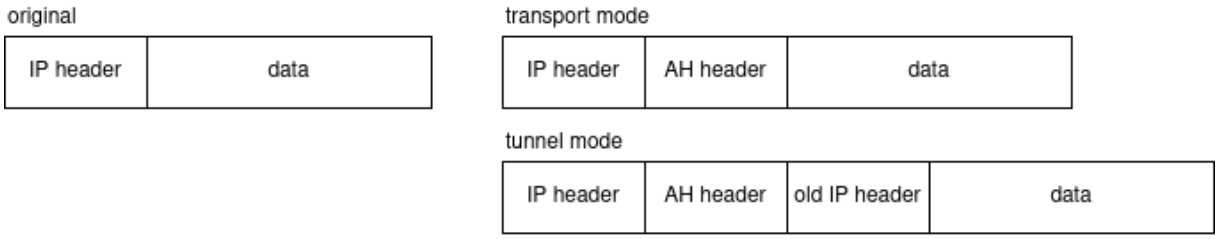
Zachycení TLS. Útočník musí mít k dispozici certifikát kterému důvěřuje prohlížeč, tj. ukradený certifikát podepsaný CA, nebo falešný a importovaný do prohlížeče/systému oběti.

[9]Mezi limitace HSTS patří náchylnost na NTP manipulaci (platnost HSTS hlavičky je určena časem: `Strict-Transport-Security: max-age=31536000`) nebo na stripping při první návštěvě, protože se HSTS hlavička přenáší až první odpovědí serveru.

9 Protokoly IPsec a TLS (princip, umístění TCP/IP, průběh komunikace, autentizace, utajení a integrita dat).

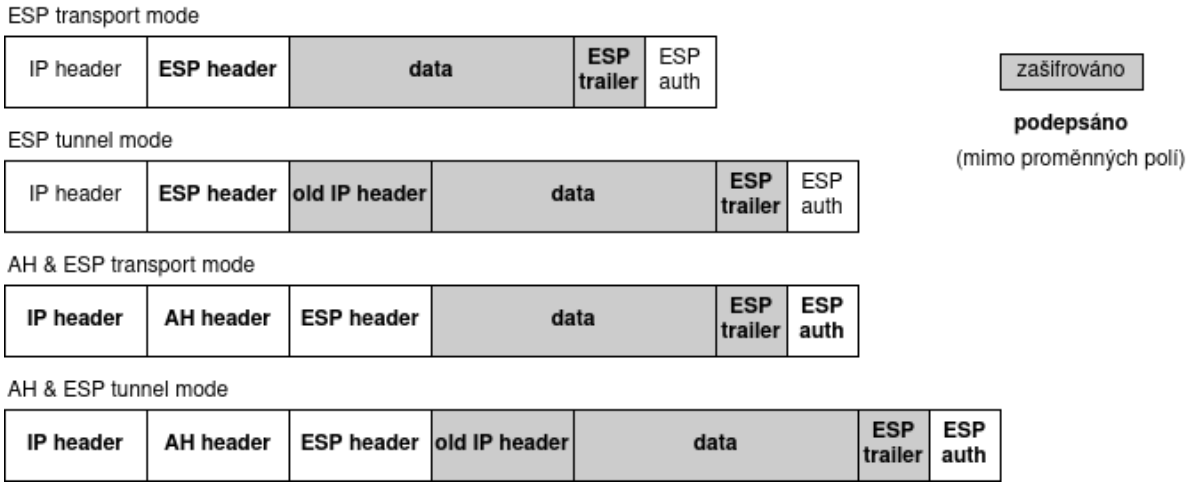
9.1 IPSec

Pracuje na síťové vrstvě (L3): end-to-end šifrování TCP/UDP komunikace mezi zařízeními s IP adresou. Šifrují se data v paketech (transport) nebo pakety celé (tunnel), včetně podpory autentizace.



Authentication header zajišťuje integritu a autentičnost IP paketů, chrání proti replay útokům. **Encapsulating Security Payloads** zajišťuje důvěrnost pomocí šifrování. **Security Association** popisuje IPSec spojení včetně parametrů zabezpečení. Aktivní spojení je uloženo v databázi (SAD), management a pravidla jsou uložena v SPD (*Security Policy Database*).

Pro ustanovení klíče IPSec využívá symetrickou kryptografii: pre-shared key, IKE1/2, Kerberos.

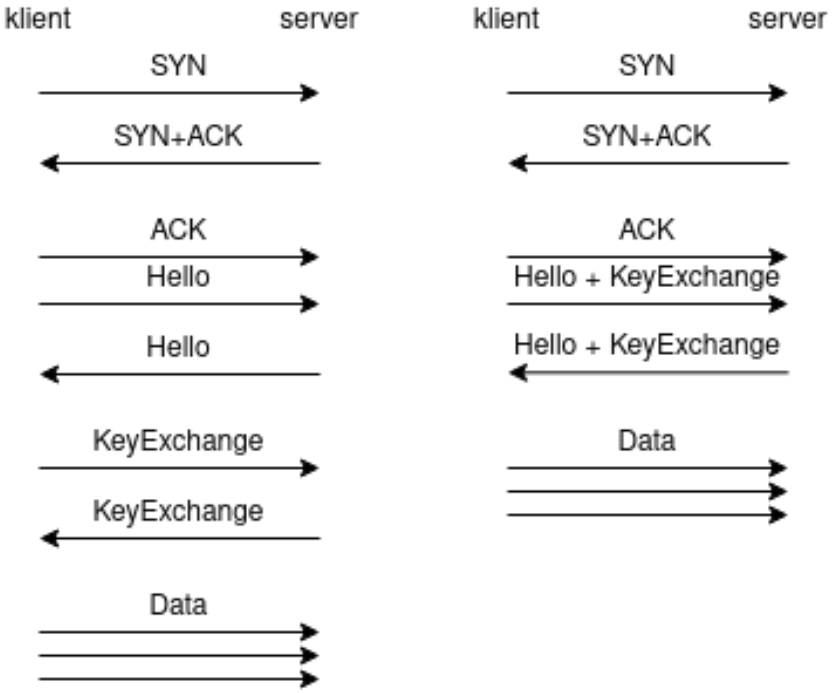


9.2 TLS

Pracuje na transportní vrstvě (L4): end-to-end šifrování TCP/UDP mezi klientem a serverem, pro aplikační vrstvu transparentní. Je složen z **handshake** (inicializace spoje, autentikace stran, ustanovení klíče), **record** (datový přenos, MAC autentizace) a **alert** (notifikace chyb a varování) protokolů.

Security strings, např. `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`.

- Ustanovení klíče: ECDHE, DHE
- Podpis: RSA, DSA, ECDSA
- Šifrování: AEC-GCM, ChaCha
- Hashování: SHA-256, SHA-384



Výměna zpráv v TLS 1.2 a TLS 1.3

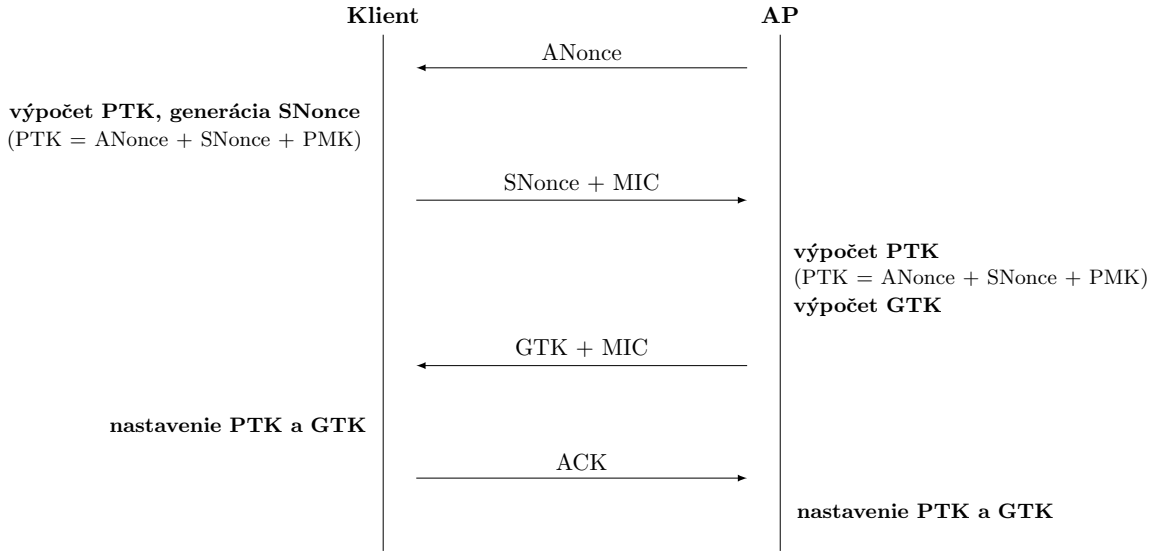
10 Zabezpečení 802.11 (WPA2, používaná kryptografická primitiva, klíčové hospodářství, popis 4Way handshake, testování bezpečnosti).

WEP (Wired Equivalent Privacy): nevhodná implementace šifrování, chybí management klíčů, předvídatelný obsah. Šifrování pomocí 64b/128b RC4 klíčů, integrita CRC-32, jednostranná autentizace. 2w handshake: open system (pouze požadavek s SSID sítě), 4w handshake: požadavek s SSID, nádhodný řetězec r, odpověď $E_{k_{\text{priv}}}(r)$, přijmutí/odmítnutí.
WPA (WiFi Protected Access): rychlé vydání kvůli nedostatečné bezpečnostni WEP. Autentizace pomocí PSK/IEEE 802.1x, důvěrnost TKIP (Temporal Key Integrity Protocol) s per-packet obměnou klíče, integrita MIC (Message Integrity Check). Zachována zpětná kompatibilita s WEP.
WPA2 (WPA II): Důvěrnost pomocí AES, integrita CCMP[10].
WPA3 (WPA III): AES-256-GCM, HMAC SHA-384. SAE (Simultaneous Authentication of Equals) zajišťuje bezpečnější výměnu a dopřednou bezpečnost v Personal módu[11].

PMK (Pairwise Master Key) je získán z úspěšné autentizace (u Enterprise zaslán serverem, u Personal je shodný s PSK, který se odvozuje z hesla[12]), další klíče jsou z něj derivovány hashováním:
KCK (Key Confirmation Key): autentizační zprávy MIC během čtyřcestné výměny,
KEK (Key Encryption Key): zajištění důvěrnostni dat během čtyřcestné výměny,
TEK (Temporary Encryption Key): šifrování dat v TKIP a CCMP,
TMK (Temporary MIC Key): autentizace dat v TKIP.

	WPA-PSK	**WPA**	**WPA2-PSK**	**WPA2**
Autentizace	PSK	802.1x (PEAP)	PSK	802.1x (PEAP)
Šifrování	TKIP (RC4)	TKIP (RC4)	CCMP (AES)	CCMP (AES)
Enterprise	nevhodné	dobrá úroveň	nevhodné	nejlepší úroveň
Personal	dobrá úroveň	nevhodné	nejlepší úroveň	nevhodné

[10] Útok **KRACK**: Key Reinstallation Attacks z roku 2017.
[11] V dubnu 2019 byla ve WPA3 objevena zranitelnost **Dragonblood** umožňující *downgrade* spojení a útok postranními kanály: umožnění zjištění hesla silou a DoS útoku na stanici.
[12] PSK = PBKDF2($password, SSID, SSID\_length$, rounds = 4096, output = 256), viz RFC 8018.



Obrázek 1: WPA2 4-way handshake.

10.1 Testování bezpečnosti

WEP: pasivní: `airodump-ng`, aktivní: `aireplay-ng` (Chopchop attack, Caffe Latte attack, ...)
WPA: bruteforce (`airodump-ng`, `aircrack-ng`) & dictionary/rainbow attacks
zmatení uživatele: vytvoření falešného AP a vyzrazení hesla
automatické nástroje `wifite`, `fluxion`