Pokusy o prienik do online Linux systémov

Attempts to penetrate online Linux systems

Pavol Sojka[1]

Abstrakt
V prvej a druhej časti nášho článku popisujeme niekoľko typov útokov, ktoré v súčasnosti ovplyvňujú bezpečnosť dát. Zameriavame sa na slovníkové útoky a útoky hrubou silou v teórii a praxi. Následne sme vybrali službu (Secure shell server), ktorá je vystavená do internetu a je známa ako nástroj pre systémových administrátorov na spravovanie a údržbu operačných systémov. Tretia kapitola popisuje metodiku, ktorú sme použili v našom výskume. Štvrtá kapitola sa zameriava na výsledky, ktoré sme získali pomocou rôznych techník, a nakoniec na protiopatrenia, ktoré sme aplikovali. Vyfiltrovali sme krajiny, z ktorých boli útoky vedené, a nakoniec sme ukázali stručný graf nákladov vynaložených na bezpečnostné opatrenia a odhadovaných budúcich nákladov.

Kľúčové slová
bezpečnosť, zraniteľnosť, online systémy, protiopatrenia

Abstract
In the first and second parts of our article, we describe several types of attacks that currently affect data security. We focus on dictionary attacks and brute force attacks in theory and practice. We then selected a service (Secure shell server), which is exposed to the Internet and is known as a tool for system administrators to manage and maintain operating systems. The third chapter describes the methodology we used in our research. The fourth chapter focuses on the results we obtained using different techniques and finally on the countermeasures we applied. We filtered out the countries from which the attacks were conducted and finally we showed a brief graph of the costs spent on security measures and estimated future costs.

Key words
security, vulnerability, online systems, countermeasures

JEL classification
M15

1 Úvod

V posledných rokoch sme svedkami rýchleho zavádzania nových technológií a modernizácie existujúcich. Každé zariadenie a služba, ktorú vlastníme, generuje určité množstvo údajov. Tieto údaje sa stávajú cennejšími ako predtým kvôli neustálemu prechodu z papierových médií na digitálne médiá v štátnej správe, podnikovej sfére a podobne. Údaje sú cenné pre čierny trh pri obchodovaní, špionáži, vydieraní a iných nelegálnych aktivitách. Štátna správa, ale aj súkromné spoločnosti investujú viac prostriedkov do posilnenia bezpečnosti svojich systémov a bezpečnostného povedomia zamestnancov. Tieto položky v rozpočtoch neustále rastú, preto je potrebné zdôrazniť najslabšie miesta v infraštruktúre. Tieto miesta by mali byť identifikované individuálne podľa potrieb spoločnosti a podľa služieb, ktoré

[1] Ekonomická univerzita v Bratislave, Fakulta hospodárskej informatiky, Katedra aplikovanej informatiky, Dolnozemská cesta 1/b, 852 35 Bratislava, pavol.sojka@euba.sk.

poskytujú. Náš článok sa zameriava na jednu z najčastejšie napádaných služieb, ktorú mnohé spoločnosti využívajú na správu svojich informačných systémov.

2 Informačná bezpečnosť

V súčasnosti existujú mnohé hrozby pre IT infraštruktúru. Toto správanie prináša zvýšené náklady kvôli opatreniam prijatým pred poškodením údajov alebo nákladom spôsobeným po ňom. Ekonomické škody môže utrpieť akúkoľvek spoločnosť. Podľa časopisu Cybercrime (Morgan, 2019) sa celosvetové výdavky zvýšili z 3,5 miliardy amerických dolárov v roku 2014 na 120 miliárd USD v roku 2017, čo je takmer 35-násobok za 13 rokov. Tieto zahŕňajú trh kybernetickej bezpečnosti ako celok – hardvérové aj softvérové opatrenia. Informačná bezpečnosť je podmnožinou celkového trhu kybernetickej bezpečnosti a jej vlastné náklady dosiahli v roku 2018 114 miliárd USD a predpokladané náklady sú približne 170 miliárd USD. Vyššie uvedené náklady sú len tie, ktoré sa vynakladajú na preventívne opatrenia. Škody spôsobené útokmi sú oveľa vyššie, predpoveď na rok 2026 je takmer 1,2 bilióna USD (Duarte, 2026). Spoločnosti musia investovať do svojej infraštruktúry, ako je špecializovaný hardvér, ktorý by mohol zabrániť narušeniu systémov spoločnosti, zálohovacie systémy a podobne. Po druhé, spoločnosti musia znášať vyššie náklady na bezpečnostné kurzy a školenia zamestnancov, aby si zvýšili svoje skutočné znalosti v oblasti bezpečnosti. Cieľom našej práce bolo zistiť, analyzovať a prijať protiopatrenia na zabránenie akýmkoľvek zisteným škodlivým aktivitám, a tým znížiť riziko straty údajov a s tým spojených zvýšených nákladov.

2.1 Typy útokov a spôsoby narušenia systémov

V praxi existuje niekoľko typov útokov, medzi ktoré patrí phishingový útok, ktorého cieľom je presvedčiť obeť, aby vykonala nejakú akciu, ktorú útočník potrebuje na úspešné preniknutie do systému. Takáto nevedomá spolupráca spočíva napríklad v oklamaní obete, aby spustila prílohu z e-mailu, napríklad falošnú fakturáciu od operátora, keď po spustení obsahu zip archívu boli v počítači zašifrované súbory s najznámejšími príponami a útočník požadoval výkupné za dešifrovanie súborov. Ďalším typom útoku je červ, ktorý prehľadáva napríklad domáce a firemné siete a vyhľadáva zraniteľné služby, ako sú služby zdieľania súborov a podobne. Ďalším typom útoku je útok prostredníctvom verejných Wi-Fi sietí, kde sa útočník môže pokúsiť zachytiť nešifrovanú komunikáciu iných používateľov. Ďalšou populárnou technikou je, keď sú USB kľúče voľne ponechané na rôznych verejných miestach a po vložení do počítača sa môžu pokúsiť ho infikovať a následne zachytiť aktivity používateľa, ako sú stlačenia klávesov, nahrávať obsah obrazovky, zapnúť kameru alebo mikrofón, aby sledovali aktivitu v okolí počítača.

V našom článku sa zameriame iba na sieťové útoky, ktoré sú zamerané na prienik pomocou nástrojov na skenovanie portov a následné testovanie známych mien a hesiel – útoky založené na slovníkoch alebo útoky hrubou silou.

2.2 Infraštruktúra

Naša infraštruktúra, na ktorej sme aktívne monitorovali pokusy o prienik, zahŕňala niekoľko typov serverov, na ktorých boli nainštalované linuxové distribúcie, a to server Ubuntu Linux a server Red Hat Enterprise Linux. Obidva servery slúžia na testovacie účely a majú nakonfigurované iba tie služby a porty, ktoré sú pre danú službu potrebné. Servery sú pravidelne aktualizované, aby bežali na najnovších verziách knižníc. Okrem známych chýb v operačných systémoch a iných softvérových produktoch existujú aj tzv. zero-day zraniteľnosti, kde výrobca softvéru ešte neaktualizoval dotknuté knižnice. Tento typ chýb je pravdepodobne najnebezpečnejší a neexistuje proti nim žiadna účinná ochrana.

Na našej infraštruktúre momentálne beží služba *ssh* (secure shell), ktorá je nevyhnutná pre vzdialenú správu serverov založených na systéme Linux. Okrem toho je webový server Apache (alebo iná alternatíva) nevyhnutný pre spúšťanie webových aplikácií. Webový server Apache nie je jediný produkt, ktorý umožňuje spúšťanie webových aplikácií, ale je jedným z najpoužívanejších. Okrem toho máme v našom prostredí spustený databázový server MySQL. Databázové servery môžu bežať úplne izolovane od internetového prostredia, ale sú nepriamo zraniteľné prostredníctvom tzv. sql-injection útokov, ktoré môže útočník vykonať prostredníctvom aplikácie bežiacej na webovom serveri Apache počas komunikácie s databázovým serverom.

2.3 Secure Shell

Secure Shell (SSH) je kryptografický sieťový protokol na bezpečné pripojenie do vlastnej siete cez nezabezpečené siete, ako je napríklad internet. Medzi typické aplikácie patrí vzdialené prihlásenie cez príkazový riadok a vzdialené vykonávanie príkazov, ale pomocou SSH je možné zabezpečiť akúkoľvek sieťovú službu.

SSH používa kryptografiu s verejným kľúčom na overenie vzdialeného počítača a umožňuje mu overiť používateľa, ak je to potrebné. Existuje niekoľko spôsobov použitia SSH, jedným z nich je použitie automaticky generovaných párov verejného a súkromného kľúča na vytvorenie šifrovaného sieťového pripojenia a následné prihlásenie pomocou overenia heslom alebo certifikátom.

3 Metodika

Na základe prehľadu literatúry sme vybrali niektoré typy útokov, ktoré sa vyskytli najmä na našich operačných systémoch. Analyzovali sme aj škodlivé správanie zaznamenané v systémových protokoloch (logoch). Podľa Pana (Pan et al., 2019) môžu mať útoky výrazne odlišné charakteristiky. Rôzne typy webových útokov, ako napríklad SQL injection, cross-site scripting, zraniteľnosti typu vzdialené spustenie kódu a zahrnutie súborov, používajú rôzne formy útočného vektora a zneužívajú rôzne zraniteľnosti vo webových aplikáciách. Tieto útoky preto často vykazujú úplne odlišné charakteristiky. Napríklad SQL injection sa zameriava na databázy, zatiaľ čo vzdialené spustenie kódu sa zameriava na súborové systémy. Naše úsilie bolo zamerané na predchádzanie útokom primárne na službu *ssh*, pretože sme použili hĺbkovú kontrolu log súborov pred výberom služby, ktorá je najviac zaplavená pokusmi o prienik do systému.

Metodika, ktorú sme v našom modeli použili, bola nasledovná:

1) Manuálna kontrola vybraných log súborov na dennej báze. Log súbory, ktoré sme monitorovali, boli *zabezpečený* log súbor, ktorý sa nachádza v adresári */var/log a access_log* v adresári */var/log/httpd (apache)*. Podľa Pompona a Heatha (Pompon, 2020) patria autentifikačné útoky medzi desať najčastejších útokov na poskytovateľov online služieb. Naše monitorovanie potvrdzuje tento predpoklad a zamerali sme sa na monitorovanie už spomínaného *secure* log súboru;
2) V *secure* log súbore sme použili špecifické techniky na detekciu pokusov s neúspešným prihlásením. Techniky sú podrobnejšie vysvetlené v časti „Výsledky“ v tomto dokumente;
3) Po identifikácii škodlivých IP adries sme prijali protiopatrenia na ich zablokovanie (popísané v časti „Výsledky“);
4) Neskôr sme monitorovali ďalšie neúspešné pokusy o prihlásenie a zároveň sme sledovali, či sa zakázané IP adresy stále pokúšali pripojiť k našim systémom;

5) Pomocou nástroja *whois* sme zistili krajinu pôvodu IP adries;
6) Štatistiky boli vypočítané za obdobie od 10. do 25. marca 2026 (tab. 1).

Pre náš vlastný výskum je potrebné mať server bežiaci na verejnej sieti – internete a povolené protokolovanie udalostí pre konkrétnu službu. Musíme vedieť, ako používať dostupné nástroje tretích strán na analýzu záznamov protokolov alebo ako používať vstavané nástroje operačného systému. Na analýzu sme použili vstavané nástroje operačného systému, pretože sú prítomné v každej inštalácii Linuxu, a preto sú okamžite dostupné.

Systém analýzy protokolov pre použitie v našej práci bol nastavený ako postupnosť krokov, kedy poskytujeme aktuálne aj archivované záznamy z protokolov (Hussain, 2013) na účely spracovania. Ako druhý krok sme pripravili skript, ktorý vykonal analýzu protokolov, výsledkom čoho bola extrakcia údajov, ktoré obsahovali iba neúspešné pokusy o prihlásenie. Keďže protokoly obsahujú stovky až tisíce záznamov o legálnych aj nelegálnych pokusoch o prihlásenie, filtrovanie relevantných údajov bolo nevyhnutným krokom. Keďže novozískané údaje sú tiež vo veľkom množstve – v závislosti od veľkosti protokolových súborov, to môžu byť tisíce riadkov v podľa zvoleného časového rozpätia – je potrebné vykonať dodatočné filtrovanie podľa IP adresy (Schmidt, 2017), kde získame početnosť IP adries, z ktorých boli vykonané pokusy o prienik. Následná analýza určí prvých päť najpočetnejších útokov a z ktorých krajín, respektíve sietí pochádzali. Na určenie poskytovateľa internetových služieb útočiacej IP adresy použijeme nástroj na kontrolu IP adries s názvom *whois* v spojení s nástrojom *nslookup*. Oba nástroje budeme používať podľa potreby, pričom *whois* bude používaný najviac. Po hlavnej analýze vieme určiť, ktoré adresy sú najviac zapojené do aktuálnych pokusov o infiltráciu našej siete, a môžeme správcom siete poskytnúť odporúčania na aktívne opatrenia. Tento nástroj je možné použiť opakovane bez obmedzení, a preto môže poskytovať odporúčania kedykoľvek, ale pre zníženie zaťaženia aktuálneho servera sa odporúča vykonávať analýzu raz denne, alebo vykonávať analýzu offline, teda podľa potreby na inom určenom serveri.

Nástroj v súčasnej fáze vývoja je navrhnutý tak, aby vyhľadával podozrivé IP adresy, z ktorých sa vykonáva vopred definovaný počet pokusov o prienik a po analýze zobrazoval IP adresu správcovi systému. V budúcnosti autor plánuje rozšíriť nástroj aj o aktívne opatrenia vo forme priameho zápisu škodlivých IP adries do súboru /etc/hosts.deny (Bandel, 2000), kde blokujeme možnosť pripojenia k serveru a v našom prípade pôjde o *ssh* službu, ktorá bola spomenutá vo vyššie uvedenom texte.

4 Výsledky

Ako už bolo spomenuté, operačný systém, na ktorom budeme analyzovať protokoly, je Ubuntu Linux verzie 22.04 odvodený od Debian Linuxu a Red Hat Enterprise Linux 8.10, ktorý sám o sebe a jeho deriváty patria medzi najpoužívanejšie operačné systémy v podnikovej oblasti (The Red Hat Enterprise Linux Team, 2018). V tejto verzii Linuxu hľadáme záznamy protokolu v ceste /var/log/ a vyhodnotíme protokoly pokusov o prienik prostredníctvom protokolu *ssh* bežiaceho na porte 22 a názov súboru protokolu je *secure*, úplná cesta k súboru protokolu bude /var/log/secure. V iných operačných systémoch Linux sa používa tiež umiestnenie /var/log/, ale názov súboru protokolu sa môže líšiť a môže sa líšiť aj vnútorná štruktúra týchto súborov protokolu. Napríklad v Ubuntu Linux sa záznamy *ssh* ukladajú do súborov s názvom *auth.log*. Analyzovali sme záznamy od 10. do 25. marca 2026.

Keďže potrebujeme nájsť pokusy o prienik, použijeme nástroje operačného systému, aby sme zistili, či existujú neplatné pokusy o prihlásenie, a spočítame ich počet pomocou iného nástroja operačného systému (nástroj *wc*, ktorý bude spomenutý neskôr). Ako je uvedené v texte vyššie, budeme musieť nastaviť prahovú hodnotu predstavovanú počtom neplatných pokusov o prihlásenie. Pre naše účely zvolíme hodnotu 5 pokusov, pokiaľ sa hodnota neukáže

ako dostačujúca (napríklad legitímny používateľ zabudne heslo a otestuje viaceré svoje heslá na prihlásenie), tak túto prahovú hodnotu upravíme. Na nájdenie neplatných pokusov o prihlásenie použijeme kombináciu príkazov Linuxu v rámci *bash* (Michael, 2011): *cat /var/log/secure | grep - i failed*. Táto kombinácia príkazov zobrazí (cat) obsah súboru a potom vykoná príkaz *grep -i* po príkaze *cat* , ktorý hľadá výskyt slova *failed*. Prepínač *-i* zabezpečuje, že slovo *failed* môže mať aj tvar *Failed*, keďže Linux rozlišuje v príkazoch veľké a malé písmená a aj vo vyhľadávaní. Táto vlastnosť sa všeobecne označuje ako rozlišovanie veľkých a malých písmen (Bresnahan, 2015). V malej ukážke si ukážeme výsledok tejto operácie:

Mar 24 20:41:03 ubuntu-2204-linux sshd[99967]: Failed password for invalid user paula from 220.119.37.141 port 52762 ssh2

Ako je znázornené na vyššie uvedenom príklade, útočník sa pokúsil pripojiť k *ssh* z kórejskej IP adresy 220.119.37.141 s neexistujúcim používateľom *paula*.

V ďalšom príklade vypočítame počet pokusov o prienik pomocou kombinácie príkazov: *cat /var/log/secure | grep -i failed| wc -l* . Táto kombinácia príkazov už nezobrazuje obsah súboru *secure* na obrazovke, ale priamo počíta výskyt riadkov so slovom *failed* v pamäti počítača a na konci operácie uvádza iba počet záznamov. Príkaz *wc* znamená „word count/počet slov“ a prepínač -l spočíta počet riadkov.

4.1 Zablokovanie IP adries útočníkov

Blokovanie adries, ktoré sa pokúšajú pripojiť k nášmu serveru cez *ssh*, je možné vykonať niekoľkými spôsobmi. Pokiaľ ide o podnikovú infraštruktúru, najjednoduchším riešením je požiadať správcu siete o aktiváciu pravidla blokovania na centrálnom firewalle, čo je zariadenie na zabezpečenie bezpečnosti sieťovej prevádzky. Tento prístup je najpoužívanejší, ale pre náš prístup má jednu nevýhodu, ktorou je neustála potreba kontaktovať správcu siete, aby zablokoval alebo odblokoval konkrétnu adresu, ak si to situácia vyžaduje. Ďalšou možnosťou je použiť firewall na našom vlastnom serveri na blokovanie IP adresy. Túto službu poskytuje napríklad utilita *firewall-cmd* (Ellingwood, 2015) alebo aplikácia *ufw* (Krout, 2019). Konfigurácia týchto utilít však vyžaduje určité skúsenosti so správou siete, ako aj znalosť sieťových protokolov, napríklad ktorá služba používa ktorý port (Russel, 2012) a podobne.

Preto použijeme systémovú službu, ktorá nám umožňuje blokovať jednotlivé IP adresy na základe zvolenej služby. Definujeme teda, ktorá služba je blokovaná pre konkrétnu IP adresu, ale ostatné služby nie sú pokryté, ak toto nastavenie nezmeníme. Stručne povedané, ak zablokujeme IP adresu v prístupe k našej *ssh* službe, potom služba *www*, teda služba webového servera, blokovanie neuplatní. Je to preto, že prístup k správe servera (prostredníctvom *ssh*) vykonáva väčšinou niekoľko málo ľudí, ale k webovej prezentácii pristupuje prakticky ktokoľvek z celého sveta, pretože webová prezentácia je určená na verejný prístup. Operačný systém Linux používa na riadenie prístupu k svojim službám dvojicu súborov, a to */etc/hosts.allow* a */etc/hosts.deny*. Súbor *hosts.allow* umožňuje prístup k službe adresám, ktoré sú explicitne definované, pričom je aplikovaný úplný zákaz prístupu a *hosts.deny* má opačný účinok, že všetky IP adresy majú povolený prístup k našej službe okrem tých, ktoré sú definované v tomto súbore. Pre naše účely sme zvolili spôsob, že všetky IP adresy majú prístup k službám nášho servera – v našom prípade k službe *ssh* – okrem tých, ktoré sú explicitne definované v súbore */etc/hosts.deny*. Adresy v tomto súbore majú byť „potrestané“ zákazom prístupu, pretože ich správanie na našom serveri sa vyhodnocuje ako pokus o prienik a nie ako štandardná komunikácia.

Ďalšou výhodou tohto riešenia je, že môžeme deaktivovať celé rozsahy IP adries (Schmidt, 2017), nielen jednu konkrétnu IP adresu. Z našich skúseností vieme, že útočníci používajú tisíce IP adries, takže nie je na škodu zablokovať celý rozsah, najmä ak vieme, že ide o lokality mimo Slovenska. Po vykonaní a uložení záznamu do tohto súboru sa aktivuje blokovanie danej adresy. Adresa je trvalo zablokovaná, kým nie je manuálne vymazaná.

Samozrejme, musíme si dávať pozor, aby sme sa sami neúmyselne nezablokovali, pretože potom je potrebné odblokovať IP adresu buď priamo na fyzickom mieste servera, alebo ho odblokovať z inej neblokovanej IP adresy. Toto platí pre *ssh* službu. Výhodou tohto prístupu je, že aj nie-IT špecialista je schopný tieto zásahy vykonať po krátkom zaškolení. Tu je malý náhľad z /etc/hosts.deny:

sshd: 138.2.76.115, 136.144.244.162, 165.154.6.49, 2.57.122.190, 103.82.27.19, 164.92.143.110, 80.94.95.115, 45.148.10.151, 165., 155., 136., **161.**

Z krátkej ilustrácie je zrejmé, že blokujeme aj konkrétne IP adresy (majú tvar X.Y.Z.W - teda majú štyri oktety (Blank, 2004)) alebo celé rozsahy IP adries, napr. 161 (označené tučným písmom) . To znamená, že žiadna IP adresa začínajúca prvým oktetom 161 sa k našej službe nepripojí. Ktorá služba používa toto aktívne blokovanie, je vyznačené na začiatku blokovaných IP adries, v našom prípade je to *sshd* (tučné), čo znamená *ssh daemon* – služba spomenutá skôr v texte. V tabuľke 1 vidíme z akých krajín boli najčastejšie pokusy o preniknutie do systému. Z tabuľky vidíme, že najviac pokusov bolo z Vietnamu, USA, Austrálie, Holandska a Bangladéša. Z tabuľky ďalej vidíme, že z USA sa najviac pokusov realizovalo z pravdepodobne cloudových služie firmy Oracle, ktorá poskytuje zdarma službu FreeTier, ktorú využívajú pravdepodobne útočníci. Počet pokusov o nelegálny prienik eliminuje aj nástroj *sshguard,* ktorý ale po čase uvoľní zablokované adresy z blokovania a preto trvalé zablokovanie prináša naše riešenie. Bez *sshguard* by boli pokusy o prienik násobne vo väčšom počte. Po aplikovaní našich pravidiel sa pokusy o pripojenie z definovaných IP adries nebudú dať realizovať už nikdy až do vymazania adresy zo zoznamu blokovaných adries.

Ukážme si efekt po aktivácii pravidiel blokovania (príkaz používaný na filtrovanie odmietnutých pripojení *cat /var/log/secure|grep -i refused*). Len za tri dni bolo pozorovaných 206 odmietnutých IP adries, pre ilustráciu ukážeme iba jednu:

Mar 24 21:24:25 ubuntu-2204-linux sshd[100201]: **refused** connect from 103.82.27.19 (103.82.27.19)

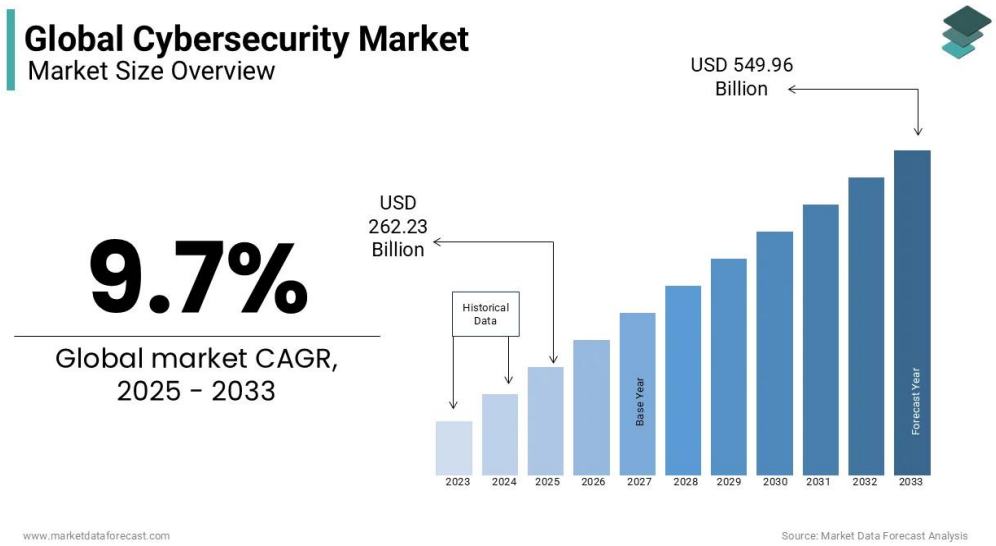
Tab. 1: Počet IP adries podľa krajiny pôvodu útočníka

Štát	IP adresa	Počet útokov
Vietnam	103.82.27.19	53
USA Oracle	152.67.251.120	18
Austrália	163.192.24.247	18
USA Oracle	138.2.76.115	16
USA Oracle	161.153.83.179	14
USA Oracle	152.69.178.152	12
USA Oracle	64.110.67.17	12
Holandsko	45.148.10.121	11
Holandsko	92.118.39.95	11
Bangladéš	103.158.206.141	10

Zdroj: vlastné spracovanie

Podľa spoločnosti Market Data Forecast náklady na kybernetickú bezpečnosť z roka na rok rastú a do budúcna porastú násobne ako je vidieť na obrázku 1.

Obr. 1: Globálne výdavky na kybernetickú bezpečnosť



Zdroj: https://www.marketdataforecast.com/market-reports/cyber-security-market

5 Diskusia

Cieľom našej práce bolo identifikovať IP adresy so škodlivým úmyslom nabúrať sa do online Linux systémov. Na tento účel sme vybrali servery založené na systéme Linux, ktoré sa používajú na testovanie rôznych úloh. Oba servery boli vystavené podobnému typu útokov. Účelom útočníkov bolo zistiť, ktoré služby sú zverejnené v internetovej sieti, a následne prispôsobiť typ útokov. Na našich serveroch je nakonfigurovaná služba World Wide Web (www) (server Apache), služba Secure Shell (ssh) a nepriamo je možné pristupovať aj k databázovému serveru (MySQL). Preto sme v predchádzajúcom texte opísali hlavné typy útokov, ktoré môžeme očakávať. Pozorovaním logovacích súborov sme identifikovali časté pokusy o nabúranie sa do našich systémov prostredníctvom Secure Shell technikou, ktorá môže byť buď slovníkovým útokom, alebo útokom hrubou silou. Prijali sme opatrenia na zastavenie týchto aktivít blokovaním konkrétnej IP adresy alebo celého bloku adries, ak útočník prichádzal z podozrivých IP adries mimo európskych krajín. Náš prístup k bezpečnostným protiopatreniam má hlavný nedostatok v tom, že v našom riešení je používateľovi navždy zakázaný prístup k službe. To môže bežným používateľom spôsobiť problém s prístupom k službe *ssh* z týchto adries, ale dá sa to vyriešiť časovo obmedzeným blokovaním. Používatelia pristupujúci k službe *ssh* sú väčšinou administrátori, takže prístup k tejto službe môže byť zablokovaný pre všetkých mimo povolených IP adries (white list).

6 Záver

Ako sme videli v analýze údajov z reálneho sveta, problém kompromitovania a hackovania systémov je aktuálnejší ako kedykoľvek predtým a dá sa predpokladať, že podobné scenáre sa odohrávajú na všetkých dostupných operačných systémoch na celom internete. Vďaka masívnemu rozsahu internetových útokov vedú k relatívne úspešným prienikom do systémov. Na základe lustrácie verejných databáz (Collins, 2014) je možné zistiť vlastníkov IP adries, ale nie je možné určiť, kto za týmito adresami skutočne stojí. Je zrejmé, že vlastníci týchto adries ich bez spolupráce so štátnymi orgánmi neodhalia.

Samozrejme, na získanie presnejších údajov by bolo užitočné analyzovať záznamy protokolov za obdobie aspoň pol roka a ideálne na aspoň desiatich a viacerých zapojených operačných systémoch. Toto môže byť predmetom budúceho výskumu.

Literatúra

1. Bandel, D. A. (2000). *Linux security toolkit*. Foster City, CA: M & T, IDG. 480 p. ISBN 978-0764546907
2. Blank, A. G. (2004). *TCP/IP foundations. San Francisco*, CA: SYBEX. 304 p. ISBN 0-7821-4370-9
3. Bresnahan, C., Blum, R. (2015). *Linux essentials*. Indianapolis: Sybex. 368 p. ISBN 978-1119092063
4. Collins, M. (2014*). Network security through data analysis: Building situational awareness*. Beijing: O'Reilly. 428 p. ISBN 978-1491962817
5. Duarte, F. (2026, March 10). *Cybercrime cost 2026: $1.2 trillion (& rising).* Programs.com. https://programs.com/resources/cybercrime-cost/
6. Ellingwood, J. (2015, June 18). *How to set up a firewall using Firewall on CentOS 7.* DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-centos-7
7. Hussain, S. (2013, December 17). *How to view and configure Linux logs on Ubuntu and CentOS.* DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-view-and-configure-linux-logs-on-ubuntu-and-centos
8. Krout, E. (2019, October 1). *How to configure a firewall with UFW.* Linode. https://www.linode.com/docs/security/firewalls/configure-firewall-with-ufw/
9. Michael, R. K. (2011). *Mastering Unix shell scripting: Bash, Bourne, and Korn shell scripting for programmers, system administrators, and UNIX gurus* (2nd ed.). Wiley Publishing.
10. Morgan, S. (2019, June 11). *Global cybersecurity spending predicted to exceed $1 trillion The software's ability to detect AI-generated text in student assignments*. https://cybersecurityventures.com/cybersecurity-market-report/
11. Pan, Y., et al. (2019). Detecting web attacks with end-to-end deep learning. *Journal of Internet Services and Applications, 10*(1). https://doi.org/10.1186/s13174-019-0115-x
12. Pompon, R., & Heath, M. (2020, February 6). *Top attacks against service providers 2017–2019.* F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/top-attacks-against-service-providers-2017-2019
13. Russel, J., & Cohn, R. (2012). *List of TCP and UDP port numbers.* Book on Demand.
14. Schmidt, P. (2017). *Základy informačných sietí.* AZ Print.
15. The Red Hat Enterprise Linux Team. (2018, October 3). *Red Hat continues to lead the Linux server market.* Red Hat. https://www.redhat.com/en/blog/red-hat-continues-lead-linux-server-market