**Souhrn otázky**

* Druhy útoků v LAN
* Druhy útoků na L2, možnosti předcházení útokům na LAN
* Zabezpečení přístupu na switche a routery

**TL;DR**

* Krádež informací, dat, atd.
* Zranitelnost může být v OS, konfiguraci, hardwaru, atd.
* ARP spoofing, MAC flooding, DHCP spoofing/starvation, ……….
* AAA, Firewall
* DHCP Snooping

**Druhy útoků v LAN**

**Důvody proč útoky**

* Získání dat ve svůj prospěch
  + Krádež informací — information theft
  + Krádež identity — identity theft
* Chuť někomu dokázat, že jeho síť je napadnutelná
* Vyřazení uzlů z činnosti, odříznutí od zdrojů informací
  + Modifikace či ztráta dat — Data loss and manipulation
  + Zamezení přístupu ke službám — Distruption/Denial of Services

**Nejzranitelnější místa**

* Technologie — OS, Protokoly
* Konfigurace — Nezabezpečené přístupové účty, slabá hesla
* Nefunkční bezpečnostní politika — Např. ve windows špatně nastavené group policy, user policy, atd.

ale jsou i hardwarové jako:

* Hardware samotný — Fyzické poškození serverů, routerů, switchů, kabeláže a jiných prostředků
* Prostředí — Teplotní extrémy, vlhkost
* Napájení z el. sítě — Napěťové špičky, výpadky, kolísavý příkon
* Údržba — Špatná manipulace s HW, elektrostatický výboj, špatná kabeláž, atd.

**Útoky na L2**

* využívají slabiny protokolů jako STP, ARP nebo VLAN
* MAC flooding, ARP spoofing, DHCP spoofing, STP manipulation

**Útoky na L3**

* IP protokoly a konfigurace
* IP spoofing, Rogue router(falešný router, který posílá provoz na škodlivé cíle)

**Útoky na L4**

* slabiny transportních protokolů TCP a UDP
* TCP SYN flood, UDP flood, TCP session hijack

**Útoky na L7**

* DNS spoofing(manipulace s DNS záznamy, aby uživatelé přistupovali na škodlivé weby)

**Druhy útoků v L2**

**ARP spoofing**

* Útočník se vydává za jiného uživatele v Síti pomocí padělaných ARP odpovědí, což mu umožňuje odposlouchávat nebo manipulovat s daty, které procházejí přes síťovou kartu oběti.

**ARP poisoning**

* ARP (Address Resolution Protocol) je typ kybernetického útoku, který spočívá v manipulaci S mezipamětí ARP síťového zařízení
* Odesláním podvržených zpráv ARP do cílového zařízení může útočník přiřadit svou vlastní adresu MAC k adrese IP jiného zařízení v síti a zachytit nebo přesměrovat provoz určený pro toto zařízení.

**MAC flooding**

* Útočník zaplaví tabulku MAC adres ve switchi falešnými MAC adresami, čímž způsobí, že switch přepne do režimu broadcastu a všechna data posílá na všechny porty, což může způsobit zahlcení sítě a zpomalení přenosu dat.

**VLAN hopping**

* Útočník využívá chyby v konfiguraci switche, aby se dostal z jedné VLAN do druhé, což mu umožňuje získat přístup k datům, ke kterým by jinak neměl přístup.

**DCHP útoky**

* Využívají zranitelnost DHCP protokolu
* Dva typy:
  1. DHCP spoofing → Útočník se vydává za DHCP server
  2. DHCP starvation → Útočník vyčerpá dostupné IP adresy z DHCP serveru
     + Ve výsledku, žádné jiné zařízení nebude moct dostat IP od DHCP serveru

**Podvržení IP adresy**

* Útočník se vydává za jiné zařízení pomocí falšené IP adresy
* Toho lze využít k různých typům útoků:
  + Například k IP spoofingu, kdy se útočník vydává za důvěryhodný zdroj (např. tiskárna) (kdo by nechtěl být tiskárnou?!)

**VLAN double tagging**

* Typ útoku, kdy rámec má dva VLAN tagy
* Útojk spočívá v tom, že když switch přijme rámec, dá dopryč první tag a pošle rámec na další uzel. Další uzel uvidí tento rámec a zase zkontroluje VLAN tag → Tento tag může odkazovat do sítí, do kterých by posílající uzel neměl přístup.

**MAC spoofing**

* Využívá zranitelnost ARP protokolu
* Útočník se vydává za jinou MAC adresu, aby získal přístup do sítě
* Tento typ útoku se používá s dalšími typy útoků:
  + ARP poisoning
  + Man-in-the-middle attack

**Spanning Tree Protocol (STP)**

* Protokol STP (**Spanning Tree Protocol**) je síťový protokol, který slouží k **prevenci smyček v topologii sítě**
* Při nesprávné konfiguraci však může být protokol STP zranitelný vůči útokům, které mohou způsobit **přetížení sítě** nebo **neoprávněný přístup k datům**.
* Jedním z příkladů útoku založeného na protokolu STP je útok typu **BPDU** (**Bridge Protocol Data Unit**), při kterém útočník odešle velké množství rámců BPDU, aby **zahltil** síť a způsobil její **výpadek+-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------**
* Abyste zabránili útokům založeným na protokolu STP, je důležité správně **nakonfigurovat protokol** a sledovat síť, zda se v ní nevyskytují **neobvyklé vzorce provozu**.

**CDP — Cisco Discovery Protocol**

* Proprietární protokol Cisco-a
* Umožňuje výměnu informací o připojených Cisco zařízeních
  + Také umožňuje automatickou konfiguraci mezi prvky pro jejich vzájemné propojení
* Když útočník odchytí CDP zprávu, může se dozvědět mnoho informací o prvku, který tuto zprávu zaslal — Model, verzi IOS, atd.
* Je doporučeno protokol zakázat

**Možnosti předcházení útokům v LAN**

**Metody**

* AAA — Authentication, Authorization, Accounting
* Kontrola vstupu do počítačové sítě a provozu v počítačové síti
* Zabezpečení koncových uzlů
* Protokoly vytvářející zabezpečenou komunikaci mezi zařízeními (SSH, SSL/TLS, etc.)
* Kryptografické prostředky (zašifrované zprávy atd.)

**Použití síťových zařízení, která podporují funkce jako je:**

* **802.1X autentizace** 
  + umožňuje zabezpečení přístupu do počítačové sítě
  + Když se počítač připojí k přípojnému bodu, je po něm pomocí IEEE 802.1X vyžadována autentizace (např. uživatelské jméno a heslo).
  + Přípojný bod blokuje veškerý ostatní datový provoz klienta do té doby, než je úspěšně autentizován
* **VLAN isolation**
* **MAC filtering**
* DHCP snooping
* IP Source Guard
* Port security

Přidělování **unikátních hesel** a uživatelských jmen pro každého uživatele sítě a **periodická změna hesel.**

Pravidelná **aktualizace firmware a bezpečnostních záplat** na síťových zařízeních.

Implementace bezpečnostních **politik** pro používání síťových služeb a aplikací.

**AAA**

**1. Authentication**

* Authentication — Ověření — Ověřuje pravost identity uživatele
  + Prostřednictvím fyzických autentizačních pomůcek — Čipová karta, kryptografický klíč v podobně USB
  + Výměnou a ověřením autentizačních informací — Loginů, hesel, klíčů, elektronických podpisů,…

**2. Authorization**

* Určuje, co uživatel může dělat a k čemu má právo

**3. Accounting**

* Sleduje a zapisuje akce a činnosti uživatele
* Pomocí těchto logů můžeme objevit uživatele, který dělá něco sus (např. zkouší najít nějakou bezpečnostní díru)

**Zabezpečení přístupu na switche a routery**

Pomocí např.

* Vytvoření databáze uživatelů, kteří mohou ke konfiguraci přistupovat
* Zaheslovat privilegový režim, stejně tak konzolový a terminálový přístup k prvku
* Zakázat telnet (zapnutím ssh)
* Vypnout nepoužívané porty (u switche)
* Trunk portům nastavit jinou native VLAN než 1
* Zakázat DTP
* Netrunkové porty nastavit jako access porty a přiřadit je do jednotlivých VLAN
  + Na access portech nastavit BPDUGuard
* Nastavit na portech port security

**Port security na portu**

* Můžeme omezit počet platných MAC adres
* Možnosti nastavení MAC adres:
  + Staticky — Ručně napsaný whitelist MAC adres
  + Dynamicky — Adresy se učí dynamicky a ukládají se do MAC adresy
  + Sticky — Naučené MAC adresy se uloží a neresetují po restartu switche
* IOS kontroluje, zda:
  + Nepřejde se přes maximální počet MAC adres na jednom portu
  + Neukáže se stejná MAC adresa na jiném portu
* Režimy porušení pravidla:
  + Ochrana — Protect — Rámce s neznámou MAC jsou zahozeny
    - Dokud se neuvolní místo pro novou MAC, nebo se nenavýší počet možný MAC
    - Neodesílá se žádné oznámení do výstupu
  + Omezení — Restrict — To samé jako protect, ale probíhá oznámení do výstupu (loguje se to)
    - A counter narušení se zvýší o jedno
  + Vypnutí — Shutdown — Výchozí mód; Při narušení port přejde do error-disabled módu, counter narušení se zvýšáí o jedlo
    - Port se zapíná pomocí shutdown příkazu a následně no shutdown

**Nasazení DHCP Snoopingu**

Na celé sítě i pro jednotlivé VLAN, lze nastavit na porty:

* Z jakých portů můžou přicházet odpovědi na DHCP zprávy
  + Aka, nějaký random access port nemůže poslat DHCPOFFER

Porty jsou označeny jako:

* Důvěryhodné (trusted) — Předává všechny DHCP zprávy
  + Do tohoto portu je námi připojený DHCP server
* Nedůvěryhodný (untrusted) — Mohou přijímat pouze DHCP requesty
  + Pokud přijde DHCPOFFER, port se vypne

DHCP Snooping si tvoří svou tabulku (DHCP binding table), se informacemi:

* Klient MAC address
* IP Adress
* VLAN s číslem port