ABSOLVENTSKÁ PRÁCE
ZÁKLADNÍ ŠKOLA, ŠKOLNÍ 24, BYSTRÉ 569 92
9. ROČNÍK

PHISHING
ANEB JAK SNADNÉ JE RHYBHAŘENÍ

Tomáš Mládek

ŠKOLNÍ ROK 2022/2023

Prohlašuji, že jsem absolventskou práci vypracoval samostatně a všechny použité zdroje jsem řádně uvedl.

Děkuji za pomoc při zpracování tématu mému garantovi, panu učiteli Janu Mužíkovi a dále děkuji svému bratrovi za cenné rady při vypracování praktické části.

V Hartmanicích dne 12. 5. 2023

Obsah

Úvod.....**2**
1 Teoretická část.....**3**
1.1 Phishing – vysvětlení pojmů.....3
1.1.1 Historie phishingu.....3
1.1.2 Techniky phishingu.....3
1.1.3 Phishingové útoky.....4
1.2 Typy phishingových útoků.....5
1.3 Znaky phishingového útoku.....6
1.4 Ochrana před phishingovými útoky.....7
1.5 Co je pharming?.....7
1.6 Rozdíl mezi phishingem a pharmingem.....8
2 Praktická část.....9
2.1 Instalace operačního systému Linux.....9
2.2 Vytvoření phishingové webové stránky.....11
2.3 Odeslání phishingového e-mailu.....13
2.4 Ukázka získání osobních přihlašovacích údajů.....16
Závěr.....**19**
Přehled použitých zdrojů.....**20**

Úvod

Ve své absolventské práci bych vám chtěl vysvětlit, co to je a jak snadný je „phishing“. Tento pojem si můžeme představit jako rybaření na internetu. Útočník (rybář) se snaží „chytit“ vaše přihlašovací údaje nebo jiné osobní informace. Vy ve své podstatě hrajete roli ryby.

Toto téma jsem si vybral kvůli tomu, že phishing bývá velmi častý a nikdo vlastně neví, jak se mu vyvarovat. Proto jsem se o něm chtěl dozvědět více a vyzkoušet si ho v praxi.

Moje absolventská práce se dělí na dvě části, část teoretickou a část praktickou. V části teoretické vám vysvětlím pojem „phishing“. Následně popíši historii a techniku phishingu, typy a znaky phishingových útoků, jak se bránit před takovým útokem a nakonec vám také popíšu blízkého kamaráda phishingu – pharming.

V praktické části se vám pokusím ukázat, jak takový útok vlastně vypadá a co všechno je potřeba k vytvoření falešné webové stránky a e-mailu.

Očekávám, že mi vypracování této práce přinese mnoho nových informací a zkušeností, které budu moci v budoucnu využít.

1 Teoretická část

1.1 Phishing – vysvětlení pojmů

Phishing je podvodná technika používaná na internetu k získávání citlivých údajů a dat v elektronické komunikaci. Jedná se např. o hesla, čísla kreditních karet, přihlašovací údaje k internetovému bankovnictví apod. Kouzlo phishingu je, že k nalákání obětí předstírá, že se jedná o ověřený web, populární sociální síť, naše internetové bankovnictví atd. Často staví na lidské důvěřivosti a lenosti ověřovat si věcí. [1]

Principem phishingu je rozesílání e-mailů či SMS, ve kterých útočník zašle také odkaz na falešnou internetovou stránku, která je téměř identická s oficiální stránkou. Stránka obvykle napodobuje přihlašovací okno do nějaké aplikace (internetové bankovnictví, pojišťovna, …), kam oběť zadá svoje přihlašovací údaje. Poté už je pro útočníka jednoduché vybrat si peníze z účtu či jinak zneužít citlivých údajů oběti. [1]

1.1.1 Historie phishingu

Technika útoku byla detailně popsána již v roce 1987 a termín phishing poprvé použit v roce 1996. K prvnímu reálnému útoku došlo v roce 1995 v síti giganta AOL ve Spojených státech. Další generace útoků se objevila v roce 2001, kdy došlo k napadení první finanční instituce (E-gold). Roku 2004 byl phishing považován za plně rozvinutou ekonomiku zločinu. Uvádí se, že mezi květnem 2004 a květnem 2005 bylo kvůli phishingu ztraceno téměř 930 milionů amerických dolarů. [2]

1.1.2 Techniky phishingu

Jaké jsou techniky phishingu? Každý rok vznikají nové a nové taktiky útoků. Všechny typy mají stejný cíl, a to získat citlivé údaje oběti. [1]

Hacking sdíleného virtuálního serveru – útočník vnikne do webového serveru, který hostuje mnoho domén (tzv. sdílený virtuální server). Jakmile útočník vnikne do takového serveru, místo „návnady“ napřed na server nahraje svůj obsah. Poté už si jen pohraje s tím, aby se server choval tak, jak on chce. Výhodou je, že útočník může infikovat několik webů najednou, podle toho, jak je server velký.

Využití poddomén – funguje tak, aby odkazy v e-mailech (a i příslušné stránky) vypadaly, že náleží falešné organizaci. Následující odkaz od *http://www.konkretnibanka.novasluzba.cz/* vypadá, jako by vedl na sekci *nová služba* na webu *konkrétní banky*; ve skutečnosti tento odkaz vede na sekci „*konkrétní banka*“ (tedy phishing) stránky „*nová služba*“.

Překlepy a zkreslení odkazů – běžným trikem bývají překlepy v odkazech nebo změna textu odkazu tak, aby vypadal podobně jako skutečný odkaz.

IDN spoofing – principem je, aby vizuálně identické adresy vedly na odlišné, nebezpečné weby (změna písma, znaků, číslic). Útočníci zneužívají tohoto rizika použitím otevřeného URL přesmě-

rování na stránkách důvěryhodné organizace k zamaskování škodlivého obsahu s důvěryhodnou doménou (cílem je, aby se co nejvíce podobali oficiální stránce).

Unikání filtrům – útočníci začali používat obrázky místo textu, aby zkomplikovali anti-phishingovým filtrům rozpoznat běžné texty nebezpečných e-mailů.

Padělání stránek – některé podvodné stránky používají JavaScript pro změnu adresního řádku. Všechno od webové adresy po bezpečnostní certifikát se jeví korektně. Ve skutečnosti je však odkaz na stránku vytvořený tak, aby provedl útok.

Evil twin – útočník vytvoří falešnou bezdrátovou síť podobnou té reálné. Často je najdeme v hotelech, kavárnách atd., kdykoli se někdo připojí, útočník se snaží zachytit jejich důvěrné údaje.

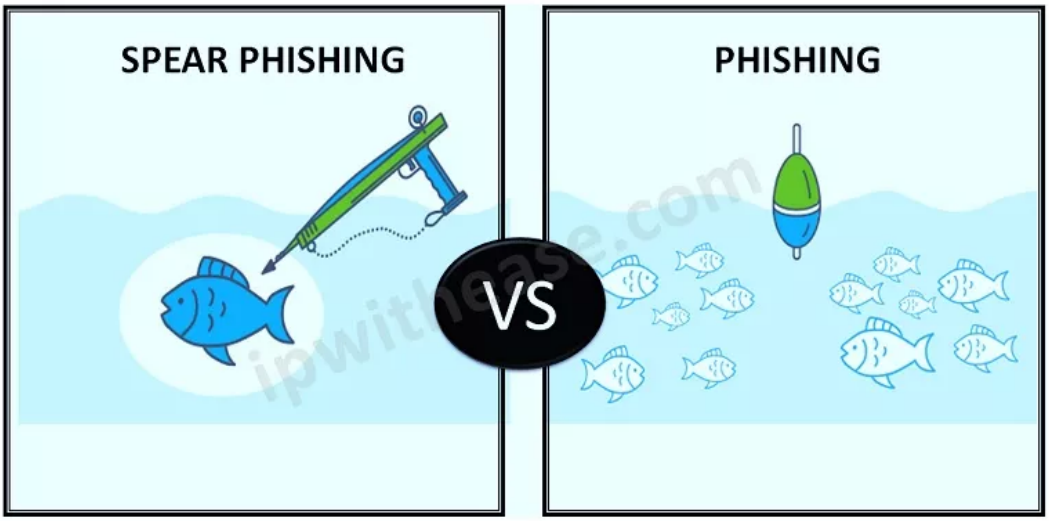
Tabnabbing – zneužívá záložek, které oběť používá a tiše přesměruje uživatele na falešnou stránku.

1.1.3 Phishingové útoky

Základní druhy phishingových útoků se dělí podle velikosti skupiny, na kterou právě útočník cílí.

Příkladem může být Spear phishing vs Normal phishing.

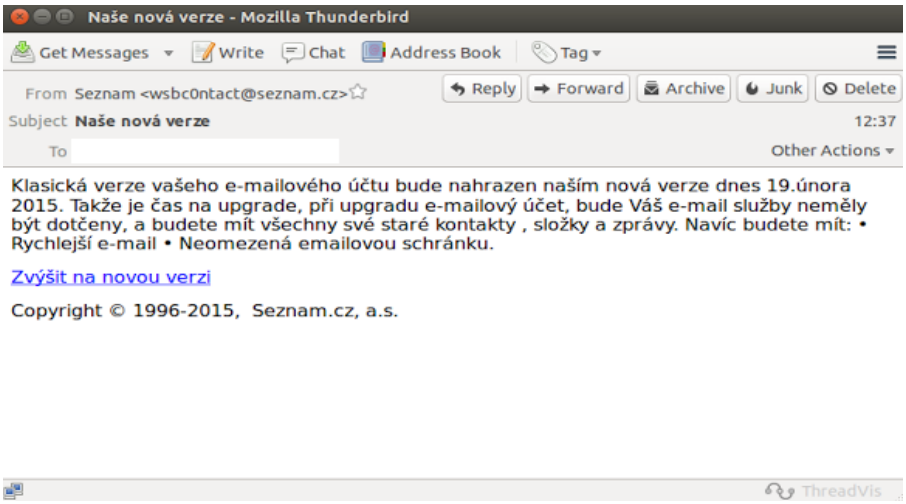
Normální phishing funguje tak, že útočník pošle několika stovkám i tisícům lidem e-mail, SMS atd. Spear phishing funguje stejně, ale je určen přímo na jednu skupinu lidí nebo dokonce na jednoho člověka (viz. Obrázek 1).



Obrázek 1: Rozdíl phishingu a spear phishingu [10]

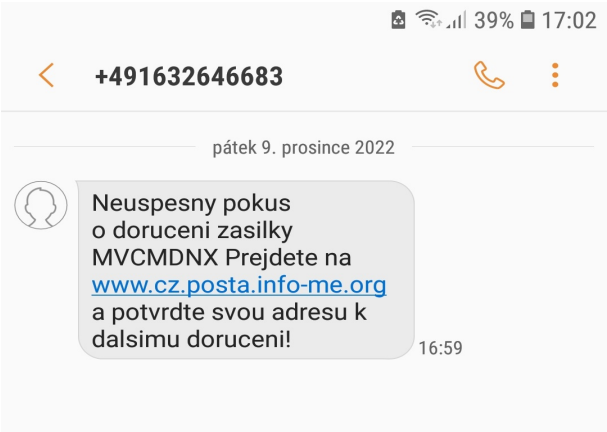
1.2 Typy phishingových útoků

E-mailové podvody – útočník zašle několika lidem e-mail s textem, který je od pohledu např. špatně napsán, text je velmi doléhavý apod. Součástí textu je i odkaz na webovou stránku, kam vás útočník směruje (viz. Obrázek 2). [1]



Obrázek 2: Příklad e-mailového phishingu [11]

Smishing – forma phishingu, která místo e-mailu spíše používá SMS zprávy (viz. Obrázek 3). Zpráva přichází od neznámého čísla a opět po oběti chce, aby klikla na odkaz, který je ve zprávě. Často se zpráva tváří, jako by ji poslala např. banka, pojišťovna nebo jiné. [3]



Obrázek 3: Příklad smishingu

Vishing – útočník v e-mailu požaduje oběť, aby zavolala na určité číslo za účelem např. odvolání problémů s jejich účtem. Jakmile oběť zavolá na určité číslo (vlastněné útočníkem), útočník se bude snažit dostat z oběti citlivé údaje (viz. Obrázek 4). Objevují se i případy, kdy útočníci mohou přesměrováním simulovat hovor ze stejných čísel patřících bankám a zároveň často vystupují profesionálně a znají některé vaše údaje. Opět se útočník bude snažit z vás dostat peníze. [4]

Obrázek 4: Vishing v praxi [12]

Whaling – phishingový útok úzce zaměřený na výše postavené lidi (zaměstnance či ředitele firem), proto whaling jako lov velryb. Útočník se vydává za jejich nadřízeného, který ve zdánlivě oficiálním e-mailu požaduje od zaměstnance citlivé informace či přesun peněz. Nebo se v e-mailu vyskytuje odkaz na web, který se velmi podobá oficiálnímu webu banky. Poté není problém citlivých údajů zneužít. [5]

Spam over instant messaging (SPIM) – nevyžádané hromadné zprávy, které cílí na Instant Messaging. Instant Messaging je služba pro okamžité zasílání zpráv. Umožňuje svým uživatelům sledovat, jestli jsou jejich přátelé online a komunikovat s nimi např. (Messenger, Facebook, atd.). SPIM obvykle obsahuje zprávu nebo odkaz na webovou stránku, kde se opět útočník snaží získat citlivé údaje nebo si oběť samotným kliknutím na odkaz stáhne do zařízení nějaký škodlivý software. [6]

1.3 Znaky phishingového útoku

Jak poznat phishingový útok? Někdy je těžké ho poznat, ale existuje pár znaků, podle kterých ho poznat můžeme.

E-mailový phishing - poznáte ho podle více parametrů. Forma e-mailu, například od banky, nemusí být taková, na jakou jste zvyklí. Text může být psán lámanou češtinou (nebo úplně strojově přeloženou) s gramatickými chybami. Doména neodpovídá oficiální adrese dané společnosti. E-mail může obsahovat podezřelé odkazy na neznámé a nezabezpečené stránky. Nakonec, žádná taková společnost po vás nikdy nebude chtít přihlašovací údaje. [7]

Smishing – zpráva přichází od neznámého čísla. Text je často naléhavý, opět s častými chybami. Text vás směruje na odkaz, který vede na webovou stránku, kde máte vyplnit své přihlašovací údaje. [7]

Vishing – poznat vishing už je poněkud obtížnější. Hovor přichází od neznámého čísla (pokud útočník nevolá z čísla např. vašeho kamaráda). V hovoru na vás doléhá a chce po vás vaše citlivé údaje. [7]

Toto samozřejmě nejsou jediné typy phishingových útoků, se kterými se můžete v dnešní době setkat. Další útoky mohou přicházet s falešnými oznámeními o výhře a následném zadání údajů kreditní karty pro vyplacení výhry atd. [7]

1.4 Ochrana před phishingovými útoky

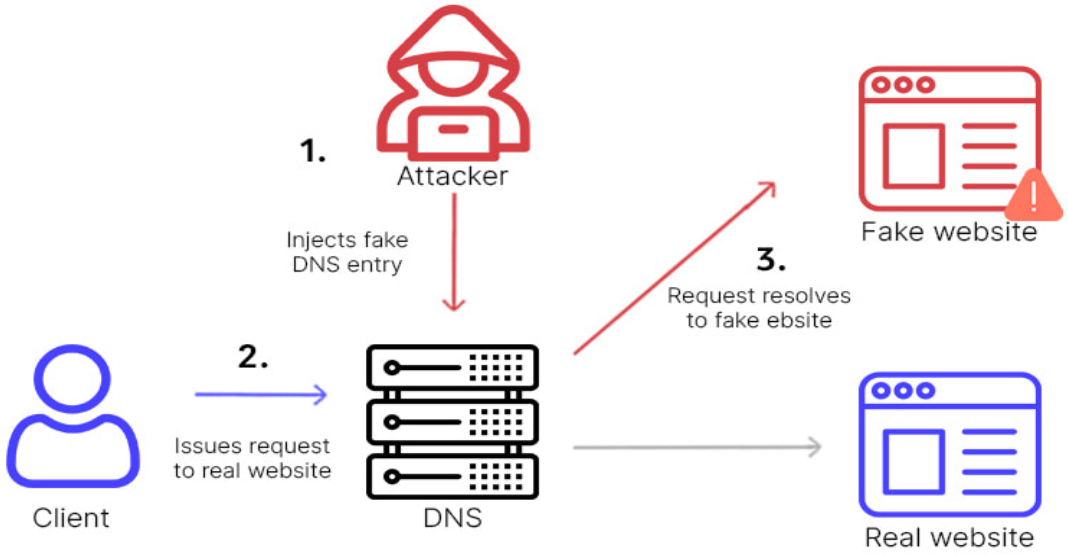
Útočníci vás budou chtít okrást všemi různými způsoby, ale vždy buďte obezřetní předtím, než něco uděláte a co kam pošlete. Vždy je lepší se předem poradit, než mít problémy. [9]

Ale jak se chránit?

- Banka, ani žádná podobná instituce, vás nebude žádat o přihlášení, obnovu certifikátu, ověření nebo změnu přihlašovacích údajů prostřednictvím emailu.
- Phishingové útoky vedené ze zahraničí lze rozeznat např. ze špatné češtiny v textu e-mailu.
- Nikdy neklikejte na odkazy v e-mailech a SMS zprávách.
- Kontrolujte ve webovém prohlížeči korektnost webové adresy, na které se nacházíte.
- Nikomu neukazujte a neposílejte své přihlašovací údaje.
- Útočníci budou doléhat na vaše pocity (budou vás nutit např. přihlásit se na určitou internetovou stránku).
- Řiďte se kroky uvedenými výše nebo těmi, které najdete na internetu.

1.5 Co je pharming?

Pharming je o něco mladší sourozenec phishingu. Opět se jedná o podvodnou techniku na internetu, při které se snaží útočník získat citlivé údaje toho, kdo na ni skočí. Princip tohoto kybernetického útoku je založen na napadení DNS (Domain name system – systém doménových jmen). DNS slouží k překladu doménových jmen na IP adresy. Při napadeni tedy útočník přiřadí doménovému jménu jinou IP adresu, než tu validní. Na této falešné podvržené IP adrese se nachází identická stránka, kterou útočník využije k získání osobních údajů oběti. Důsledek uvedu na příkladu. Při zadání URL „seznam.cz“ do webového prohlížeče nejsme přesměrováni na pravou stránku, ale na útočníkem vytvořenou stránku, která je identická. Při zkontrolování URL uživatel nepozná, že se jedná o stránku vytvořenou útočníkem. Byla totiž změněna jenom IP adresa (viz. Obrázek 5). [8]



Obrázek 5: Princip pharmingu [13]

1.6 Rozdíl mezi phishingem a pharmingem

Hlavním rozdílem mezi phishingem a pharmingem je princip jejich fungování. Phishing – útočník rozesílá e-maily s odkazem na internetovou stránku podobné nějaké oficiální. Stránku ale můžete poznat podle nějakých znaků. Naopak pharming – útočník napadá DNS a přepisuje IP adresu. Takže URL webové stránky je stejná jako má stránka oficiální, ale IP adresa ne. A to při pohledu na stránku nepoznáte. To znamená, že pharming je těžší na rozpoznání. Jediná věc, kterou mají společnou, je cíl. Získat něčí citlivé údaje.

2 Praktická část

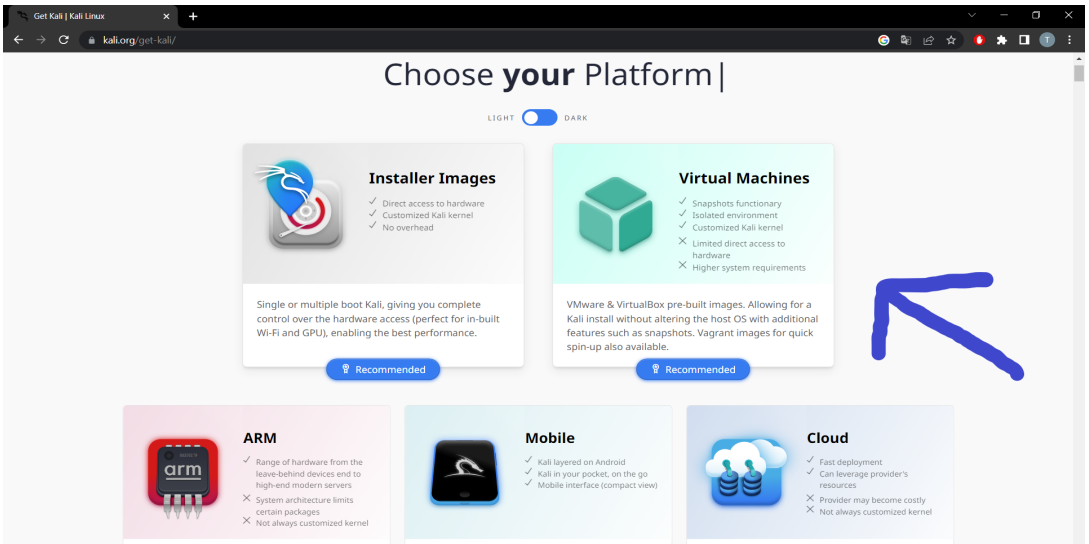
2.1 Instalace operačního systému Linux

Pro instalaci operačního systému Linux (konkrétně distribuce Kali Linux) je potřeba také nainstalovat program VirtualBox.

Kali Linux má přibližně 600 programů pro testování penetrace, bezdrátových sítí LAN, skenerů webových aplikací a má také grafický nástroj pro správu kybernetických útoků. Má ovšem také několik programů určených k „hackování“.

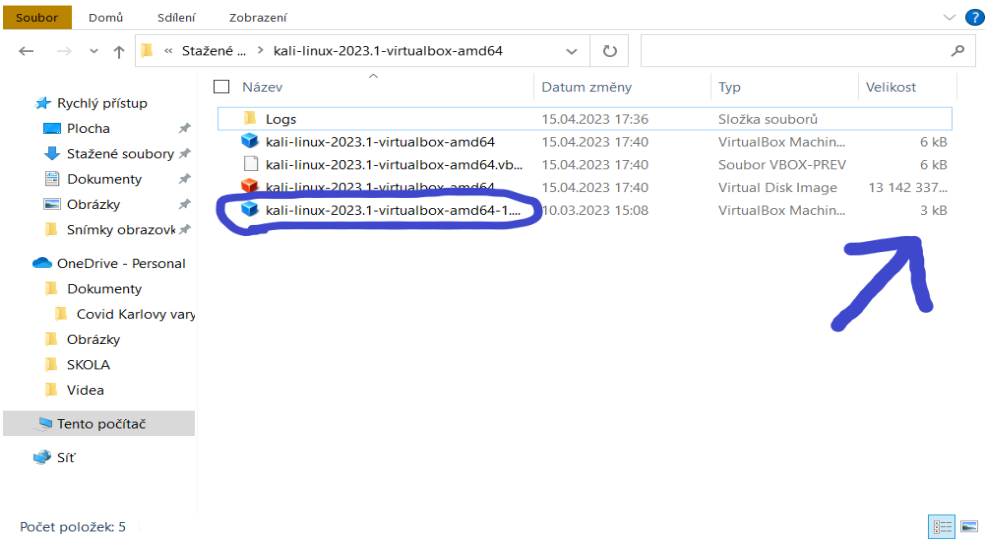
VirtualBox je software pro virtualizaci, který umožňuje vytvářet a spouštět virtuální počítače na vašem fyzickém počítači. Virtuální počítač je jako samostatný počítač s vlastním operačním systémem, ale je hostován na vašem fyzickém počítači. Největší výhodou je tedy fakt, že nemusíme mít zvláštní počítač s jiným operačním systémem, ale můžeme mít „spuštěných“ více operačních systémů najednou. VirtualBox umožňuje uživateli nainstalovat různé operační systémy, jako jsou Windows, Linux a macOS, jako virtuální stroje. Tyto virtuální stroje mohou být spuštěny v samostatném okně na fyzickém počítači, což umožňuje uživatelům testovat různé operační systémy nebo aplikaci bez nutnosti hlubšího zásahu do námi používaného operačního systému.

Abychom dokončili instalaci VirtualBoxu, musíme ještě nainstalovat Python (programovací jazyk). Poté nainstalujeme samotný Kali Linux určený pro VirtualBox (viz. Obrázek 6).



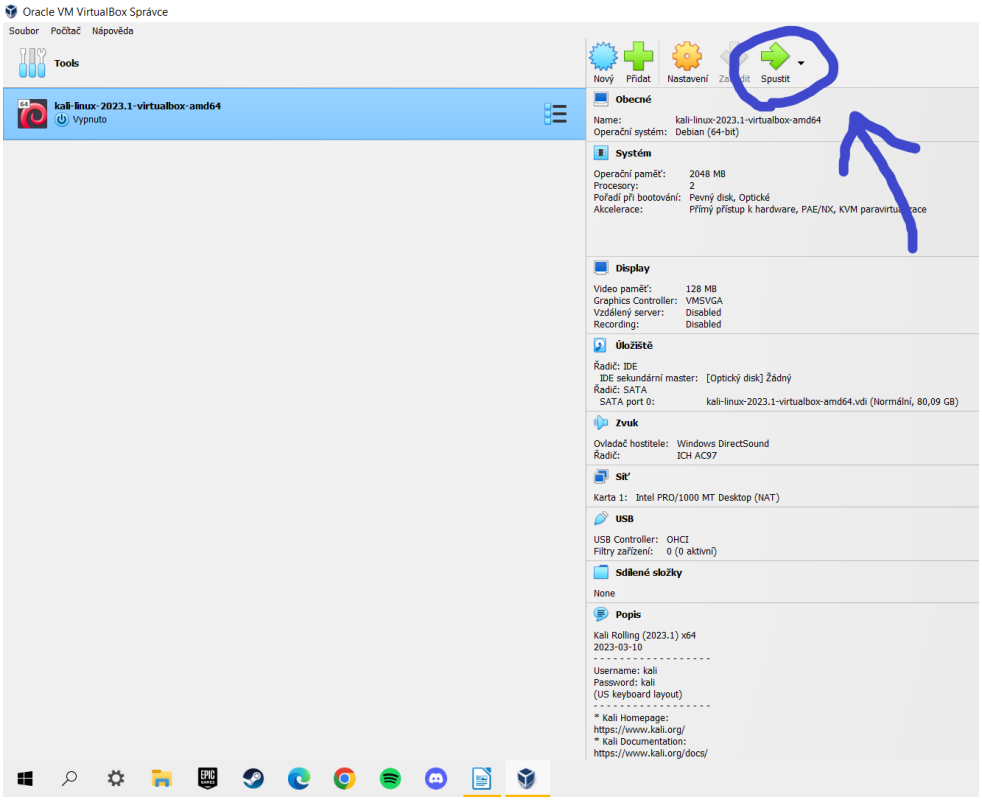
Obrázek 6: Instalace OS Kali Linux pro VirtualBox

Nyní už jen ve složce stažené soubory otevřeme složku, kterou jsme si stáhli a dvakrát klikneme na soubor s velikostí 3kB (viz. Obrázek 7).



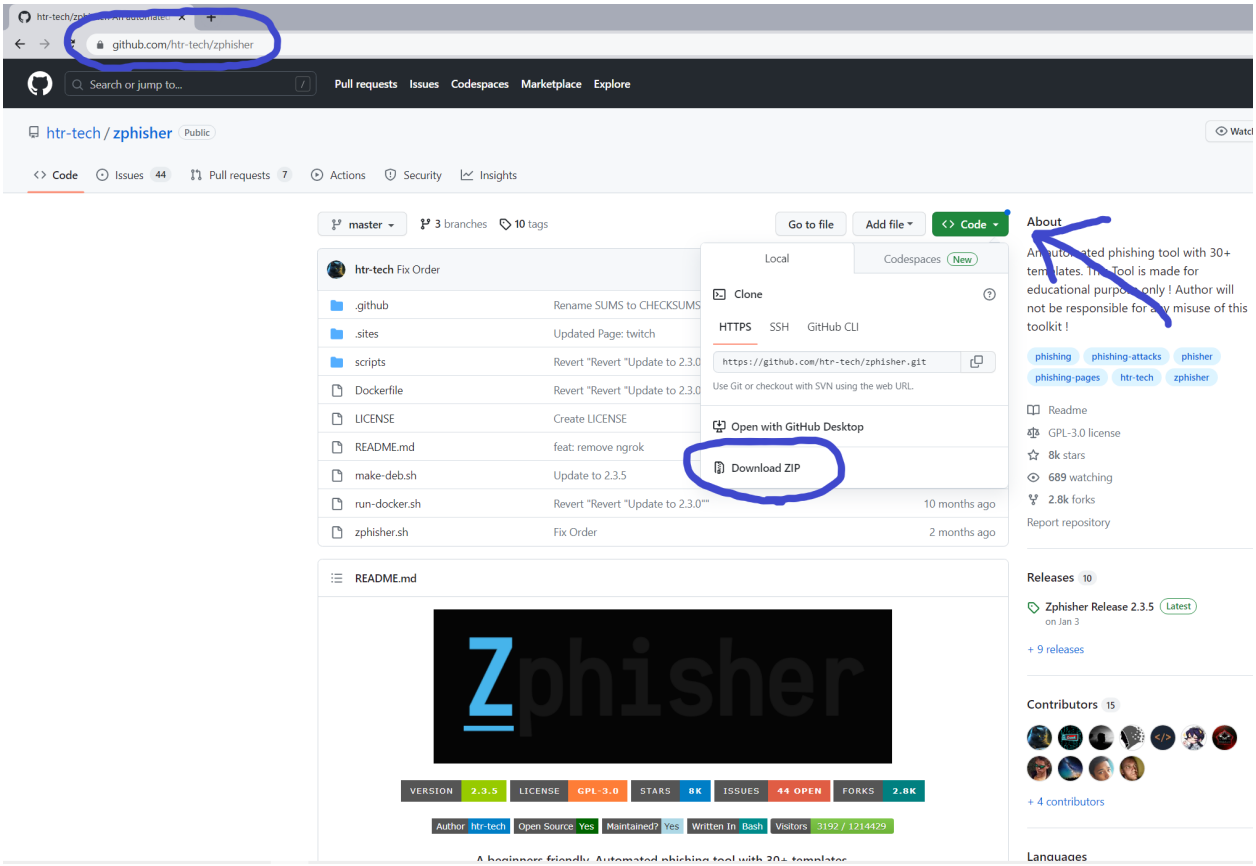
Obrázek 7: Instalace OS Kali Linux pro VirtualBox 2

Teď už se nám systém Kali Linux přidal do VirtualBoxu a už s ním můžeme pracovat. Systém je již nakonfigurovaný, stačí jej tedy spustit tlačítkem (viz. Obrázek 8).



Obrázek 8: Spuštění OS Kali Linux

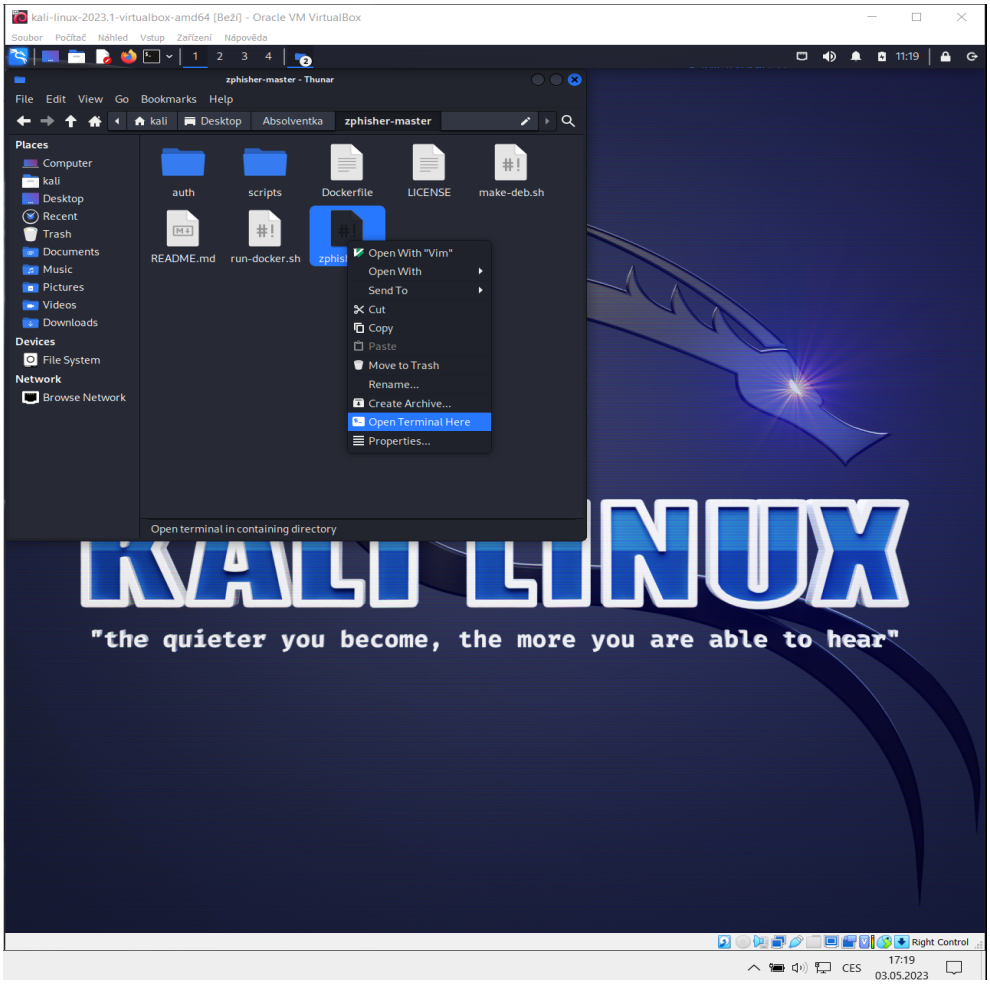
2.2 Vytvoření phishingové webové stránky



Obrázek 9: Instalace programu Zphisher

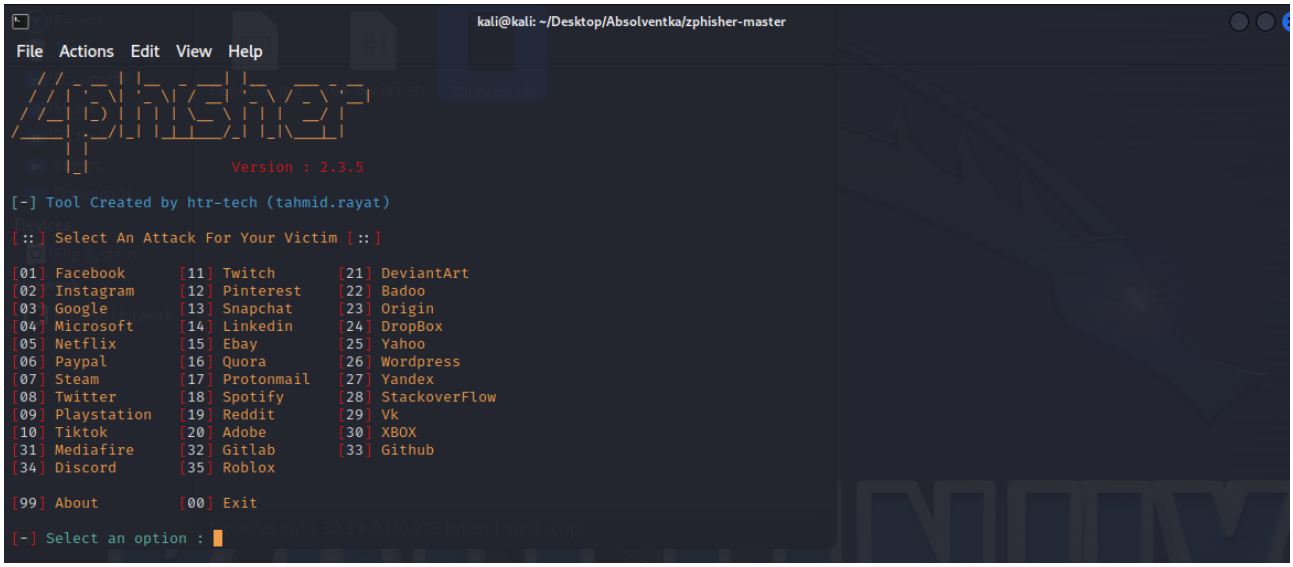
Vše co potřebujeme k vytvoření phishingové webové stránky je jeden jediný program. Já osobně jsem použil Zphisher. Program jsem nainstaloval přímo v prostředí Kali Linuxu z oficiálních stránek Githubu jako soubor ZIP (viz. Obrázek 9).

Poté, co se nám složka Zphisher - master stáhla, ji pouze rozzipujeme. Složku otevřeme a pravým tlačítkem myši klikneme na soubor s názvem „zphisher“ a poté klikneme na „Open Terminal Here“. Tím se nám otevře terminál ve složce, kde se nachází Zphisher (viz. Obrázek 10).

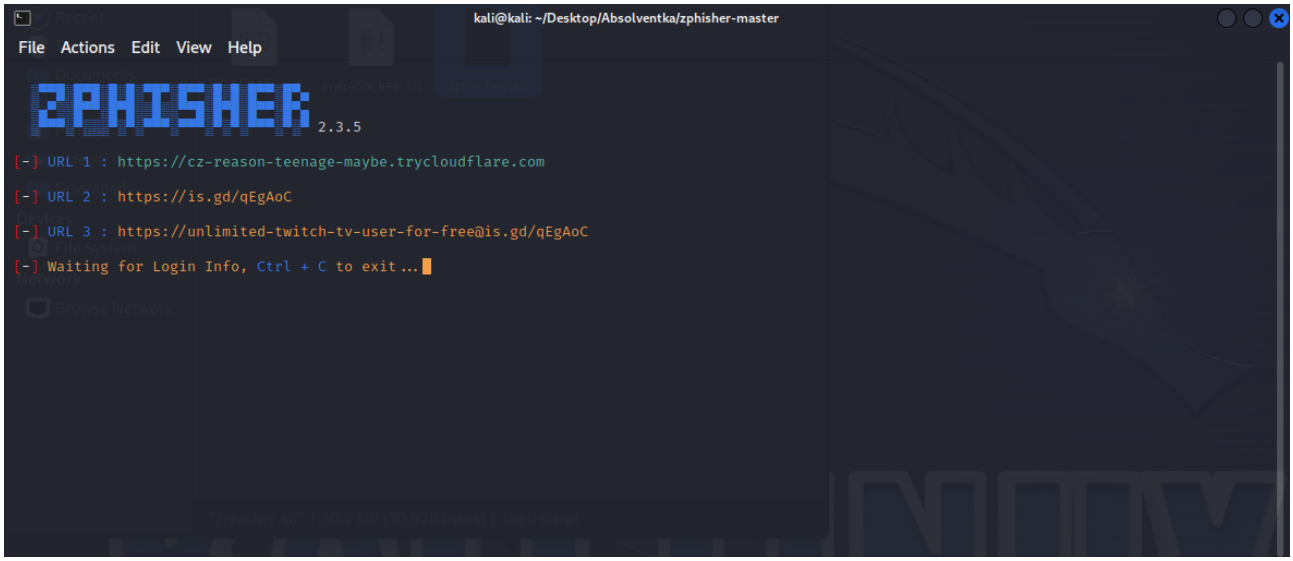


Obrázek 10: Otevření programu Zphisher

Je možné, že se po otevření terminálu ještě bude Zphisher aktualizovat. Jinak do terminálu vložíme příkaz „bash zphisher.sh“ a program se nám následně spustí. Vzhled programu bude vypadat následovně (viz. Obrázek 11). Samotná práce s programem je velmi jednoduchá. Do terminálu pouze píšeme pomocí čísel. Čísla nám udávají, kterou aplikaci jsme si vybrali a ostatní potřebné věci k vytvoření phishingové stránky. Poté, co vše vyplníme, nám program sám vytvoří odkaz na phishingovou stránku (viz. Obrázek 12).



Obrázek 11: Hlavní stránka programu Zphisher

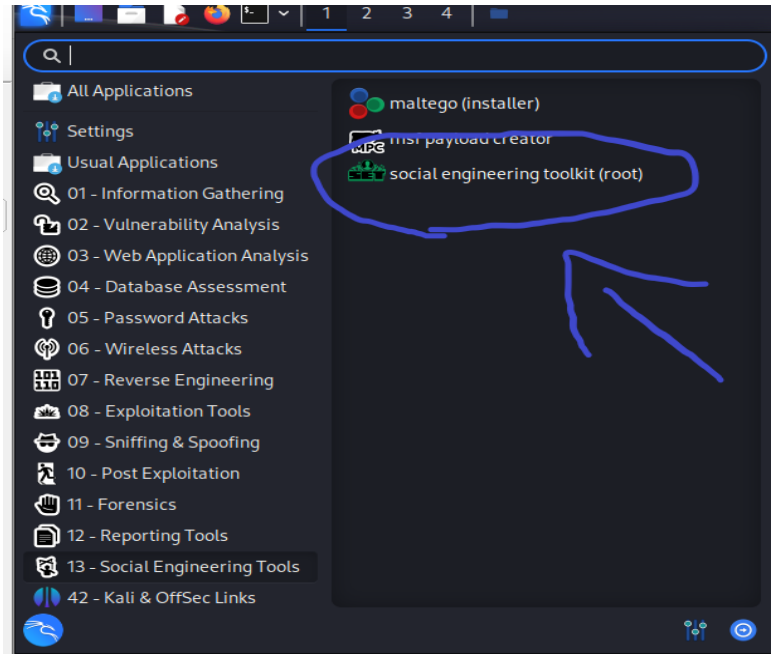


Obrázek 12: Odkaz na phishingovou webovou stránku

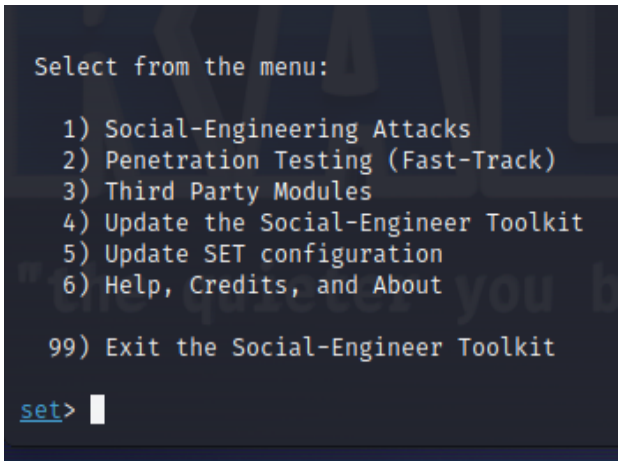
Po vložení odkazu na webový prohlížeč se nám otevřela phishingová stránka a po vložení přihlašovacích údajů proběhlo přesměrování na oficiální stránku aplikace a tak uživatel nemusí poznat, že zadal své přihlašovací údaje někam, kam neměl.

2.3 Odeslání phishingového e-mailu

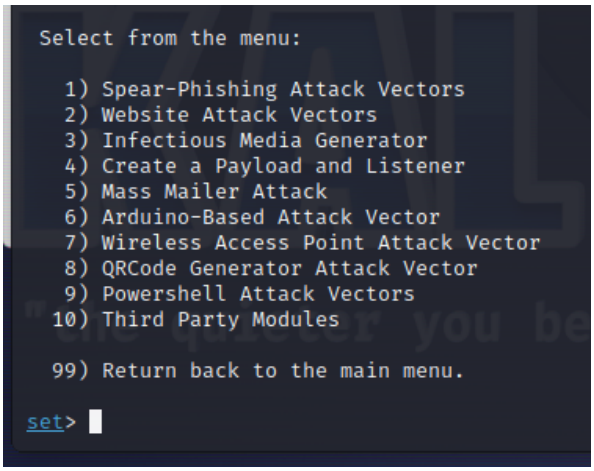
Pro vytvoření phishingového e-mailu si v Kali Linuxu otevřeme nástroj se jménem – Social engineering toolkit - SET (viz. Obrázek 13). Uvnitř nástroje je nutné vyplnit několik informací k vytvoření samotného phishingového e-mailu (viz. Obrázek 14-16). Informace k vyplnění: e-mail odesílatele, heslo e-mailu odesílatele, phishingové jméno e-mailové adresy odesílatele, e-mail příjemce, předmět zprávy e-mailu a hlavně samotný obsah zprávy. Po dokončení všech těchto kroků pouze napíšeme na další řádek „END“ a e-mail by se měl poslat (viz. Obrázek 17).



Obrázek 13: Nástroj SET



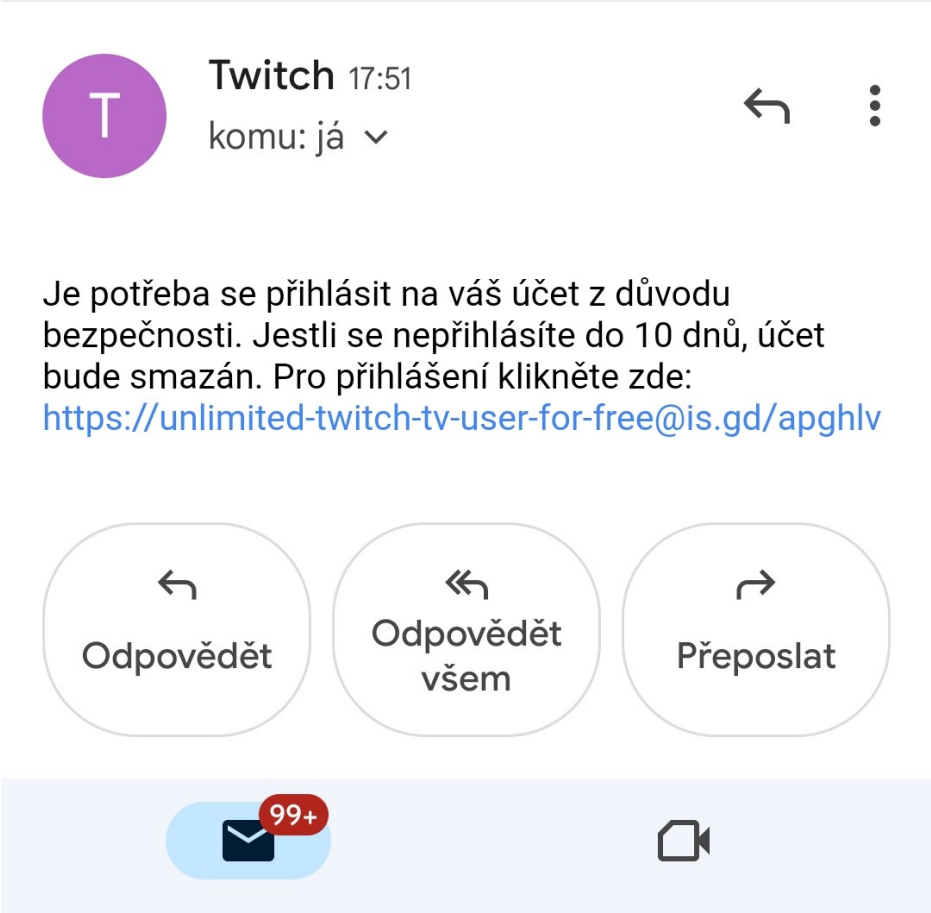
Obrázek 14: Vybereme možnost 1)



Obrázek 15: Vybereme možnost 5)

To by ale vše muselo fungovat bez problémů. Bohužel jsem narazil na situaci, kdy se nástroj ne-spokojil s heslem mého e-mailu a proto jsem žádný phishingový e-mail neposlal. S pomocí mého bratra jsem hledal řešení problému a zjistil jsem, že je nutné zapnout si u svého e-mailu dvoufázové ověření a následně vygenerovat heslo pro aplikaci „třetí strany“. Tedy, toto heslo funguje pouze při používání aplikace „třetí strany“ a po vložení vygenerovaného hesla do nástroje SET mně vše fungovalo, jak mělo.

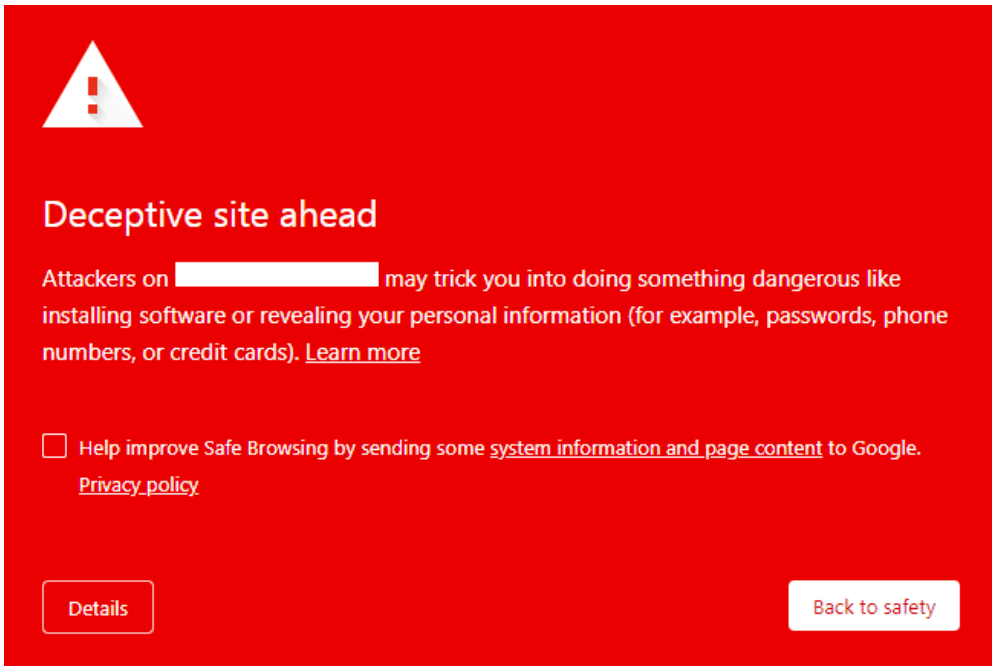
Obrázek 16: Proces vytváření phishingového e-mailu



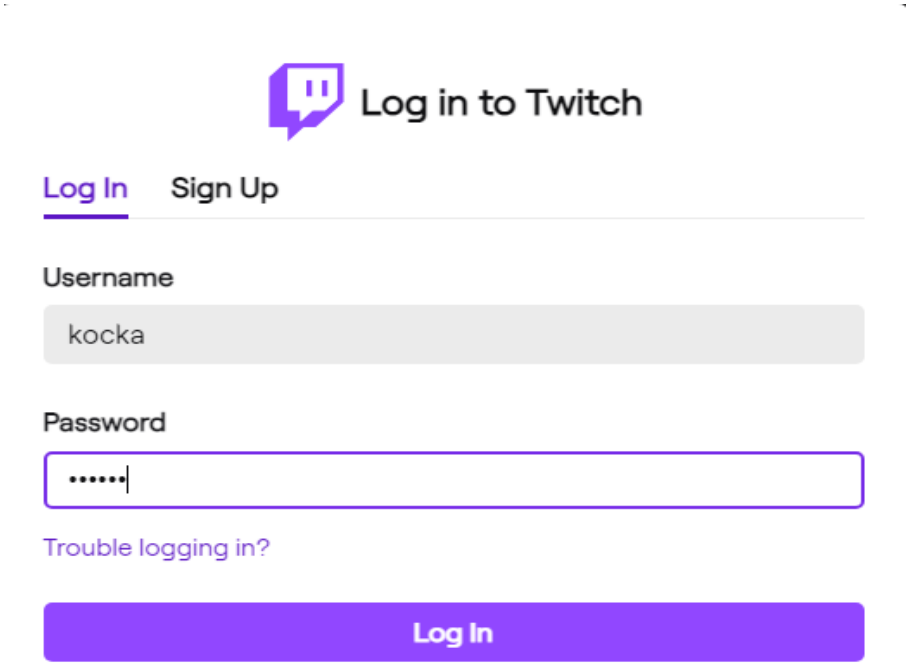
Obrázek 17: Ukázka phishingového e-mailu

2.4 Ukázka získání osobních přihlašovacích údajů

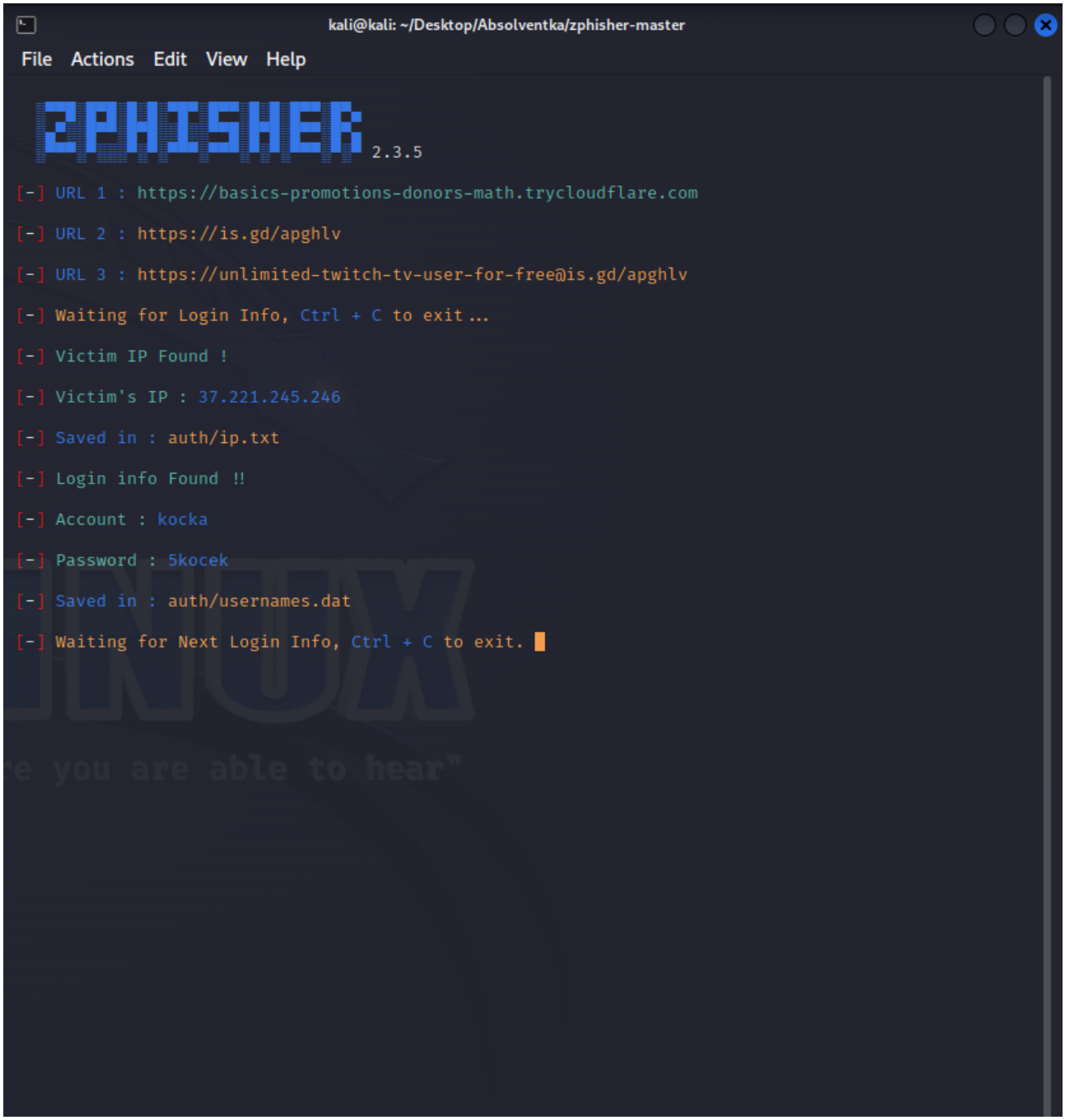
K získání citlivých údajů je potřeba mít pouze zapnutý program Zphisher po celou dobu, protože se nám jinak program vypne a žádné citlivé údaje nezískáme. Jelikož program má hodně webových stránek na výběr, několik z nich jsem vyzkoušel. Zjistil jsem, že některé z phishingových stránek byly internetovým prohlížečem rozpoznány (viz. Obrázek 18). Záleží také na druhu internetového prohlížeče a jeho verzi. Proto jsem si vytipoval ty, které prohlížeč nerozpozná. Jednalo se např. o stránku Twitch (viz. Obrázek 19). Poslední, co nás tedy zajímá jsou získané přihlašovací údaje (viz. Obrázek 20).



Obrázek 18: Rozpoznaná phishingová stránka internetovým prohlížečem



Obrázek 19: Doplnění přihlašovacích údajů na phishingovou stránku



Obrázek 20: Ukázka získání přihlašovacích údajů

Závěr

Vypracování této absolventské práce mně přišlo velmi zajímavé a zjišťování informací mě velice bavilo. Jsem moc rád, že jsem si phishing mohl vyzkoušet a zjistit si několik informací o tom, jak funguje. Jediné, co bych příště udělal jinak, je můj časový harmonogram. Protože je vždy lepší mít nějakou časovou rezervu, než věci dodělávat na poslední chvíli.

Pro mě nejzajímavější částí práce bylo vytvoření falešné webové stránky a e-mailu a zkusit získat přihlašovací údaje některého z mých kamarádů. Bohužel, nikoho z nich jsem nenachytal. Na druhou stranu jsem si vyzkoušel phishing v praxi.

Nakonec bych chtěl zmínit a zdůraznit, že práce byla vypracována pouze pro vzdělávací účely a ne k tomu, aby někoho inspirovala ke krádeži přihlašovacích údajů jiných osob.

Přehled použitých zdrojů

[1] Phishing. Wikipedie: Otevřená encyklopedie [online]. 5. 3. 2009 [cit. 2023-05-12]. Dostupné z: https://cs.wikipedia.org/wiki/Phishing

[2] Co je phishing a jak se proti němu bránit. Antimalware [online]. 15. 9. 2012 [cit. 2023-05-12]. Dostupné z: https://www.antimalware.cz/blog/co-je-phishing

[3] Smishing. SkipPay [online]. [cit. 2023-05-12]. Dostupné z: https://skippay.cz/blog/slovnik-pojmu/pismeno-s/smishing/#redirected

[4] Co je vishing. SPRÁVA SÍTĚ: slovník pojmů [online]. [cit. 2023-05-12]. Dostupné z: https://www.sprava-site.eu/vishing/

[5] Whaling ve 3 bodech: Co to je, proč to funguje a jak se uchránit?. Whalebone [online]. 11. 11. 2021 [cit. 2023-05-12]. Dostupné z: https://www.whalebone.io/post/whaling-ve-3-bodech-co-to-je-proc-to-funguje-a-jak-se-uchranit

[6] SPAM-over-Instant Messaging (SPIM). Documentation.avaya.com [online]. 4. 12. 2012 [cit. 2023-05-12]. Dostupné z: https://documentation.avaya.com/en-US/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/SPAM_over_Instant_Messaging_.html

[7] Phishing: definice phishingu, jak jej rozpoznat a jak na phishingový útok vyzrát. Cnews.cz [online]. 3. 3. 2022 [cit. 2023-05-12]. Dostupné z: https://www.cnews.cz/co-je-phishing-a-jak-se-branit

[8] Pharming. SPRÁVA SÍTĚ [online]. [cit. 2023-05-12]. Dostupné z: https://www.sprava-site.eu/pharming/

[9] Ochrana před útoky phishing. Microsoft [online]. [cit. 2023-05-12]. Dostupné z: https://support.microsoft.com/cs-cz/windows/ochrana-p%C5%99ed-%C3%BAtoky-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

[10] Spear Phishing Attack: Cyber Security. In: IPWITHEASE [online]. [cit. 2023-05-22]. Dostupné z: https://i0.wp.com/ipwithease.com/wp-content/uploads/2022/03/SPEAR-PHISHING-ATTACK-2.jpg?w=800&ssl=1

[11] Na uživatele pošty Seznamu míří přímo cílený phishing. In: Lupa.cz [online]. [cit. 2023-05-22]. Dostupné z: https://i.iinfo.cz/images/528/na-uzivatele-posty-seznamu-miri-primo-cileni-phishing-3.png

[12] What is Vishing and Is It A Threat to Your Business?. In: Bolster [online]. [cit. 2023-05-22]. Dostupné z: https://bolster.ai/wp-content/uploads/2023/04/shutterstock_2128640126.jpg

[13] What Is DNS spoofing DNS Cache Poisoning. In: Wallarm [online]. [cit. 2023-05-22]. Dostupné z: https://assets.website-files.com/5ff66329429d880392f6cba2/60c35205a08c01989ab2f764_DNS%20Spoofing.jpg