Základní škola
SLOUP
679 13 Sloup 200 Tel./fax: 516 435 337

KYBERNETICKÁ BEZPEČNOST

Ročníková práce

Školní rok 2021/2022

Autor: Ondřej Sedlák

Konzultant: Mgr. Vladěna Ševčíková

Prohlášení

Prohlašuji, že jsem tuto ročníkovou práci vypracoval samostatně a použil jen uvedené parametry.

V Šošůvce dne 24. 6. 2022

Ondřej Sedlák

Poděkování

Rád bych tímto poděkoval své konzultantce Mgr. Vladěně Ševčíkové za rady, vstřícnost při konzultacích a pomoc při ročníkové práce.

Obsah

1. Úvod

Kybernetická bezpečnost mi přijde v dnešní době dost důležitá, a proto jsem si vybral tohle téma. Rád bych vám teď řekl, čemu se vyhýbat na internetu, dávat pozor na co klikáte, jak se bránit proti virům a jak být všeobecně na internetu v bezpečí.

2. Charakteristika

Kybernetická bezpečnost je obor v informatice.

Především se zabývá bezpečností internetu:

- Ochranou souborů a dat
- Ochranou před neoprávněnou manipulací se zařízeními
- Bezpečnou komunikací a přenos dat (kryptografie)
- Pomoci v zabránění kybernetických útoků

3. Útoky

Útoky můžeme dělit na několik různých typů:

1) • Zranitelnost
2) •Odepření služby
3) •Clickjacking
4) •Phishing
5) •Spoofing

Pokud je na vaše zařízení proveden útok, pravděpodobně jde poznat přes zpomalení PC. Útok také můžeme poznat skrz neznámé nainstalované soubory a spouštění aplikací ve správci.

4. Zranitelnost

Jinak řečeno programátorská chyba, způsobí určitý bezpečnostní problém.

Zranitelnost má dohromady 3 třídy

- **Ohrožení čistě na osobní úrovni**-útočník může poškodit data (krádeže dat, e-mailové adresy…)
- **Zvýšení oprávnění lokálního uživatele**-útočník se může stát správcem
- **Vzdálený přístup do systému**-útočník se může dostat do systému přes síť.

Nejvíce zranitelností bylo registrovaných v operačních systémech a aplikacích:

- Debian Linux
- Google Android
- Ubuntu Linux

Aplikace:

- Mozilla Firefox
- Adobe Acrobat Readers

5. Odepření služby

Též známý jako Denial of service (DoS)
používá převážně na internetové stránky a služby. Cíl tohoto útoku je znefunkčnit a zpřístupnit stránku, uživatel se poté na danou stránku nedokáže připojit.
Útok také může cílit na danou síť či server. Většinou jsou prováděny z více strojů. (DDoS)
Důvod útoku může být odplata, demonstrace, konkurence či jen kybernetický terorismus.
Možný útok na stránku jde poznat přes:

- Zpomalení stránky
- Nedostupnost celé stránky nebo částí stránky

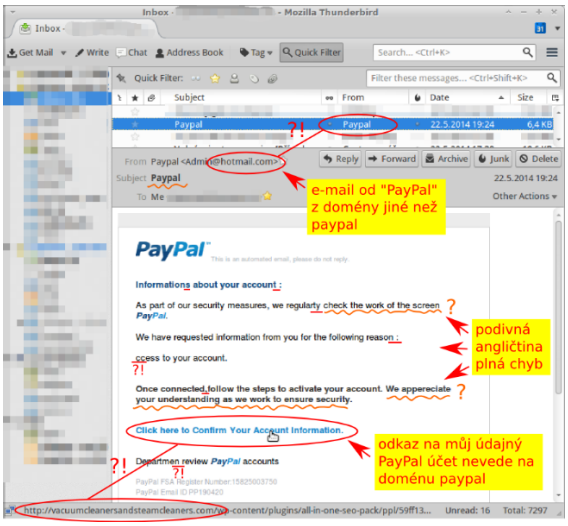
6. Clickjacking

Clickjacking známý jako UI redressing nebo interface redressing, je škodlivá technika, ve které útočník oklame uživatele, aby kliknul na tlačítko nebo odkaz na webovou stránku, zatímco uživatel měl v úmyslu kliknout na vrchní úroveň stránky. Útočník v podstatě “unese” kliknutí určené pro horní stránku a přesměruje jej na nějaké jiné irelevantní stránky, s největší pravděpodobností ve vlastnictví někoho jiného. Uživatel si poté může nevědomky stáhnout do počítače vir.

7. Phishing

Phishing se většinou používá na ukradení bankovních účtu, ale také na odcizení hesel. Obvykle se používá skrz falešné zprávy, maily, smsky

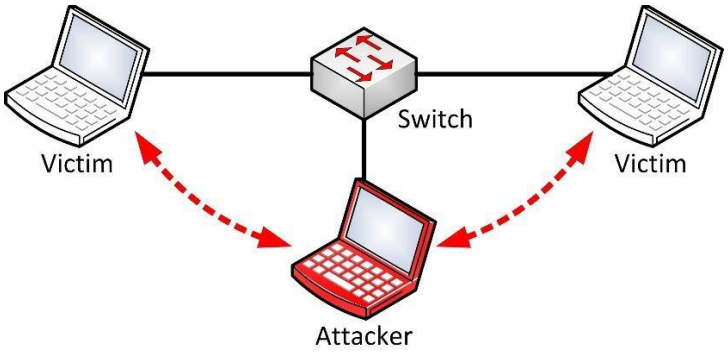
Většinou jsou to odkazy na nepravé známe přihlašovací stránky např: facebook, instagram, twitter. Stránky jsou prakticky nerozeznatelné od oficiálních a je třeba se dívat na doménu, která nemůže být nikdy totožná a tím se tak ochráníte před daným podvodem.



8. Spoofing

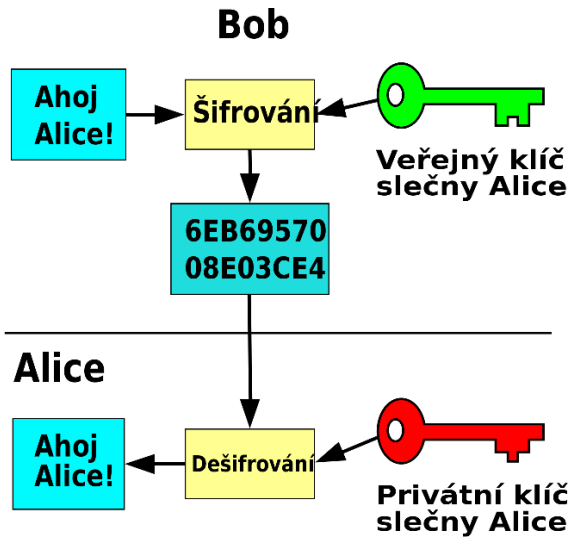
Spoofing, je podvod, který používají útočníci proto, aby získali osobní údaje nebo dostali přístup k cenným informacím. Používá se k maskování kybernetických útoků tak, aby vypadaly jako známý přijímač zdroje. Nejvíce se vyskytuje v méně zabezpečených komunikačních mechanismech. Může se vyskytnout i přes mobilní komunikaci. Útočník maskuje číslo, které se vydává například za vaší, banku. Poté po vás chce přihlašovací údaje.

Další možností jsou falešné weby, nejčastější webové stránky bank. Podobně jako phishing mají tyto stránky za úkol získání hesel nebo číslo karty.



9. Kryptografický systém

V dnešní době věda, která se zabývá vytvářením šifrování zpráv. Jsou to nástroje pro utajování důležité komunikace. Dnes se s tím moc nesetkáme, ale můžeme to každý použít pro maximální bezpečí našich zpráv. Jako jsou: hesla, citlivé údaje, bankovní spisy.



10. Odposlech

Můžeme dělit na legální a ilegální

Narušitelé můžou využít veřejné sítě pro hosty které jsou plně otevřený a způsobit tak únik odposlechů hovoru z jiných zařízení.

Odposlouchává se soukromý rozhovor, nejčastěji mezi hosty v síti

Známé programy na odposlech, které používala FBI a NSA jsou:

- Carnivore
- Narusinsight

11. Elevace oprávnění

Elevace oprávnění je v informatice zneužití chyby tak, že útočník získá například v operačním systému vyšší oprávnění, než mu byla správcem počítače udělen.
Typicky chyba v SUID program s právy správce provede nechtěnou akci
Pro elevaci oprávnění je využíván např:

- Exploit (často ve formě skriptu pro masivní útok)
- Sociální inženýrství
- Fyzický přístup k počítači

12. Závěr

V své ročníkové práci jsem chtěl upozornit na to, čemu se vyvarovat na internetu a ukázat vám, jak funguje celá síť a její zabezpečení. Dále jsem také chtěl ukázat jaké jsou možné hrozby, které mohou vaše zařízení napadnout nebo jinak ohrozit, popřípadě vaše účty například bankovní...

13. Resumé

My final work is about computer security, cybersecurity or information technology security (IT security). It is the protection of computer systems and networks from the theft of or damage of hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

14. Zdroje

https://upload.wikimedia.org/wikipedia/commons/thumb/5/52/Asymetrick%C3%A1_kryptografie.svg/1280px-Asymetrick%C3%A1_kryptografie.svg.png

https://upload.wikimedia.org/wikipedia/commons/5/54/Jak_snadno_poznat_phishing.png

https://www.soselectronic.cz/articles/sos-supplier-of-solution/kryptograficke-systemy-2127

https://www.comptia.org/content/articles/what-is-spoofing

https://cs.wikipedia.org/wiki/Zranitelnost

Kniha:

SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.