Ročníková Práce

Materiály ke kyberbezpečnosti

Jan Filipec

Základy sítí

představení základních pojmů v sítích

- ### Co je to počítačová síť

  lidi a zařízení jsou entity (subjekty), které komunikují jeden s druhým přes sebe, jako když si lidi povídají v kroužku - zařízení v digitálním světě také mají kroužek

(zdroj : colcampus.com)

Toto prostředí vytvořené ze zařízeních v digitálním světě se nazývá “počítačová síť”’

Jinými slovy, struktura ve které jsou aspoň dvě zařízení, které spolu komunikují může být nazýváno “počítačová síť”.

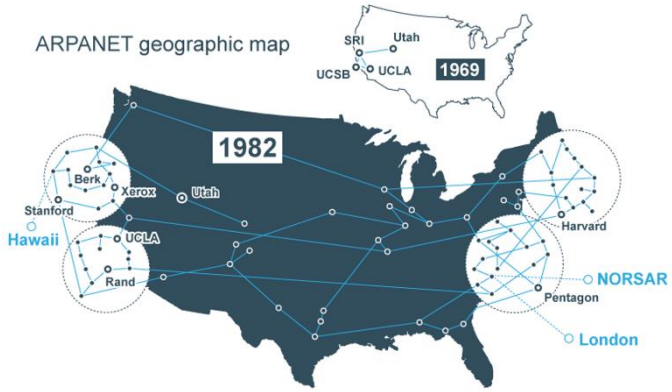
(zdroj : speaknetworks.com)

Účely počítačových sítí

sítě se staly užitečnými hned v několika směrech ve vývoji technologiích. sítě se používají hlavně pro:

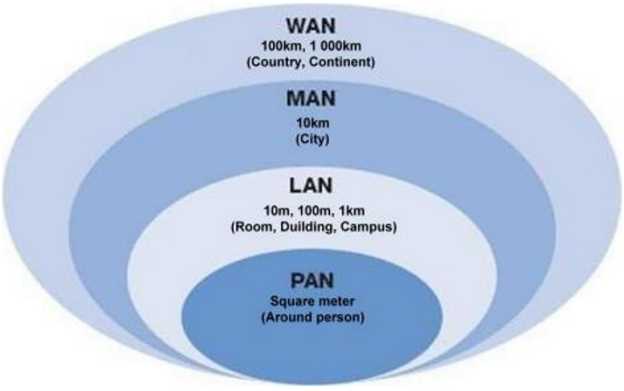
1. Přenášení obrázků a zvuku (chatování a online schůzky)
2. sdílení hardwaru (tiskáren)
3. sdílení, posílání dat, souborů a informací
4. sdílení softwaru
5. Centrální vedení
6. podpora (support)

- **ARPANET a Internet**
  - Internet je systém, který propojuje sítě, kde spolu zařízení komunikují
  - Internet prošel několika procesy ve vývoji až do posud. Když se poprvé objevil, nebyl tak oblíbený a rozrostlý jako teď. Internet byl na začátku využíván pouze pro armádní potřeby.
  - Advanced Research Projects Agency Network (ARPANET) je počítačová síť braná jako počátek internetu. Základy internetových technologiích jsou technologie použité právě v ARPANETu. V roce 1969 byl ARPANET připojen do třech univerzitních sítí v USA, vytvářející síť, která se později ohromnou rychlostí rozrostla po celém světě
  - Obrázek zachycuje ARPANET v roce 1969 a 1982



(Zdroj : portswigger.net)

  - tato síť, která se stále rozšiřuje i v současnosti se nazývá Internet.
- **Typy sítí**
  - počítačové sítě jsou geograficky rozděleny do několika skupin podle velikosti. Mohou být sítě s miliony zařízeními, ale také sítě které mají 2 - 3 zařízení.
  - Obrázek ukazuje typy sítí podle velikosti.



(Zdroj: networking.layer-x.com)

Osobní počítačová síť (personal area network - PAN)

  - osobní počítačová síť neboli PAN představuje sítě s minimálním počtem zařízení, které jsou ve velmi malé vzdálenosti (např. v deseti metrech). Pro

představu - mobilní zařízení a bezdrátová sluchátka k sobě připojena přes Bluetooth jsou příkladem této sítě. Jsou tu pouze dvě zařízení v této síti, mobil a bezdrátová sluchátka

(Zdroj : pelfusion.com)

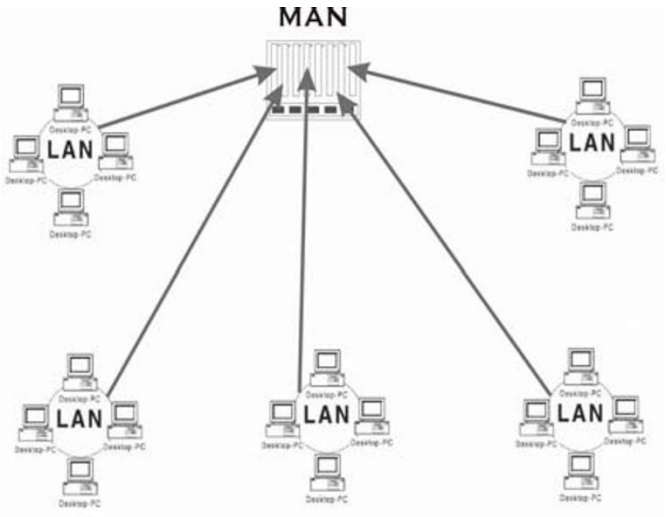
Lokální počítačová síť (Local Area Network - LAN)

- Lokální počítačová síť neboli LAN je síť s větší vzdáleností než PAN. Počet zařízení může být o dost větší. Tento typ je nejpoužívanější ze všech. Občas může být síť se dvěma zařízeními také nazývána LAN. Například domácí sítě, které sdílí Internet po budově se může jednat o LAN

(Zdroj: Ipcisco.com)

Metropolitní počítačová síť (Metropolitan Area Network - MAN)

- Metropolitní síť může být geograficky velká asi jako město, ve které jsou LANky propojeny. Síť je propojena optickými kabely (optika je jeden z druhů přenosu dat, který přenáší data pomocí skleněných vláken, ve kterých proudí světelné paprsky)



(Zdroj: researchgate.net)

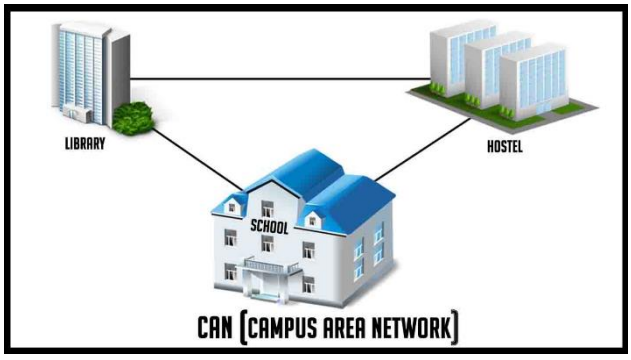
Globální počítačová síť (Wide Area Network - WAN)

- globální síť je největší počítačová síť ze všech sítí na světě. Tato síť je tak velká, že může přesahovat i kontinenty. Hostuje všechny ostatní sítě v ní. Jako příklad takové sítě je Internet.

(Zdroj: ipxo.com)

Univerzitní počítačová síť (Campus Area Network - CAN)

- univerzitní síť je geograficky menší než MAN, ale větší než LAN. Tato síť může obsahovat více LAN sítí. Většinou jí používají univerzity, instituce, nebo soukromé podniky.



(Zdroj: itrelease.com)

- **Síťové topologie**
  - síťová topologie je mapa vytvořená pro pochopení fyzických nebo logických struktur sítě. Umístění zařízení a kabelů v síti jsou mimo jiné fakta, která určují topologii sítě. Mít síťové topologie má mnoho plusů. například je možné vidět která zařízení v síti budou ohrožena pokud nastane nějaký kyberútok, nebo pokud nějaké zařízení selže s vykonáním úkolu. Síťové topologie se dělí do dvou typů:

1. fyzické topologie
2. logické topologie

Fyzické topologie

- typ sítě ve které jsou všechna zařízení a komponenty v síti zakresleny kde přesně se nachází. Díky této topologii vidíte kde je jaký kabel a k čemu je připojen. To co vidíme na obrázku má fyzickou podobu. Například pokud je zařízení v cestě z bodu A do bodu B, tak to zařízení je vidět ve fyzické topologii.

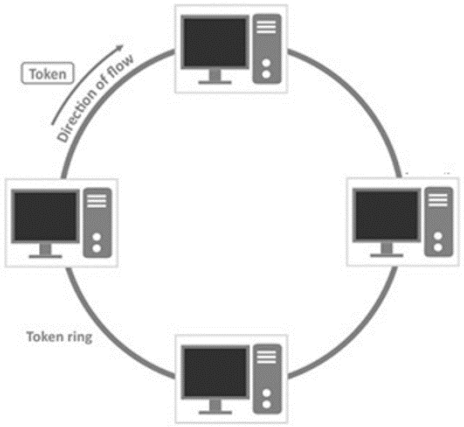
Logické topologie

- Tato topologie neukazuje přesné umístění zařízení jako fyzická. Obsahuje méně prvků oproti fyzické topologii. Protože proud dat je důležitý - například data, která jdou ze zařízení A do zařízení B nemusí být zahrnuté v té topologii pokud to prochází přes zařízení C, které je mezi A a B a pokud to C nemá žádný vliv na data která potřebují být zobrazená na něm. V této topologii se zapisují cesty dat, ve fyzické umístění zařízení a kabelů. Příklady logických topologiích:

1. kruhová topologie
2. hvězdicová topologie
3. pletivová topologie
4. autobusová topologie
5 .point - to - point topologie
6. stromová topologie

Kruhová topologie

- Tato topologie funguje na principu uzavřené (často kruhové) smyčky. Poslaná data cestují po obvodu v jednom určeném směru dokud nenarazí na cílový bod. Každý uzel (směrovač, switch, nebo zařízení které přeposílá data) přepošle dál dokud se nedostanou do cíle. Není tu žádná hierarchie v uzlech, takže jsou si rovni.

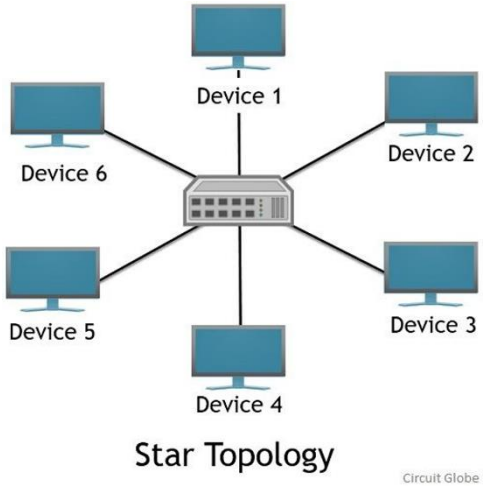


(Zdroj: elprocus.com)

- plusy: výkonnější než autobusová pokud se jedná o velká data, nepotřebuje to hlavní uzel, jednoduché na instalaci a konfiguraci, díky point-to-point struktury, errory jsou jednoduché na opravení
- mínusy: pokud je v ní uzel, který nepřeposílá data tak celá síť je dotčena, rychlost přenosu se zmenšuje s více uzlami

Hvězdicová topologie

- Každý uzel v této topologii je připojen na centrální uzel, všechna data jsou posílaná přes centrální uzel. Hvězdicová topologie je jedna z nejčastějších sítových topologií.



(Zdroj: circuitglobe.com)

- Plusy: pokud jeden z uzlů přestane fungovat, ostatní běží, pokud se přidávají, nebo odendávají uzly, na síť to nemá vliv, je vhodná pro velké sítě s mnoha zařízeními
- Mínusy: velký rozpočet díky hodně potřebným kabelům, Pokud selže centrální uzel, všechny uzly přestanou přijímat data

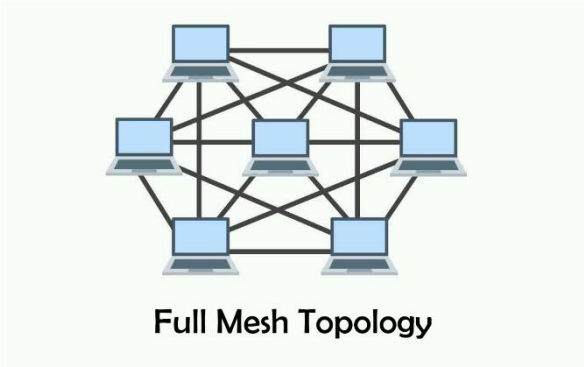
Pletivová topologie (síťová)

- Topologie, kde není žádný centrální uzel a každý uzel může být přímo připojen k jinému. Tato topologie není vhodná pro velké sítě. dělí se do dvou typů:

11. plně pletivová
12. částečně pletivová

Plně pletivová

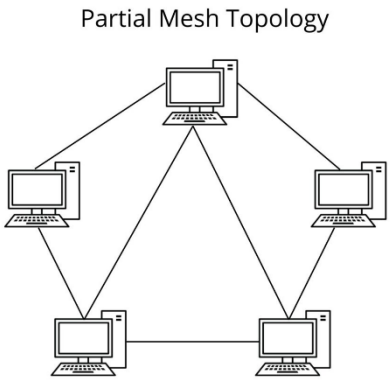
- Každý uzel v síti je připojen do všech ostatních uzlů kabelově. Pokud jedno spojení je přerušeno, nevadí, data si najdou jiný přes jiné uzly.



(Zdroj: itrelease.com)

Částečně pletivová

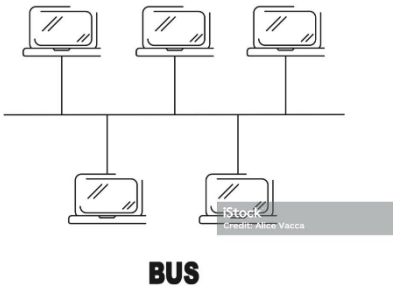
Každý uzel není propojený ke každému uzlu, ale jsou logicky propojeny tak, aby když selže jedno spojení se mohly data dostat k cíli jinak.



(Zdroj: ofbit.in)

Autobusová topologie

- Topologie, kde uzly jsou umístěny v běžných cestách a převody dat jsou vytvořeny s obousměrným spojením. V této topologii, každý uzel přijímá každé putující data i když pro ně nejsou. Není tu žádná hierarchie uzlů, takže žádné přeposílání není upřednostněno.

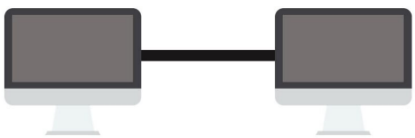


(Zdroj: istockphoto.com)

- Plusy: přidávání směrovačů (uzlů) je jednoduché, vhodné pro menší sítě, malé náklady na kabely
- Mínusy: velká pravděpodobnost ztráty paketu (data/informace v síti), výkon může být pomalejší díky hodně uzlů, velké riziko errorů

Point-to-Point topologie

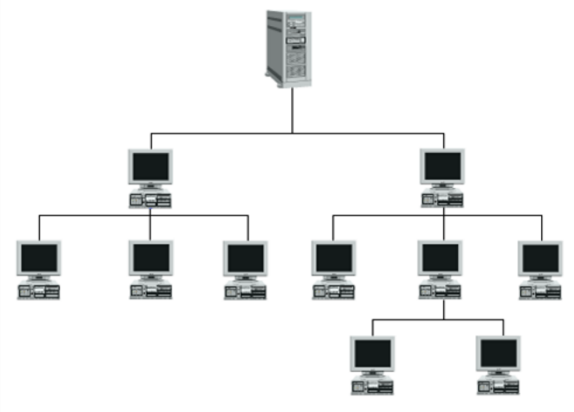
- Nejjednodušší topologie, skládá se ze dvou uzlů, nebo zařízeních propojených do sebe. Například zvednutí hovoru z jiného zařízení se dá říkat point-to-point topologie.



(Zdroj: studyfix.de)

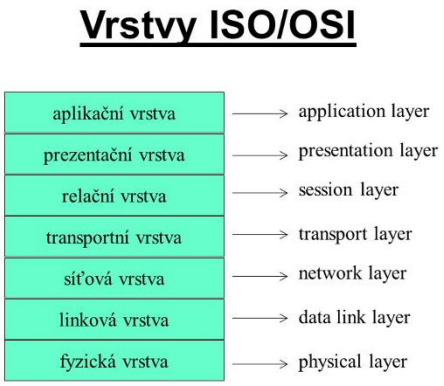
Stromová topologie

- Je to směs hvězdicové a autobusové topologie. Stromová topologie má hierarchické seskupení uzlů a koncových bodů a každý uzel může mít jakékoliv číslo poduzlů.



(Zdroj. hardwaresiti.webnode.cz)

- **OSI Model**
  - OSI model (Open Systems Interconnesction) je vytvořen organizací ISO (International Organization of Standardization) v roce 1978. OSI model je vytvořen pro umožnění komunikaci mezi dvěma Operačníma systémy. S tímto modelem se pochopení síťových struktur zlehčilo. Má vrstvovou strukturu, každá vrstva vykonává jiné úkoly. Je hierarchicky uspořádaná tak, aby jedna vrstva navazovala na další. Vrstev je celkem 7 a hierarchie je od spodu nahoru.



(zdroj: sideplayer.cz)

1. **Fyzická vrstva** - V této první vrstvě jsou data překládána na bity (bit: základní datová jednotka v počítači) přes komunikační kanály. Tato vrstva se stará pouze o přesun dat, takže se nestará o to jaký typ dat přenáší.
2. **Linková vrstva** - V této druhé vrstvě OSI modelu se zpracovávají data z Fyzické vrstvy a připravují se na poslání do další vrstvy. Těmto operacím se říká fyzické směrování.
3. **Síťová vrstva** - Třetí vrstva (síťová) je zodpovědná za doručení dat do cílové IP adresy (IP adresa: ID každého zařízení v síti. Připojování zařízení je vykonáno právě pomocí IP adres.) Této operaci se říká logické směrování.
4. **Transportní vrstva** - Čtvrtá vrstva je zodpovědná za bezpečný převod dat. Vrstva provádí několik kontrol errorů, aby data mohly být úspěšně zobrazeny.

5. **Relační vrstva** - Pátá vrstva je zodpovědná za provedení nezbytných operací, aby prezentační vrstva mohla fungovat. Nejdůležitější operací je shromažďování a organizace dat.
6. **Prezentační vrstva** - Šestá vrstva zobrazuje data. Dva komunikační uzly musí použít běžnou řeč pro zobrazení dat.
7. **Aplikační vrstva** - Sedmá vrstva je poslední vrstva OSI modelu. Tato vrstva je nejblíž k uživatelům - zobrazuje data.

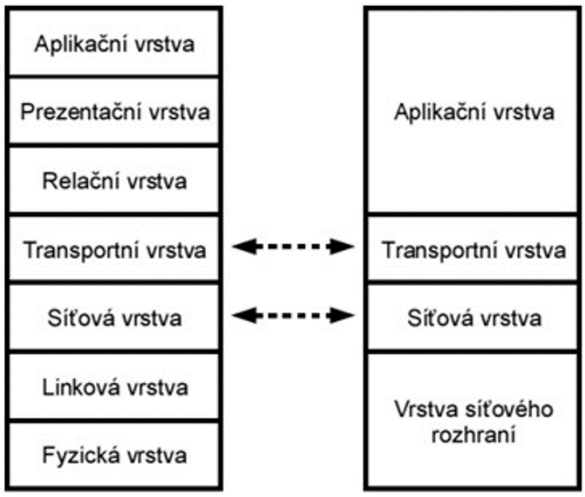
- ## TCP/IP Model

    - TCP/IP model byl navržen organizací Department of Defense (DoD) v roce 1960. Když představili tento model, nebyli tu žádné standardy v počítačových sítích. Tento model ukazoval jak by měla vypadat komunikace zařízení na internetu. Má vrstvenou strukturu jako ISO/OSI a má vrstvy:

(Zdroj: ijs2.8u.cz)

1. **Vrstva síťového rozhraní** - je to první vrstva TCP/IP modelu. skládá se z technologiích, které jsou v OSI/ISO modelu na první a druhé vrstvě. Tato vrstva zahrnuje fyzický přístup a hardwarové kontroly.
2. **Síťová vrstva** - Je to druhá vrstva TCP/IP a zahrnuje podobné funkce jako třetí vrstva v OSI/ISO modelu. V této vrstvě se provádí síťová komunikace díky logickému adresování.
3. **Transportní vrstva** - Je třetí vrstva v TCP/IP modelu a odpovídá čtvrté vrstvě OSI/ISO modelu. Na této vrstvě se přenášejí data a stará se o spolehlivost přenosu. Pokud jsou data dobře, nebo špatně odeslána se zjišťuje na této vrstvě.
4. **Aplikační vrstva** - Je čtvrtá vrstva TCP/IP modelu a odpovídá páté, šesté a sedmé vrstvě OSI/ISO modelu. Kontrola aplikací a operace v nich jsou v této vrstvě.

OSI/ISO vs TCP/IP



(Zdroj: ijs2.8u.cz)

- **Síťová zařízení**

  - V počítačové síti jsou zařízení. Každé z nich je zodpovědné pro různé úkoly. Bez těchto komponentů v síti by síť nemohla fungovat. Pokud víme jaké úkoly a jaké kapacity mají jaké zařízení, můžeme jimi řešit problémy v síti. Tady je řešením rychlá akce.

Switch

  - Switch neboli přepínač je síťové zařízení pracující na druhé vrstvě OSI modelu. Některé switche s více nastavitelnými prvky pracují na třetí vrstvě OSI modelu. Switch je propojovací zařízení a používá se k propojení dvou uzlů v síti. Velikost je dána počtem portů (rozhraní pro připojení zařízení pomocí konektoru). Switch posílá data ze zdrojového portu přímo do cílového čímž se nezpomaluje výkonnost sítě.

(Zdroj: tp-link.com)

Router - Směrovač

  - Router je jeden ze síťových zařízení pracující na třetí vrstvě OSI modelu. Jeho úkolem je směrování paketů k cílovým IP adresám s pokročilými prvky, které obsahují nějaký operační systém. Používá se mezi dvěmi počítačovými sítěmi. Například se často používá v LAN-MAN propojení a WAN-LAN propojení. Nejběžnější použití routeru je směrování paketů, a díky tomuto zařízení jsou segmenty sítě od sebe rozděleny.

(Zdroj: indiamart.com)

Hub - rozbočovač

- Hub je síťové zařízení pracující na fyzické vrstvě OSI modelu. Je to velmi jednoduché zařízení, které připojuje další zařízení do sítě.

(Zdroj: eu.dlink.com)

Repeater - Opakovač

- Repeater pracuje na fyzické vrstvě OSI modelu. Má dva vstupní porty, jeden z nich mění přicházející signál na signál výstupní a pošle ho na cílovou adresu. Posiluje slabší signál a tím prodlužuje vzdálenost přenosu dat. Je podobný hubu ale nemá tolik portů.

(Zdroj: hardwaresiti.webnode.cz)

Bridge - most

- Bridge pracuje na linkové vrstvě OSI modelu. Jeho úkolem je směrování paketů tím, že propojí dvě koncové zařízení v síti. Má podobný úkol jako router ale je to velmi jednoduché zařízení s méně porty. Může být také použit v LAN-LAN propojení.

(Zdroj: landisgyr.cz)

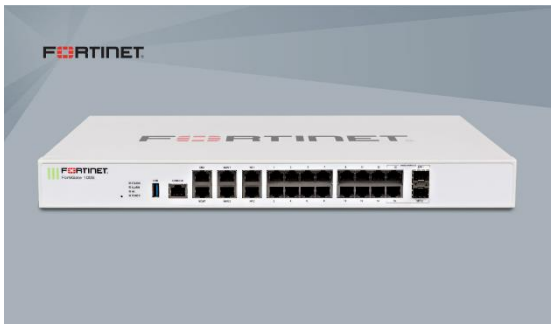
Modem - Modulátor

- Modem je menší síťové zařízení ve kterém jsou nějaké zařízení jako switche spojené do jednoho. Obsahuje malý operační systém. Používá se často v domácích sítích pro připojení internetových prostředků.

(Zdroj: medium.com)

Firewall

- Firewall - česky ochranná zeď před viry, je síťové zařízení pracující na transportní vrstvě OSI modelu. Firewall je nezbytný síťový hardware, který se nachází mezi internetem,. Je brán jako pojistka sítě se sítí opravdovou. Firewall je v sítí důležitý, protože je to pojistka bezpečnosti, která blokuje, nebo povoluje průchod dat díky pravidlům. Je velké množství typů firewallu ale nejvíce používaná je hardwarová podoba firewallu. Vlastnit pouze firewall nestačí pro ochranu sítě proti vnějším hrozbám. Musí být dobře nakonfigurován, jinak může zhoršit výkon a způsobit bezpečnostní slabiny.



(Zdroj: ccivoice.com)

Gateway

- Gateway je síťové zařízení, které může pracovat na každé vrstvě OSI modelu. Jeho úkolem je provádět vnitřní síťovou komunikaci mezi dvěmi sítěmi - propojuje dvě sítě aby spolu mohly zařízení komunikovat. Má podobné vlastnosti jako router, ale router narozdíl od gatewaye nemůže pracovat na každé vrstvě OSI modelu. Gateway je pomyslná brána pro uzly z jiných sítí. Díky tomuto zařízení, uzly v jedné síti mohou komunikovat s uzly v jiné síti.

(Zdroj: telehopbusinessservices.com)

• IP Adresování

- Při vytváření TCP/IP sítí musí být součástí každého zařízení IP adresa. Tento úkol se nazývá IP Adresování.
- IP adresa je ID každého zařízení v síti. Připojování zařízení je vykonáno právě pomocí IP adres. Rozdělují se na dva typy IPv4 a IP6. příklady obou typů:

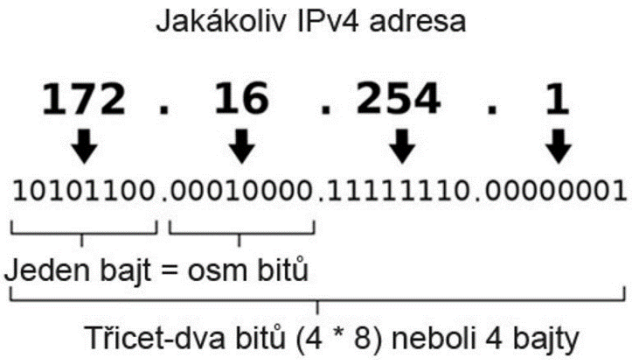
IPv4: 192.168.10.20

IPv6: 2001:0db8:85a3:0000:0000:8a2e0370:7334

Struktura IP Adres

IPv4:

- IP adresa se skládá ze 4 bajtů (32 bitů) (bity = nuly a jedničky označující například síť ve které je zařízení, jeden bajt = 8 bitů). Tečka je umístěna mezi každým bajtem a představuje hodnotu v desítkové soustavě (nejvyšší možné číslo je 255).



(Zdroj: swmag.cz)

IPv6:

- Ke dnešnímu datumu, počet zařízení připojených k internetu je velmi vysoký. Za předpokladu, že by mělo každé zařízení na světě svojí IP adresu, IPv4 adres by nebylo dost. Pro tento případ se vytvořila technologie NAT a IPv6. Srovnání IPv4 s IPv6:

.	IPv4	IPv6
Vynalezeno:	1981	1999
Velikost adres	32 – bitové číslo	128 – bitové číslo
Formát adres:	192.148.21.25.0	3FFE:F200:0234:AB56:5656:DE56:15987:ABCD
Počet adres:	2^{32}	2^{128}

Privátní IP adresy

- Některé z IP adres jsou rezervované na speciální použití. Tyto rezervované IP adresy se používají v privátních sítích. Privátní sítě jsou sítě, které nejsou přímo připojené na internet ale používají k připojení speciální zařízení. Například domácí síť. V domácích sítích se modem stará o připojení k internetu a přenášení dat. Toto je rozsah privátních IP adres:

Od: 10.0.0.0 do 10.255.255.255

Od: 172.16.0.0 do 172.31.255.255

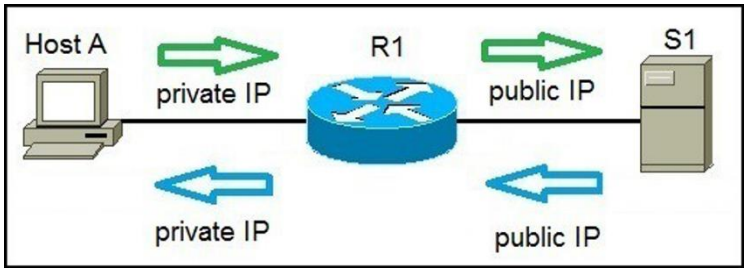
Od: 192.168.0.0 do 192.168.255.255

localhost

- Lokální host (localhost) je rozsah IP adres ukazující přesný počet zařízení v celé síti. Používá se pro spuštění služeb lokálně přes zařízení (není potřeba jiné zařízení atd.) Většinou je localhost pod IP adresou “127.0.0.1”. Jakákoliv adresa v rozsahu 127.0.0.1 - 127.255.255.255 může použít tuto službu.

NAT

- Netwrok Address Translation (NAT) je metoda, která převádí privátní IP adresy na veřejné. Privátní adresy nejsou ve směrovací tabulce routeru, takže nemohou být přímo připojeny na internet. Díky NATu limitované IPv4 adresy jsou využívány vícekrát najednou. To znamená že více privátních adres v síti může používat jednu veřejnou IP adresu k připjení k internetu
- Příklad NATu



(Zdroj: study-ccna.com)

- Pokud zařízení s adresou 10.6.1.2 půjde na internet musí nejdříve přesměrovat pakety do gatewaye, který je pak vyšle na internet. Při doručení odpovědi gateway se musí podívat na cílovou adresu v paketu. Po tom co se podívá, zjistí že tato adresa jde z internetu jako veřejná IP adresa, takže se musí podívat do NAT tabulky, kde má napsané všechny IP adresy a k nim přiřazené zařízení a podle ní, pak veřejnou IP adresu přepíše na veřejnou a pošle odpovídajícímu zařízení.

- **VLAN**

  - VLAN (Virtual Local Area Network) nebo virtuální lokální síť znamená, že uvnitř LAN je vytvořena další virtuální síť. Funguje na principu značkování dat, které se po síti posílají. Data se označí tak aby bylo jasné, že se jedná o virtuální síť. Důvody proč vznikl VLAN jsou ty, že lidé chtěli seskupit určité uživatele do jedné skupiny která bude spolu komunikovat a bude mít jednodušší přístup k souborům a informacím a to, že se ethernetové (ethernet = kabelový internet) technologie neposouvali vpřed.

- **VPN**

  - VPN (Virtuální privátní síť) je jednoduchá aplikace, která má posílit vaši online bezpečnost a soukromý. VPN posílá záznamy o aktivitách přes jeden ze svých privátních serverů a zároveň je šifruje. Tím dochází k maskování dat, podle kterých lze zjistit například vaší polohu, historii atd. Neslouží ovšem jen k ochraně soukromí, ale také například pro sledování obsahu blokovaného na základě polohy. Pokud tedy posíláte data přes americký server, máte přístup k aplikacím a službám které třeba nejsou v česku dostupné.

(Zdroj: blog.avast.com)

- **MAC Adresa**

  - MAC (Media Access Control) adresa je jedinečný identifikátor zařízení, které používá různé protokoly druhé vrstvy OSI modelu. Přiřazuje se ke každé síťové kartě při její výrobě. Také se můžete setkat s názvem fyzická adresa. Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel např. 0123.4567.89ab. Mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami např. 01:56:84:45:a8:b2. Při převodu na 48 bitové číslo se převede každá šestnáctková dvojce na dvojkové číslo např. 01 = 00000001, 23 = 00100011 atd.

- **Síťové Protokoly**

  IP Protokol

- Jde o přenosový protokol, zajišťuje směrování a přenos IP datagramů (virtuální paket) v síti. Je univerzální nevyužívá specifika fyzických přenosových technologiích, je zaměřen na jednoduchost, efektivnost a rychlost. Problém je ve spolehlivosti - negarantuje doručení datagramu, nepoužívá potvrzení, negarantuje nepoškození dat a smí datagram zahodit když: překročil svou životnost (ochrana proti zacyklení v síti pokud nenajde cílový port), hrozí zahlcení sítě. Velikost IP protokolu je proměnná, max je 65535 bajtů.

ICMP Protokol

- Internet Control Message Protocol jinak ICMP protokol je pomocný protokol používající se k diagnostice a monitorování sítě. Používá se především k přenosu zpráv o chybách a dalších výjimečných situací. Protokol ICMP definuje asi 12 typů zpráv. Každá zpráva je vložena do paketu IP. nejčastěji používané zprávy:

Typ zprávy	Zpráva	Popis
0	Echo Reply	Odpověď na žádost o odpověď
3	Destination Unreachable	Cíl nedosažitelný
4	Source Squench	Datagram byl zničen
8	Echo Request	Vyžádejte si odpověď („zeptejte se hostitele, zda je naživu“)
11	Time Exceeded	Hodnota pole Lifetime klesla na nulu
12	Parameter Problem	Nesprávná záhlaví IP
13	Timestamp Request	Stejné jako o žádost o odpověď, ale s časovým razítkem
14	Timestamp Reply	Stejné jako žádost o odpověď, ale s časovým razítkem

(Zdroj: vovcr.cz)

ARP Protokol

- Address Resolution Protocol - ARP protokol je síťový protokol, který se používá pro zjištění MAC adres za využití IP adres. Používá se pouze výhradně. Jeho velkou slabinou je to, že může být zneužit pomocí ARP spoofingu (tváří se jako jiný počítač a posílá si zprávy určené někomu jinému), nebo DDoS útokům (Přehlcení a následný výpadek sítě)

Routování (Směrování)

- Routování je posílání dat do jiných sítí. Jinými slovy hledání cesty. Router - směrovač je hlavní zařízení pro tento úkol. Řekněme, že jste v česku a pošlete zprávu někomu kdo je v Anglii. Paket s daty, které posíláte z vašeho routeru doručí na další router, který vede k cílové adrese v Anglii. Druhý router přijme paket a podívá se, kam musí být doručen a opět pošle data na další router, který vede k cílové adrese. Takhle to pokračuje dokud nedojde až na cílovou adresu. Někdy se stane, že paket tzv. zabloudí, to znamená, že nějaký router udělal chybu a poslal ho na špatnou stranu. Aby paket nebloudil do nekonečna má vlastnost TTL (Time To Live), která se s počtem navštívených routerů o jedno číslo zmenší. Jakmile dojde číslo na nulu dřív než router do cíle, paket se zahazuje. Tento celý proces se vykonává na Transportní vrstvě ISO/OSI protokolu i TCP/IP protokolu.

Základy Operačního systému Windows

- **Verze Windows**
  - Windows je název operačního systému, který má hodně verzí a je vytvořen společností Microsoft. Poprvé byl uveden v roce 1985. S novou verzí Windows přichází i zlepšení systému.

Windows verze:

Name	Release Date	Name	Release Date
Windows 1.01	1985-11-20	Windows XP	2001-10-25
Windows 3.0	1990-05-22	Windows Vista	2007-01-30
Windows NT 3.1	1993-07-27	Windows 7	2009-10-22
Windows 95	1995-08-24	Windows 8	2012-10-26
Windows 98	1998-06-25	Windows 10	2015-07-29
Windows 2000	2000-02-17	Windows 11	2021-10-05

(Zdroj: wikipedia)

Použití Windows

- Tento operační systém je velmi používaný. Používá se téměř v jakémkoliv zaměření, hlavně v IT. Microsoft dal velmi velký důraz na Uživatelské grafické prostředí (GUI) aby mohl dát uživatelům tu největší flexibilitu. První věc co vás napadne u Windows je ta, že je velmi jednoduchý na používání a na orientování se v něm pro kohokoliv.

- **Systémové soubory**
  - Systémové soubory jsou strukturovaná data, která obsahují digitální úložiště, jejichž prvky jsou soubory. Operační systém nemůže fungovat s diskem bez systémových souborů. Tyto soubory mají různé typy a data struktury. Některé z typů Systémových souborů ve Windows:

1. FAT - Tabulka vytvořena v roce 1977 obsahující informace o obsazení disku v systémových souborech. FAT systém není v základu pro Microsoft Windows. V dnešní době je použit pouze v například USB, nebo flash disk (fleškách).

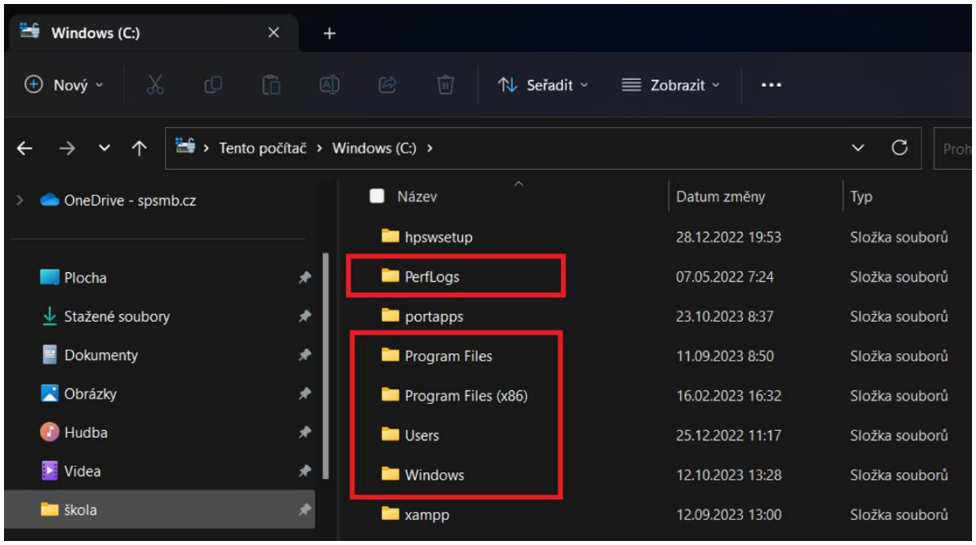
2. exFAT - Systémový soubor, který Microsoft představil v roce 2006 pro optimalizaci USB a flash disků.

3. **NTFS** - Systémové soubory tohoto typu byly používány ve starších verzí Windows a do dnes některé jsou používány. Byl nahrazen FAT systémem, který je více přizpůsobený pro novější technologie. NTFS systém podporuje i například operační systém Linux.

- **Struktura složek**
  - V každém operačním systému jsou souborové struktury i složkové struktury,. Windows verze mají všechny podobné struktury složek. ve Windows je jako root složka (root: tzv. superuživatel, má oprávnění měnit soubory, které běžný uživatel měnit nemůže) většinou nějaký disk, u většiny je to disk “C:/”. Složky se oddělují lomítkem.

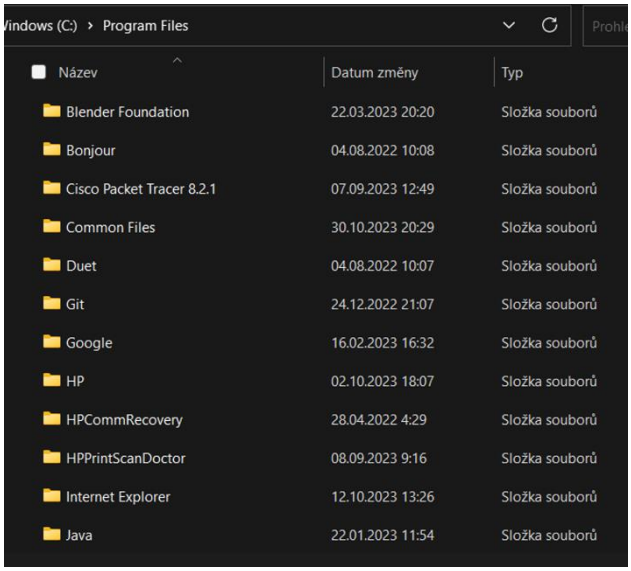
Složky ve Windows

- Systémové složky jsou vytvořeny při instalaci Windows a jsou to tyto:

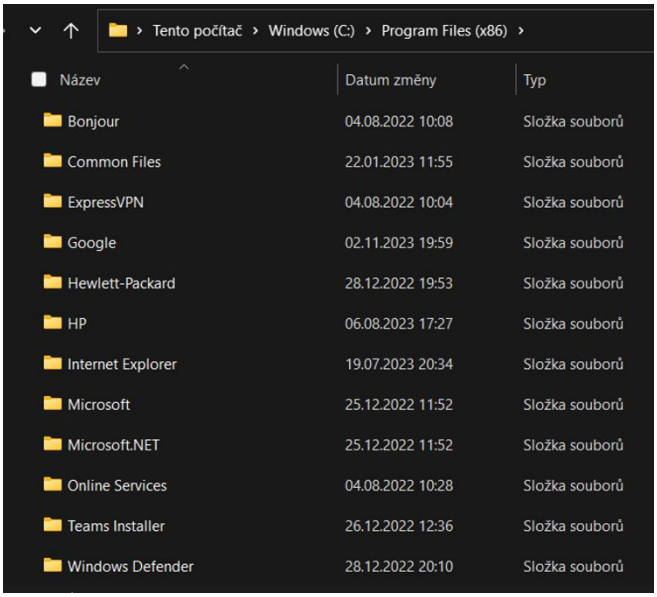


1. PerfLogs - Je to složka vytvořená pro Windowsové výkonnostní záznamy (Windows logs). Pokud do ní vejdete, zjistíte, že je prázdná. To je proto, že dělání těchto záznamů je běžně vypnutý.

2. Program Files (programové soubory) - V této složce se nachází všechny nainstalované programy, které jsou stejně bitové jako operační systém (buď 32-bitů nebo 64-bitů)

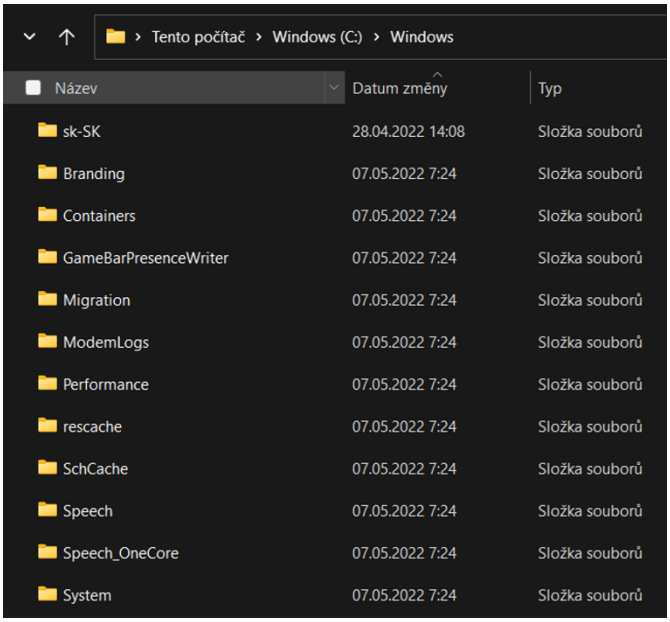


3. Program Files (x86) - Tato složka je pouze na WIndows s 64-bitovou verzí. Jsou tu uložené 32-bitové programy.



4. **Users (Uživatelé)** - Tato složka obsahuje soukromé složky každého z uživatelů co je, nebo byl přihlášený na zařízení aspoň jednou. Složky jako plocha, stažené soubory, obrázky atd. jsou uloženy v těchto složkách.

5. **Windows** - Jedna z nejdůležitějších složek. V této složce je uložen a nainstalován celý operační systém Windows. Má to svojí strukturu a obsahuje hodně systémových informací v určitém pořadí. Pro příklad, databáze, kde se ukládají hesla uživatelů jsou v této složce.

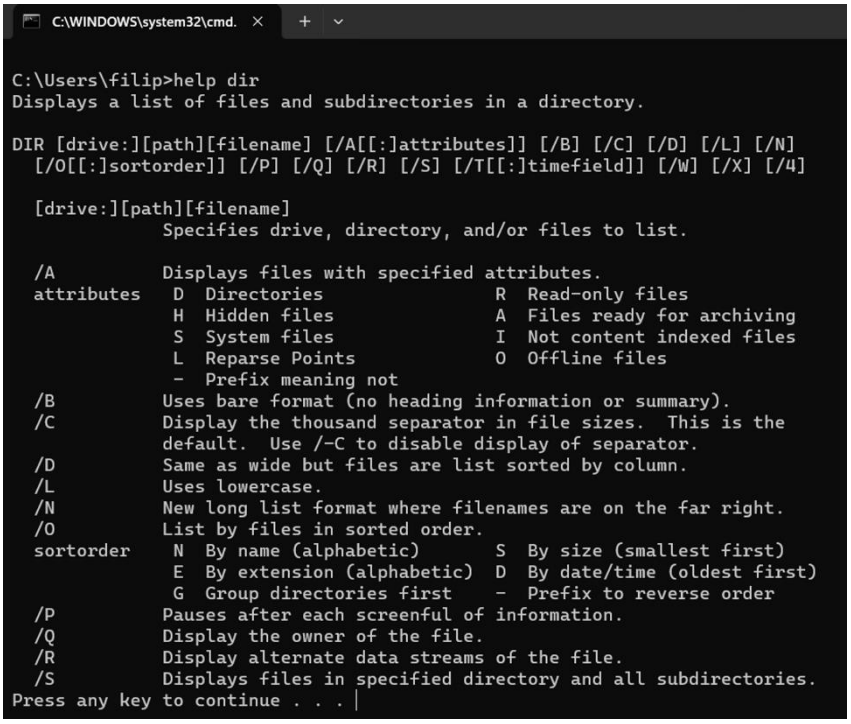


- **Příkazový řádek Windows**
  - příkazový řádek je program, který přijímá příkazy přes klávesnici a mění je v nějakou operaci

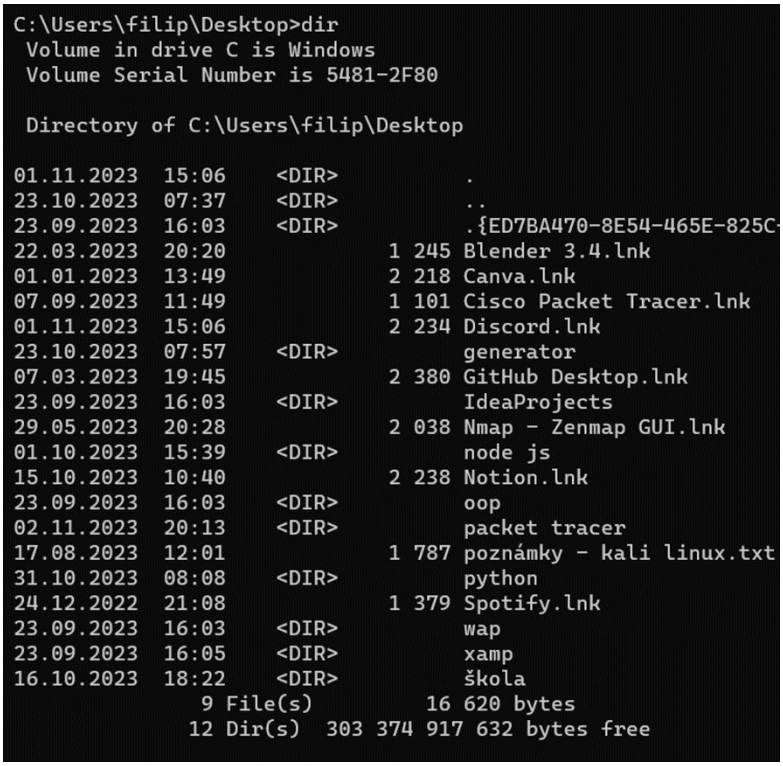
Běžné příkazy

- Ve Windows je hodně operací, které jdou vykonat přes příkazový řádek. Zde máme ty nejzákladnější:

1. Příkaz "Help" - Příkaz help vám vypíše všechny informace o příkazech použitých po příkazu help. Můžeme vidět parametry příkazů u kterých potřebujeme zjistit informace. Například tady můžeme vidět co se stane s příkazem "dir" pokud k němu napíšeme help.

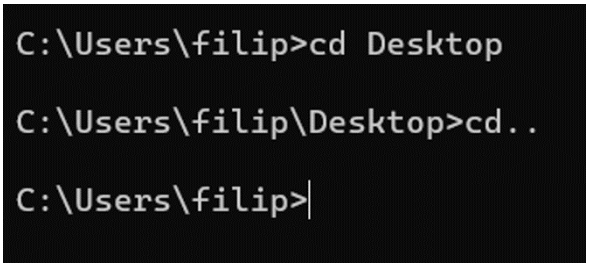


2. příkaz “dir” - Je to příkaz, který listuje v souborech a v podsložkách v té jedné složce. Názorná ukázka co se nám vypíše pokud půjdeme do “C:/Users/filip/Desktop”:



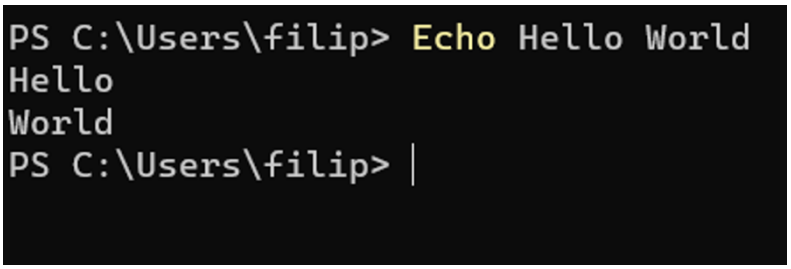
- Obrázek ukazuje programy a složky, existující na Ploše.

3. **Příkaz “Cd”** - S tímto příkazem se pohybujete mezi složkami. napíšeme příkaz cd a složku kam chceme jít:



- pro vrácení o jednu složku zpět použijeme také příkaz cd, ale přidáme dvě tečky jako vidíte na obrázku.

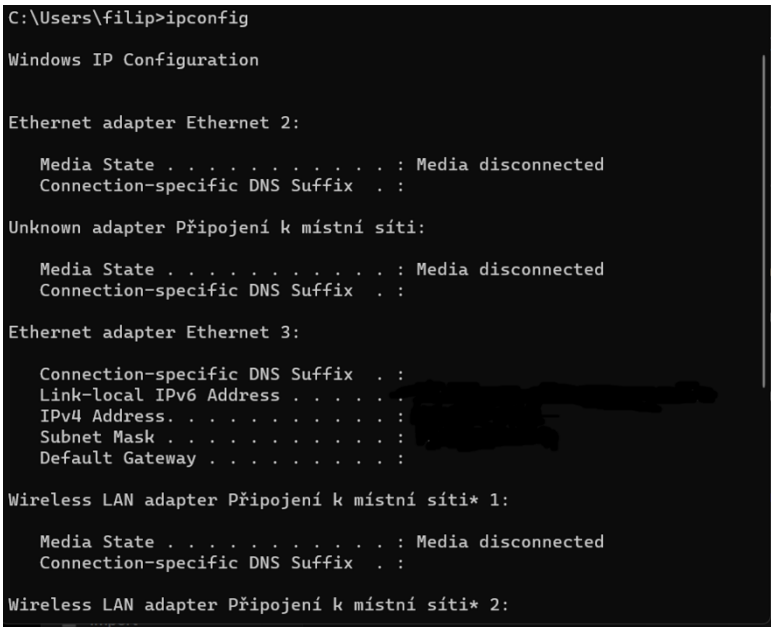
4. příkaz "Echo" - Používá se pro vypsání čehokoliv na obrazovku. Například zkusíme vypsat "Hello World":



5. příkaz "hostname" - tento příkaz vám ukáže pod jakým uživatelem jste momentálně přihlášeni:

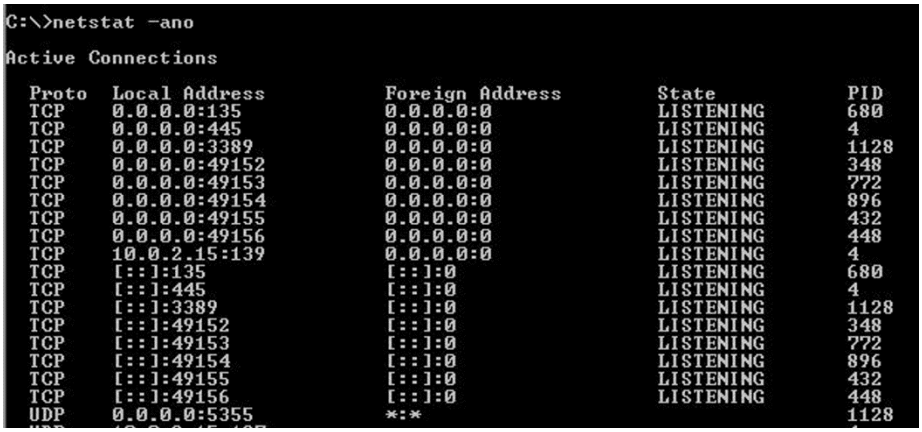
příkazy pro sítě

1. **příkaz "ipconfig"** - Ukazuje informace o síťovému rozhraní např:



(citlivé informace z bezpečnostních důvodů zamazány)

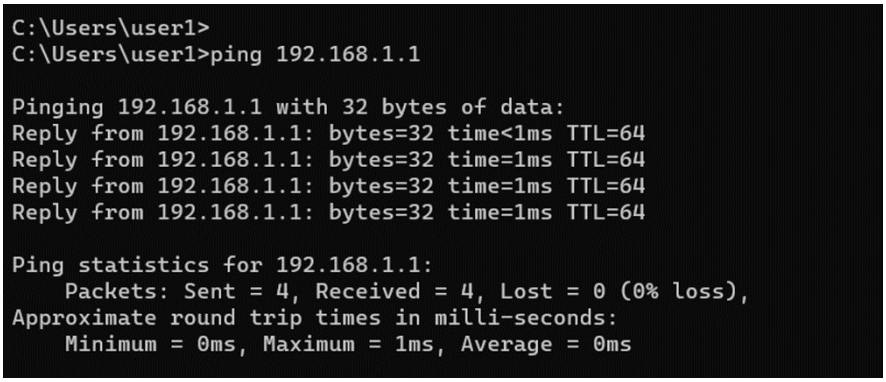
2. příkaz "netstat " - Pro vypsání všech internetových připojení a jejich statusech:



(Zdroj: ionos.com)

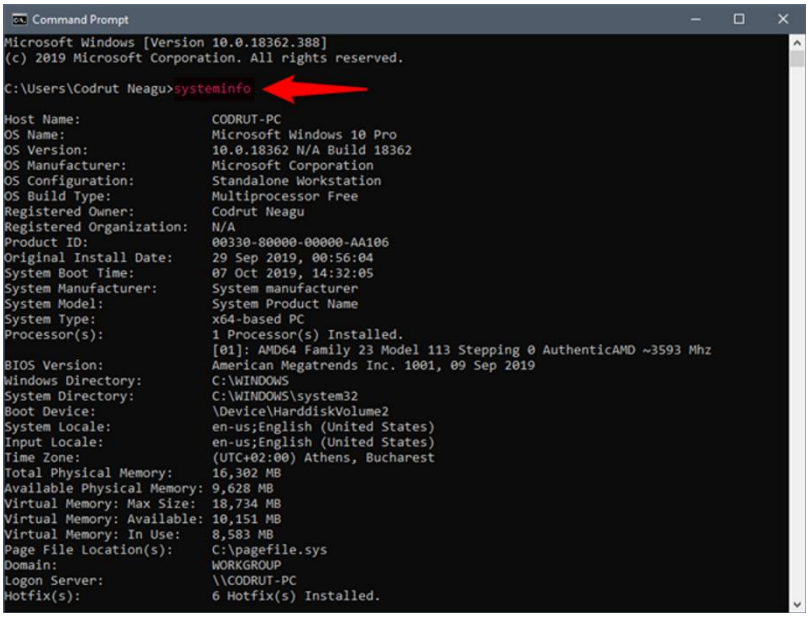
- vysvětlení parametrů použitých s netstat:
- “a” - zobrazuje všechny připojení a porty na kterých běží
- “n” - zobrazuje adresy a číslo portů v číslicích
- “o” - zobrazuje ID procesů spojených s každým připojením

3. **příkaz “ping”** - Je potřebný pro testování spojení dvou zařízení v jedné síti. Je možné tím zjistit jestli je cíl v dosahu, či nikoliv. Síťové pakety jsou posílány a čeká se na odpověď s ping příkazem. Z pohledu kyberbezpečnosti, některé zařízení mohou být nakonfigurovány tak, aby neodpovídaly na ping příkaz proto, aby se nestali obětí případného kyberútoku v síti. Pro příklad jako první do příkazového řádku zadáte příkaz ping s následujícím odkazem co chcete “pingovat” (odkaz na stránku, IP adresu..)



(Zdorj: configserverfirewall.com)

4. příkaz “systeminfo” - Příkaz vypíše detailní informace o systému.



(Zdroj: digitalcitizen.life)

Operace se soubory

1. **Příkaz „Copy“** – Příkaz copy se používá ke kopírování souborů/složek. První parametr v copy je cesta souboru z které kopíruješ, druhý parametr je cílová cesta:)

```
C:\Users\filip>copy /Plocha/Discord /Plocha/škola/Discord
```

2. **Příkaz „mkdir“** – příkaz používaný pro vytvoření složek – make directory (mkdir):

```
C:\Users\filip\Desktop> mkdir slozka1
```

3. **Příkaz „Move“** – Tento příkaz se používá pro přesunutí souborů do jiných složek. Např. přesuneme soubor soubor1.txt do složky slozka1:

```
C:\Users\filip>move soubor1.txt slozka1/
```

4. **Příkaz „rmdir“** – Tento příkaz maže složky – zkráceně remove directory:

```
C:\Users\filip>rmdir slozka1
```

Pokud ve složce co chceme smazat jsou další podsložky, nebo soubory musíme za příkaz rmdir připsat parametr /S – který maže vše co je ve složce.

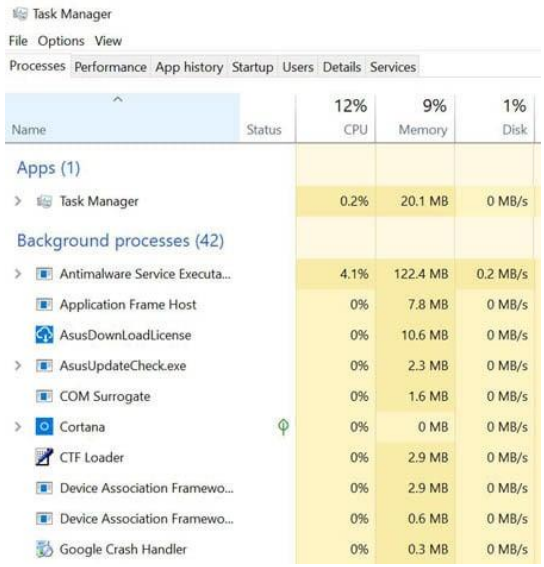
Příkazy pro uživatele a skupiny

1. **Příkaz „whoami“** – pokud do příkazového řádku napíšete tento příkaz, vypíše se vám pod jakým uživatelem jste právě přihlášeni:

```
C:\Users\filip>whoami
honza\filip
```

Task Manager

- Aplikace, která vám ukazuje všechny procesy co probíhají na ploše i v pozadí. Můžete tak sledovat co se vám kde děje a případně vypnout zbytečně běžící programy



(Zdroj: pcmag.com)

Windows Firewall

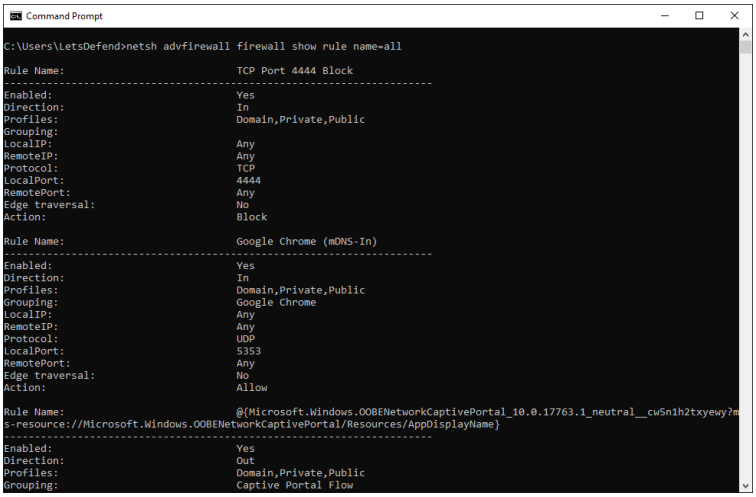
- Firewall je bezpečnostní nástroj, který povoluje nebo zakazuje IP paketům projít v síti k hostům, díky určitým pravidlům. Tyto pravidla jednoduše blokují podezřelý připojení. Naopak připojení, které tyto pravidla vyhodnotí jako bezpečné tak je přidají do povolených připojení. Windows Firewall je jedno z nejzákladnějších metod, které předchází hackerům aby se dostali do systému. Firewall poskytuje efektivní obranu proti hrozbám, které můžou přijít z jiných sítí. Protože ale hackeři ví o Firewallu a o jeho schopnosti blokovat tyto připojení, tak se soustředí na poškození, shození firewallu, nebo se snaží vytvořit pravidlo, které obejde ostatní pravidla a pustí je do systému. Po tom co se dostanou dovnitř tak pokračují v útoku tím, že píšou příkazy na cíl aby dostali kontrolu nad celým serverem. Aby se tomuto předcházelo tak kyberbezpečnostní analytici by měli monitorovat firewall podmínky a sledovat, pokud se objeví nová podmínka, která by tam být neměla. Zároveň by měli dávat pozor aby firewall nebyl poškozený, nebo shozený.

Inbound a Outbound pravidla (přicházející a ocházející)

- Přicházející pakety mají filtrovaná pravidla, která přecházejí ze sítě k lokálnímu zařízení řídící se těmito pravidly. Pro odcházející pakety jsou pravidla, která se posílají z lokálního počítače do sítě a měli by být filtrovány podle filtrovacích pravidel.

Správa Firewall pravidel s příkazovým řádkem

- Příkaz „netsh“ se používá pro vypsání pravidel. Sám nefunguje, ale s určitými parametry ano.

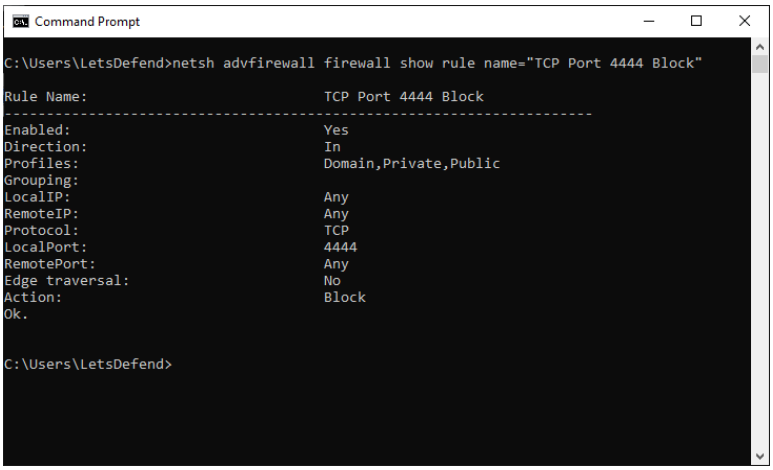


(Zdroj: app.letsdefend.io)

- Na obrázku můžeme vidět detaily všech Windows Firewall pravidel.

Zobrazování informací o pravidlu Firewallu v příkazovém řádku

- Pokud chceme vypsat jen nějaké pravidlo abychom viděli vše o něm použijeme stejný příkaz jako pro všechny pravidla, ale místo všech napíšete pouze jméno pravidla:



(Zdroj: app.letsdefend.io)

Linux

Linux je jeden z nejběžněji používaných počítačových operačních systémů hned za Windows. Je to Projekt, který vytvořila společnost GNU. Linux je od jména zakladatele Linuse Torvaldse v roce 1991

Využití linuxu

- Linux může být použit v hodně oblastech pro hodně věcí. Pokud chceš používat Linux, stáhneš si ho a používáš ho zdarma bez licencí. Linux je velmi flexibilní a kód linuxu vám dovoluje pracovat komfortně. Má potenciál být rozšířeně používán. Má schopnost pracovat s procesorem tak, že přidává nebo ubírá výkon podle potřeby. Nejčastěji se používá pro serverové systémy, osobní počítače, chytré zařízení a mobilní zařízení.

Běžné Linux distribuce

- Existuje hodně verzí linuxu, které sedí různým uživatelům pro různé účely. Každá z těchto verzí se říká distribuce. Toto jsou ty nejpoužívanější:
  - Ubuntu

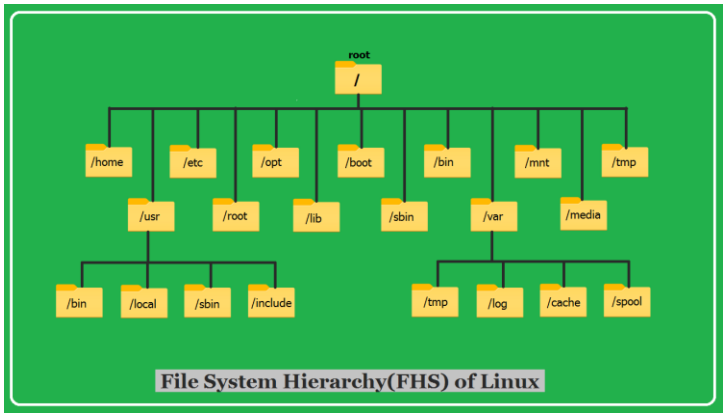
- CentOS
- Fedora
- Debian
- Red Hat enterprise Linux
- Linux Mint
- Open SUSE
- Manjaro

Pro vidění většin distribucí můžete navštívit stránku distrowatch.com.

Hierarchie systémových souborů

„/“ – Root složka

Tato složka je nejvýše postavená z celé hierarchie v linuxu. Každá složka, která je v systému je pod touto složkou. Například složka /bin je složka s názvem „bin“ a je podsložkou root „/“



(Zdroj: tecadmin.net)

Složka /bin – V této složce jsou uloženy téměř všechny příkazy, které můžete spustit a které jsou nainstalované jako součást systému

Složka /boot – Jsou v ní soubory, které jsou potřeba když se zapíná systém aby se vše zapnulo správně (nabootvalo)

Složka /etc – V této složce jsou konfigurační soubory systému. Je to jedna z nejdůležitějších složek v Linuxu z pohledu bezpečnosti. Například i šifrování hesel je v této složce.

Složka /home – Uživatelé v této složce mají uložené osobní soubory. Stažené soubory, dokumenty, atd.

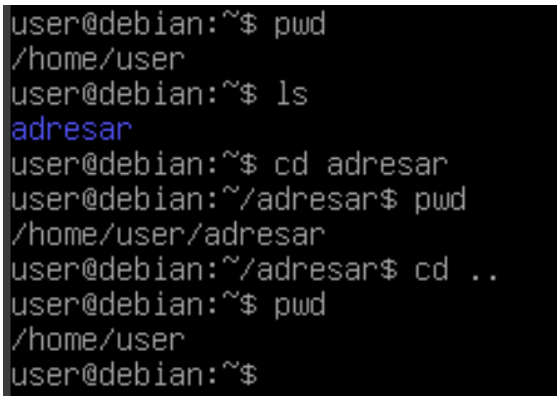
Základní příkazy v linuxu

Příkaz „pwd“ - pwd (Print working directory) vám ukáže v jaké složce, nebo v jaké cestě se zrovna nacházíte.

Příkaz „ls“ – tento příkaz vám vypíše podložky, které se v dané složce nachází. V našem případě jediná podsložka je adresář. Můžete přidat parametr -a pro vypsání

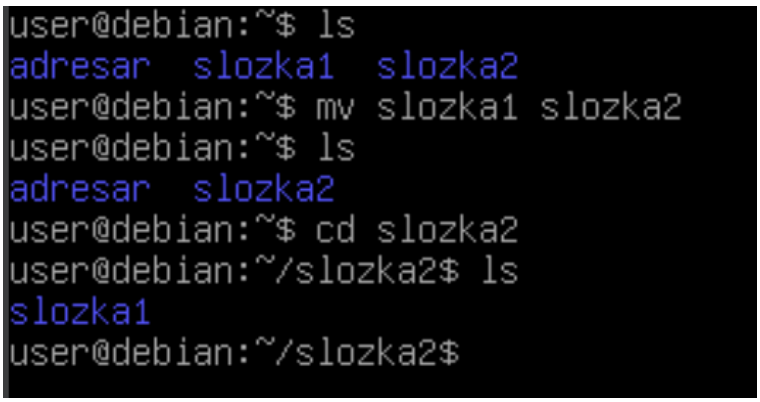
všech i skrytých podsložek, nebo parametr -l pro vypsání oprávnění pro dané podsložky.

Příkaz „cd“ – Díky tomuto příkazu se můžete pohybovat mezi složkami. V našem případě jsem vešel do složky adresar a následně se vrátil o jednu zpět pomocí dvou teček za cd.



Příkaz „mkdir“ – Tento příkaz vytváří složku. Za tento příkaz napište jméno složky, kterou chcete vytvořit a to je vše.

Příkaz „mv“ – tento příkaz přesouvá složky. Z obrázku můžeme vidět, že první se píše složka, kterou chceme přesunout a jako druhou píšeme složku do které ji chceme přesunout. V našem případě slozka1 přesouváme do slozka2



Příkaz „cp“ – cp (copy) je příkaz pomocí kterého kopírujeme složky. První parametr, který píšeme je cesta složky, která chce být kopírována, druhý parametr je cesta složky, do které chce být vložena.

Příkaz „rm“ – tento příkaz odstraňuje složky. Jediný parametr, který napíšete za příkaz je název složky, kterou chcete smazat. Pokud chcete smazat i to co je ve složce přidejte za příkaz parametr -r.

Příkaz „cat“ – Tento příkaz vám vypíše obsah souboru. Za tento příkaz stačí napsat název souboru.

Analyzování Malwaru

- V praxi se budeme často shledávat s různými typy podezřelých souborů. Podezřelé soubory, jsou soubory, které mohou obsahovat nějaký typ malwaru, který se snaží nějakým způsobem poškodit počítač, nebo z něj něco dostat.

Definice malwaru

- Slovo malware je od slova MALicious softWARE (škodlivý software). Je pojmenovaný po softwaru, který napadá bezpečnost systémů za nějakým účelem.
- Dnes hackeři a kyberútočníci používají malware, aby dosáhli svého cíle jako například poničení systému, kradení osobních informací atd.
- Vzhledem k tomu, že tu nejsou žádné podmínky pro vytváření malwaru, můžete se setkat s malwarema napsanýma v téměř jakémkoliv programovacím jazyce. Nepotřebujete znát všechny programovací jazyky, ale je to výhodou znát aspoň nějaké.
- S každým dnem hackeři zdokonalují a vytvářejí komplexnější malwary. Útočníci používají různé metody k tomu, aby jejich malware byl hůře analyzovatelný.

Typy malwaru

- Malware má více typů. Rozdělují so podle toho co mají za úkol, nebo jaká je jejich funkce.

Backdoor – Tzv. zadní vrátka. Pokud se vytvoří zadní vrátka v zařízení, kde je nainstalovaný malware, útočník se dostane lehce do systému právě přes zadní vrátka. Pro příklad pokud otevřete nějaký síťový port, který je připojen do shellu(rozhraní pro ovládání zařízení a operačního systému), dáte tím možnost komukoliv vstoupit do vašeho zařízení právě přes tento port.

Adware – Většinou přichází s nainstalovaným softwarem díky kterému se vám na displeji budou stále ukazovat reklamy. Ne všechny adwary jsou škodlivé, některé ale mění defaultní prohlížeč.

Ransomware – Je to typ malwaru, který se objevuje poslední roky. Vyžaduje výkupné po lidech tak, že odšifruje a vyfiltruje všechny soubory a složky v jejich zařízeních.

Virus – Je to jeden z prvních malwaru, který se objevil. Virusy se sami opakují tím, že infikují další soubory v zařízení.

Worm - Vzhledem k tomu, že se tento malware roznáší z infikovaných zařízeních do dalších, tak se mu říká worm (červ). WannaCry, worm malware, který se roznesl po celém světě zapříčinil paniku.

Rootkit - Upraví tvůj operační systém aby vytvořil zadní vrátka které pak může použít jako přístup do tvého zařízení na dálku. Větsina rootkitů berou příležitosti u softwarových slabin aby dostali přístup do souborů které jinak nejsou přístupné (např. oprávnění). rootkity také mohou upravit systém tak, aby bylo velmi těžké je detekovat (např. monitoring tools). Pokud vás napadne rootkit budete muset jít do továrního nastavení a následně celý systém přeinstalovat.

RAT(Remote Acces Trojan) – Typ malwaru, který poskytuje útočníkovi plnou kontrolu nad zařízením.

Banking malware – Typ malwaru, který útočí na bankovní aplikace a krade peníze z obětí.

Keylogger – Typ malwaru, který si ukládá klíče a hesla a posílá tyto informace útočníkovi.

Spyware - Je nadesignovaný tak aby vás stoalkoval, monitoruje vaší onlinové aktivity a ukládá si každou klávesu na kterou zmáčknete a také ukládá téměř každé informace včetně osobních údajů, detaily banky atd. Aby to spyware dokázal mění vaše zabezpečení v nastavení ve vašem zřízení. Většinou není samotný, posílá se s nějakým legitimním softwarem nebo trojskými koni

- Většina malwarů obsahuje více typů v jednom. Například WannaCry malware obsahuje oboje worm i ransomware.

Denial of Service (DoS)

- Denial of service útoky je typ síťového útoku, který je relativně jednoduchý ho udělat i pro začátečníky
- DoS útoky mají na svědomí výpadky nebo záseky sítí

Overwhelming

- když síť pošle hostovi nebo aplikaci tolik dat najednou že to nemůžou zpracovat a buď extrémně zpomalí nebo úplně spadnou

Mlicious packets

- Je to upravený packet, který když někomu přijde tak ho ta síť nezvládne udržet a celá síť spadne
- například když útočník pošle packety, které v sobě mají errory nebo nesprávně formátované packety které nemohou být identifikované aplikací (následný pád nebo zpomalení aplikace)

Distributed DoS

- Distributované DoS útoky (DDoS) jsou podobné DoS útokům ale z více zdrojů např.
- útočník vytvoří síť (botnet) s infikovanými hosty tzv. zombíky kteří jsou kontrolovaný útočníkem
- zombí zařízení budou neustále scanovat a infikovat ostatní hosty vytvářející tím více a více zombíků
- jakmile ready útočník bude ovládat systém tak aby botnet tombíků vykonal DDoS útok

Etické Hackování

- Etické hackování je o tom, že se někdo snaží probourat do vaší infrastruktury organizace a tím zjistit vaše slabiny s vaším vědomím a souhlasem a následně je nahlásí té organizaci se závěrem, kde mají co slabé a co mají naopak dobré. Hackeři se snaží najít nějaké zákony v systému které mohou být změněny, nebo úplně zničeny. Tím sbírají informace a následně vyhodnocují bezpečnostní stav organizace.

- Každý etický hacker provádí různé operace podle toho pro jakou organizaci to dělá. Každý etický hacker by měl znát tyto kroky:

  1. **Hledání povolení –** před začátkem nějaké kontroly se etický hacker musí domluvit a dohodnout s organizací

2. **Stanovení rozsahu vyhodnocování** – musíte stanovit a přesně definovat jakým způsobem a do jaké hloubky budete vyhodnocovat vaší práci. Pak musíte s organizací probrat co budete přesně dělat, jak to budete dělat, a kdy to budete dělat.

3. **Ponechat zjištění soukromé** – Jako etický hacker se snažíte zabezpečit síťový systém, a je třeba podepsat určité smlouvy před začátkem projektu. Je to důležité proto, že se budete snažit zjišťovat slabiny organizace a tyto smlouvy vám budou bránit sdílet to, co jste zjistili s kýmkoliv jiným.

4. **Okamžité nahlašování slabin** – Jakmile etický hacker najde nějakou chybu v systému musí ji okamžitě nahlásit organizaci, aby byla co nejdříve opravena.

5. **Smazání všech stop** – Dobrý hacker je někdo kdo po sobě nenechá žádnou stopu. Po inspekci systému by měli tedy všechny stopy smazat. Budou tím předcházet neautorizovaným hackerům a budou mít bezpečnější systém.

Offenosivní bezpečnost

- Je to proces nabourávání se do zařízení, nalézání chyb a nabývání neautorizovaného přístupu. Pokud chceme vyhrát proti hackerovi, musíme se jako něj chovat, hledat slabiny v systému a opravit je dříve než je njade on.

Defensivní bezpečnost

- Proces u kterého se snažíme chránit síť analyzováním a zabezpečováním potenciálních digitálních chyb. Můžete se setkat zde u infikovaných zařízeních nějakým malwarem, u čeho musíte vědět jak vznikl a jak ho odstranit.

Pentesting

- Penetrační test, neboli pentest je etický testovací pokus pro analyzování bezpečnosti, aby se zjistilo zda jsou data a celý systém dost zabezpečený před útočníky. U pentestů se používají stejné nástroje a techniky, které by používal i neetický hacker. Podle Security magazínu je každý den provedeno zhruba 2200 kyber útoků.
- Pentesting je vždy hodně kontrovezní. Pojmy jako „hacker“ většinou nesou negativní význam. Nápad legálně se dostat do někoho počítače je těžké.
- Předtím než začne pentesting, musí být provedena formální domluva mezi pentesterem a řídícím společnosti. Musí se probrat jaké techniky a nástroje bude používat.
- Během pentestu se budete většinou potkávat se sensitivníma datama v například databázích.

Hackeři jsou rozděleny do skupin podle baarvy klobouků:

- **white hat hackers -** snaží se dostat do sítí, nebo počítačového systému se souhlasem vlastníka a najít nějaké slabiny, chyby v nich a následně je předat správci toho systému nebo sítě, aby tyto chyby opravil
- tyto operace MUSÍ být schváleny předem správcem nebo odpovědným člověkem
- **gray hat hackers** - mohou najít chyby v systému, ale pouze je nahlásí správci pokud chtějí, na druhou stranu mohou tyto informace rozšířit na internet tak, aby jiní hackeři je mohli využít
- **Organized hackers** - skupina nebo organizace kriminálníků, “hacktivistů”, teroristů ale také státem sponzorovanými hackery, většinou jsou velmi dobře spojení a organizovaní a mohou poskytovat kyber útok jako servis pro jiný kriminálníky
- **hacktivists** dělají politické výroky aby vytvořili obavy o chybách, které jsou pro ně důležité

Footprinting v Etickém Hackování

- Footprinting neboli stopování je sbírání co nejvíce informací o daném cíly. Dělá se to proto, aby se našli nějaké slabiny, nebo možnosti jak se dostat do systému a jaké útoky provést.
- Proces také zahrnuje hledání a sbírání dat o hostech a sítích. Tyto informace mohou obsahovat například firewally, IP adresy, operační systémy, VPNky, emailové adresy atd.

Typy Footprintingu:

- **Aktivní footprinting** – V aktivním footprintingu se používají určité nástroje aby se dalo připojit na cílovou síť.
- **Pasivní** footprinting – Na druhou stranu pasivní footprinting používá data o uživatelech, která jsou dostupná na internetu, například skrz webové stránky, sociální sítě atd.

Zdroje k sbírání informací s footprinting technikami

- **Sociální media -** Většina lidí sdílí své detailní informace online, hackeři je mohou zneužít tím, že si vytvoří falešný účet proto, aby se s vámi spojili online a například se tvářili jako vaši online kamarádi a pak z vás dostali citlivé informace.
- **Webová stránka „Whois“ –** Stránka whois.com je využívaná hlavně hackerama, aby zjistili například email id, kde se podle IP adresy nacházíte a tyto data následně použít.
- **NeoTrace –** NeoTrace je program, který je nejvíce použitý pro sbírání informací. Graficky reprezetuje cestu mezi vámi a nějakou stránkou, uzly přes které půjdete vám budou ukazovat informace jako kontaktní informace, IP adresu nebo lokaci.