Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Komparace nástrojů pro penetrační testování

Matěj Juričič

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Matěj Juričič

Informatika

Název práce

Komparace nástrojů pro penetrační testování

Název anglicky

Comparison of Penetration Testing Tools

Cíle práce

Cílem bakalářské práce bude provedení a vyhodnocení etického hackingu za použití nejpoužívanějších nástrojů pro penetrační testování a porovnání, který z těchto nástrojů je nejvhodnější dle předem daných kritérií. Dále se práce bude zaměřovat na možné kybernetické útoky, které lze těmito nástroji provést a v poslední řadě na ochranu proti těmto útokům anebo možnostem, jak se těmto útokům bránit.

Metodika

Hlavní metodou v teoretické části, bude rešerše informačních zdrojů a k definování základních pojmů bude použita metoda deskripce. Hlavním zdrojem informací budou vědecké, odborné články a knihy zaměřené na toto téma. Teoretická část bude zaměřena také na stanovení hodnotících kritérií nástrojů pro penetrační testování. V praktické části bude proveden výběr a definovány vlastnosti samotných nástrojů pro penetrační testování. Bude provedeno měření a porovnávání nejpoužívanějších nástrojů na penetrační testování, jejich následná analýza a výběr vhodného řešení pro použití v oblasti testování zabezpečení online systémů.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Penetrační testování, etický hacking, kybernetický útok, hacker, kybernetická bezpečnost

---

Doporučené zdroje informací

KOLOUCH, Jan, BAŠTA, Pavel a kol. CYBERSECURITY. Praha : CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8.

MITNICK, Kevin. The art of invisibility. New York : Little, Brown and Company, 2017. ISBN 978-0-316-38049-2.

OCCUPYTHEWEB. LINUX BASICS FOR HACKERS: Getting Started with Networking, Scripting, and Security in Kali. San Francisco : No Starch Press, Inc., 2019. ISBN-13: 978-1-59327-855-7.

SABIH, Zaid . Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing. Birmingham : Packt Publishing Ltd., 2018. ISBN 978-1-78862-205-9.

WEIDMAN, Georgia. Penetration testing: A Hands-On Introducton to hacking. San Francisco : No Starch Press, Inc., 2014. ISBN: 978-1-59327-564-8.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Jana Hřebejková

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 5. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2022

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Komparace nástrojů pro penetrační testování" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2022 _____

Poděkování

Rád bych touto cestou poděkoval paní Ing. Janě Hřebejkové za vzorné vedení bakalářské práce a za všechny rady a připomínky, které mi byly poskytnuty při psaní práce.

Komparace nástrojů pro penetrační testování

Abstrakt

Tato práce se zabývá porovnáním nástrojů pro penetrační testování webů a webových aplikací a problematikou kybernetické bezpečnosti.

Dále je práce zaměřena na stanovení vhodných kritérií na základě, kterých lze určit a vyhodnotit kvalitu nástroje.

Pro demonstraci byl zvolen emulátor VirtualBox, ve kterém je spuštěn operační systém Kali Linux. Zranitelná webová aplikace je DVWA.

Pro testování jsou použity nástroje Burp Suite, Sqlmap, Nmap, John the Ripper, Wireshark a pro samotné porovnání je použita metoda komparativní.

Klíčová slova: penetrační testování, kybernetické útoky, kybernetická bezpečnost, hacking, white hacker, nástroje pro penetrační testování, kritéria.

Comparison of Penetration Testing Tools

Abstract

This thesis deals with the comparison of tools for penetration testing of websites and web applications and the issue of cyber security.

Furthermore, the work is focused on the determination of appropriate criteria on the basis of which the quality of the instrument can be determined and evaluated.

For the demonstration, the VirtualBox emulator was chosen to run the Kali Linux operating system. The vulnerable web application is DVWA.

The tools used for testing are Burp Suite, Sqlmap, Nmap, John the Ripper, Wireshark and for the actual comparison, the comparative method is used.

Keywords: penetration testing, cyber-attacks, cyber security, hacking, white hacker, penetration testing tools, criteria.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V teoretické části jsou definovány pojmy, co je to hacking, a to z pohledu white hat, black hat a také gray hat hackera. Dále je práce zaměřena na penetrační testování, na jeho dělení, metody, fáze a typy.

V další části se práce zaobírá kybernetickou bezpečností, kde je především rozvedeno, jak se chránit proti kybernetickým útokům z pohledu běžného uživatele a jak ochránit firmy proti těmto útokům tohoto typu.

Dále v části o kybernetických útocích jsou rozvedeny nejběžnější útoky, se kterými je možné se setkat a také zaměření na útoky, které se používají při samotném testování.

Následuje část o použitých nástrojích pro penetrační testování, které jsou pak dále použity v praktické části této práce.

A jako poslední část teoretické části je popis a stanovení hodnotících kritérií pro komparaci nástrojů.

V praktické části je rozvedena příprava na samotné testování, která je následována samotnými testy, a to jedny z nejvíce populárními nástroji mezi uživateli, konkrétně Burp Suite, Sqlmap, Nmap. John the Ripper a Wireshark.

Práce je zakončená komparací všech nástrojů a určení, který ze zmiňovaných je nejlepší dle předem stanovených kritérií.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem bakalářské práce je provedení a vyhodnocení etického hackingu za použití nejpoužívanějších nástrojů pro penetrační testování a porovnání, který z těchto nástrojů je nejvhodnější dle předem daných kritérií. Dále se práce zaměřuje na možné kybernetické útoky, které lze těmito nástroji provést a v poslední řadě na ochranu proti těmto útokům anebo možnostem, jak se těmto útokům bránit.

2.2 Metodika

Hlavní metodou v teoretické části, je rešerše informačních zdrojů a k definování základních pojmů je použita metoda deskripce. Hlavním zdrojem informací jsou vědecké, odborné články a knihy zaměřené na toto téma. Teoretická část je také zaměřena na stanovení hodnotících kritérií nástrojů pro penetrační testování. V praktické části je proveden výběr a definovány vlastnosti samotných nástrojů pro penetrační testování. Je provedeno měření a porovnávání nejpoužívanějších nástrojů na penetrační testování, jejich následná analýza a výběr vhodného řešení pro použití v oblasti testování zabezpečení online systémů.

3 Teoretická východiska

3.1 Hacking

Hacking je činnost, jejíž cílem je kompromitovat digitální zařízení, jako jsou počítače, chytré telefony, tablety, a dokonce i celé sítě za účelem získat, změnit data a tomu podobné činnosti, ke kterým hacker nemá přístup. A přestože hacking nemusí být vždy veden se škodlivými úmysly, v dnešní době jej většina odkazů na hacking a hackery charakterizuje jako nezákonnou činnost kyberzločinců - motivovanou finančním ziskem, protestem, shromažďováním informací. (Kovalčík, 2020) (Malwarebytes, 2021)

Samotné hackování je nelegální a trestné. V případě jeho provozování muže dojít i k odnětí svobody na několik let. Po celém světě se nachází velké množství hackerů, kteří jsou schopni docílit nějakých útoků. Proto existují etičtí hackeři nebo také jak se jim říká "pentesteři". Ti používají stejné metody a nástroje jako hackeři, s vy jímkou že mají povolení od majitele systému, do kterého se pokouší dostat a tím odhalit chyby, které mohou uškodit systému ve smyslu ztráty nebo změny dat. Z tohoto důvodu je tato činnost legální, a proto je etický hacking a penetrační testování spojeno s hackingem. (Kovalčík, 2020) (Malwarebytes, 2021)

Existuje několik typů hackerů, ale pro účely této práce budou stačit 3 základní, a to White hat, Black hat a Grey hat. Tyto termíny jsou odvozeny od barevného kódování, které se objevovalo ve westernech z 50. let, kde padouši nosili černé klobouky a ti hodní bílé nebo jiné světlé barvy. (Kaspersky, 2021)

3.1.1 White hat

Tento typ hackera je označovaný jako "etický hacker" anebo také jako "dobrý hacker". Jedná se profesionála s odbornými znalostmi v kybernetické bezpečnosti. Hlavním cílem těchto hackerů je pomoci odhalovat bezpečnostní nedostatky s účelem zamezit dalším útokům, tedy chránit firmu, systém, společnost a další před nebezpečnými hackery, kteří jsou popsáni v následujícím typu pod názvem Black Hat. Využívá své schopnosti k poškození organizace nebo systému, ale v dobrém slova smyslu. Jak bylo již dříve zmíněno toto jsou etičtí hackeři, kteří mají povolení k hackování systému. Často jsou najímány firmami anebo pracují pro vládu v zájmu bezpečnosti. Toto hackování se provádí za účelem otestování úrovně zabezpečení, identifikaci slabin a jejich následné opravení. Provádějí zátěžové testy informačních systémů, dále také provádějí hloubkové skenování sítí na malware a pokoušejí

se nabourat do informačních systémů metodami, které by použili black hat hackeři. A dokonce se snaží oklamat zaměstnance, aby klikali na odkazy, které vedou k napadení malwarem. (Sarangam, 2021) (Kaspersky.com, 2021) (Rafter, 2021)

White hat hackeři jsou tak jedním z důvodů, proč mají velké organizace obvykle méně prostojů a méně problémů se svými webovými stránkami. Většina hackerů ví, že proniknout do systémů spravovaných velkými společnostmi bude těžší než do systémů provozovaných malými firmami, které pravděpodobně nemají prostředky na to, aby prověřily všechny možné bezpečnostní úniky. (Sarangam, 2021) (Kaspersky.com, 2021) (Rafter, 2021)

Podskupinou etických hackerů jsou penetrační testeři neboli "pentesteři", kteří se zaměřují zejména na vyhledávání zranitelností a hodnocení rizik v systémech. (Sobers, 2020)

Z tohoto důvodu je pro každou online firmu velmi důležité, aby zajistila silná preventivní opatření instalací kvalitního zabezpečení proti malwaru, nástrojů pro odstranění spywaru a softwarové obrany firewallu. White hat hacker pracuje dle pravidel a předpisů stanovených vládou. (Sarangam, 2021) (Kaspersky.com, 2021) (Rafter, 2021)

3.1.1.1 Vlivní hackeři typu white hat

Jak již bylo zmíněno, white hat hackeři využívají systémy, aby vylepšili anebo zabránili black hat nebo jiným hackerům do nich vniknout. Níže jsou uvedeni někteří vlivní white hat hackeři. (Sobers, 2020)

Tim Berners-Lee

Berners-Lee, jedno z nejznámějších jmen v oblasti informatiky, je zakladatelem World Wide Webu. Dnes působí jako ředitel konsorcia World Wide Web Consortium (W3C), které dohlíží na vývoj webu. (Sobers, 2020)

Greg Hoglund

Odborník na počítačovou forenziku Hoglund je známý především svou prací a výzkumnými příspěvky v oblasti detekce malwaru, rootkitů a hackování online her. V minulosti pracoval pro americkou vládu a zpravodajskou komunitu. (Sobers, 2020)

Richard M. Stallman

Stallman je zakladatelem projektu GNU, projektu svobodného softwaru, který prosazuje svobodu v oblasti používání počítačů, a je ukázkovým příkladem hackera "správňáka".

Stallman založil hnutí svobodného softwaru v polovině 80. let 20. století s myšlenkou, že počítače mají podporovat spolupráci, nikoli jí bránit. (Sobers, 2020)

Dan Kaminsky

Kaminsky je známou osobností ve světě kybernetické bezpečnosti, je hlavním vědeckým pracovníkem společnosti White Ops, která se zabývá detekcí škodlivého softwaru prostřednictvím JavaScriptu. Nejvíce se proslavil objevem zásadního toku v protokolu DNS (Domain Name System), který by hackerům umožnil provádět rozsáhlé útoky typu cache poisoning. (Sobers, 2020)

Jeff Moss

Etický hacker Jeff Moss byl během vlády Baracka Obamy členem Poradní rady pro vnitřní bezpečnost USA a spolu předsedal pracovní skupině rady pro kybernetické dovednosti. Založil také hackerské konference Black Hat a DEFCON a je komisařem v Globální komisi pro stabilitu kyberprostoru. (Sobers, 2020)

3.1.2 **Black hat**

Black hat hacker je hackerem opačného typu než white hat hacker. Tito hackeři jsou považováni za zločince, kdy všichni mají zlé úmysly. Tito zločinci se snaží nabourávat do počítačových sítí, vypouštět škodlivý software, který může poškodit nebo ničit soubory, držet počítače jako rukojmí a využívat je k další činnosti, krást hesla, čísla kreditních karet a další osobní údaje, které jdou dále využit k případnému vydírání a podobně. (Kaspersky, 2021) (Rafter, 2021)

Tito hackeři pronikají do systémů bez jakéhokoliv povolení. Dále je tato skupina velmi ovlivněna svými znalostmi neboli znalostmi útočníků, protože se zde nachází úplní amatéři, ale i profesionálové. Většinou pracují sami, ale najdou se zde i tací, kteří spolupracují s organizacemi organizovaného zločinu. (Sarangam, 2021) (Kaspersky, 2021) (Rafter, 2021)

Hlavním cílem této skupiny je finanční obnos. Zatím co samotáři se zaměřují na bankovní údaje, finanční prostředky anebo citlivé informace, kterými dále mohou vymáhat danou osobu, tak organizace hackerů, které mohou být najati jednou organizací k poškození té druhé nebo k poškození státu a jiných a připravení je tak danou o zisk, případné cenné údaje a mnoho dalších. (Sarangam, 2021) (Kaspersky, 2021) (Rafter, 2021)

Problém této skupiny zasahuje do globálních měřítek. Problémy pro orgány činné v trestním řízení spočívají v tom, že hackeři často zanechávají málo důkazů, používají počítače nic netušících obětí a překračují hranice více jurisdikcí. Přestože se úřadům někdy podaří odstavit hackerský web v jedné zemi, stejná operace může mít více uzlů v mnoha zemích. (Kaspersky, 2021) (Rafter, 2021)

Obecně lze říct, že hackeři se snaží proniknout do počítačů a sítí z některého ze čtyř důvodů.

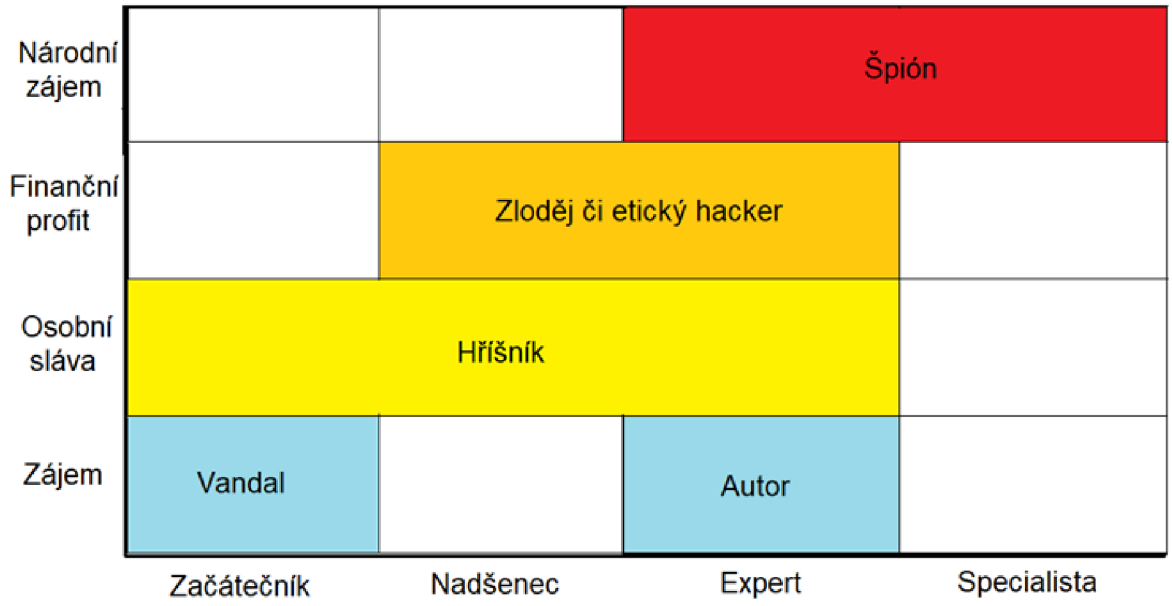
1. Jde o finanční zisk z trestné činnosti, což znamená krádež čísel kreditních karet nebo podvody v bankovních systémech.
2. Dále je pro některé hackery motivací získání kreditu na ulici a vylepšení si pověsti v rámci hackerské subkultury, protože na webových stránkách, které poničí, zanechávají své stopy jako důkaz, že se jim hackerský útok podařil.
3. Pak je tu firemní špionáž, kdy se hackeři jedné společnosti snaží ukrást informace o produktech a službách konkurence, aby získali výhodu na trhu.
4. A jako poslední věc je kdy se celé státy se zapojují do státem sponzorovaných hackerských útoků s cílem ukrást obchodní anebo národní informace, destabilizovat infrastrukturu protivníka nebo dokonce zasít v cílové zemi neshody a zmatek. (Malwarebytes, 2021)

3.1.3 **Grey hat**

Grey hat hacker je někdo, kdo může zneužít morální normy nebo standardy, avšak bez zlovolného účelu. Pohybují na pomezí mezi white hat hackery, kteří pracují ve prospěch těch, kteří udržují bezpečné rámce, a black hat hackery, kteří jednají pomstychtivě a zneužívají slabin v rámcích. Tato skupina hackerů spadá mezi oba předešlé typy. Zde se bere v úvaze záměr hackera, jestli jsou dobré či špatné. (Sarangam, 2021) (wallarm.com, 2021)

Mohou se podílet na činnostech, které se zdají být ne úplně za hranou, ale často pracují ve prospěch všech. Nebo se jedná o hackery, kteří rádi experimentuje se systémy, hledají mezery a obecně je baví prolamovat obranu a hackovat. (Sarangam, 2021) (wallarm.com, 2021) (Rafter, 2021)

Někdy když se jim podaří proniknout do systémů a sítí bez povolení (stejně jako black hat). Ale místo toho, aby páchali něco v rozporu se zákonem, mohou svůj objev oznámit vlastníkovi cíle a nabídnout opravu zranitelnosti za malý poplatek. (Sarangam, 2021) (wallarm.com, 2021) (Malwarebytes, 2021)



Obrázek 1: Rozlišení dle cílů a schopností, (Rafter, 2021)

3.2 Penetrační testování

Penetrační testování neboli také pentesting je legální a autorizovaný pokus o nalezení a úspěšné zneužití počítačových systémů za účelem zvýšení jejich bezpečnosti. Zahrnuje simulaci skutečných útoků s cílem vyhodnotit riziko spojené s potenciálním narušením bezpečnosti. Tento proces dále zahrnuje sondování zranitelností, které mohou být v operačních systémech, službách a aplikacích, nesprávných konfiguracích nebo rizikovém chování koncových uživatelů. Dále také útoky, které mají prokázat, že zranitelnosti jsou skutečné. (Engebretson, 2011) (Weidman, 2014) (HelpSystems, 2021)

Rozsah pentestů se bude u jednotlivých klientů lišit. Někteří klienti budou mít vynikající zabezpečení, zatímco jiní budou mít nebo mají zranitelnosti, které by mohly útočníkům umožnit prolomit perimetr a získat přístup k interním systémům. Někdy může být zapotřebí aby se pentester choval jako Insider neboli zaměstnanec se zlými úmysly anebo také jako útočník, který už dávno pronikl do systému. (Weidman, 2014) (Engebretson, 2011)

Penetrační testování se obvykle provádí pomocí manuálních nebo automatizovaných technologií za účelem systematického ohrožení serverů, koncových bodů, webových aplikací, bezdrátových sítí, síťových zařízení, mobilních zařízení a dalších potenciálních míst ohrožení. (HelpSystems, 2021)

Každé penetrační testování by mělo končit s konkrétním doporučení pro řešení problémů, které se odhalily během testu. Obvykle se tyto informace o všech bezpečnostních zranitelnostech úspěšně zneužitých prostřednictvím penetračních testů předkládají správcům IT a síťových systémů. (Engebretson, 2011) (HelpSystems, 2021)

Jinými slovy se penetrační testování dá popsat jako pokus zjistit, zda se někdo může vloupat třeba do domu, tím že to provedete sami. Celkově se tento proces používá k zabezpečení počítačů a sítí proti budoucím útokům. (Weidman, 2014) (HelpSystems, 2021)

Penetrační testování je také známo pod těmito názvy:

- Pentesting
- PT
- Hacking
- Ethical hacking
- White hat hacking (Engebretson, 2011)

3.2.1 **Dělení penetračních testů**

Podle toho, kde se útočník nachází:

1) Externí

   Tyto testy jsou prováděny z pozice útočníka, který se nachází ve vnější síti neboli na internetu. Během externího penetračního testu se tester pokouší získat přístup do interní sítě s využitím zranitelností objevených na externích prostředcích. (Integra, 2021) (Redlegg Blog, 2019)

   Případně se tester může pokusit získat přístup k privilegovaným datům prostřednictvím externích aktiv, jako jsou e-mail, webové stránky a sdílené soubory. (Redlegg Blog, 2019)

   Během testu tester provádí průzkum vnitřních prostředků a shromažďuje informace o všech prostředcích v rozsahu. Tyto informace zahrnují otevřené porty, zranitelnosti a obecné informace o uživatelích. Jakmile je perimetr úspěšně prolomen, bylo dosaženo cílů externího penetračního testu a tester tak může přejít k internímu penetračnímu testu. (Redlegg Blog, 2019)

2) Interní

   Je prováděno z vnitřní sítě. Tedy například simulují útoky zevnitř firmy. Při tomto testu je nutné si uvědomit že útočník nemusí fyzicky útočit. Může nejprve prolomit vnější ochranu jako firewall, firemní intranet emailový server atd. (Integra, 2021)

   Během interního penetračního testu, tester buď využije zneužitou schránku z externího penetračního testu, anebo použije testovací schránku či notebook uvnitř sítě k provedení hodnocení. Jejich použití je preferovanou metodou, protože se často jedná o stabilnější způsob testování než spouštění nástrojů prostřednictvím zneužitého externího prostředku. (Redlegg Blog, 2019)

   Z tohoto počátečního předmostí je zahájen interní průzkum a útoky. I když špatně zabezpečená kontrola domény může vést k úplné kontrole sítě, většina testů vyžaduje k dosažení cílů testování více cest útoku. Jakmile je dosaženo přístupu správce domény nebo jakmile útočník získá kontrolu nad nejcennějšími informacemi organizace, je test zpravidla ukončen. Tato metoda často zahrnuje zneužití méně důležitých systémů a následné využití informací zjištěných v těchto systémech k útoku na důležitější systémy v síti. (Redlegg Blog, 2019)

Podle způsobu provedení:

1) Manuální testy
   - Manuální testy, jak název napovídá jsou testerem vykonávány manuálně.
   - Mezi výhodami lze klasifikovat možnost vytvořit sofistikované procedury a testy na míru pro specifické podmínky, což třeba zrovna automatické testy někdy nedokážou. Další velkou výhodou manuálních testů je, že je provádí člověk a ten umí popsat, co, jak a proč testuje. Výsledky je schopen interpretovat i nezainteresovaným osobám, které nemají o dané oblasti potřebné znalosti (top management, vedení atd.). (Selecký, 2012)
   - Za nevýhody je možné považovat časovou a znalostní náročnost. Vzhledem k téměř neomezeným možnostem, jak například vytvořit webovou aplikaci, jsou nezbytné rozsáhlé znalosti testované oblasti (HTML, SQL, JavaScript aj.). (Selecký, 2012)
2) Automatizované testy
   - Automatizované testy mají oproti manuálním výhody v rychlosti, možnostech, rozšiřitelnosti podle vlastních potřeb a v relativně jednoduché verifikovatelnosti a reprodukovatelnosti. (Selecký, 2012)
   - Další výhodou je že nástroje byly vytvořeny profesionály, kteří v dané oblasti pracují. (Selecký, 2012)
   - Mezi nevýhody je možné zařadit neschopnost prezentovat výsledky v uživatelsky přívětivé formě či blíže vysvětlit podrobnosti k danému problému. Pro správnou interpretaci jsou opět nutné znalosti o použité aplikaci a testované oblasti. Další nevýhodou je také nemožnost testovat některé typy zranitelných míst. (Selecký, 2012)
3) Semiautomatické testy
   - Poslední třetí způsob provedení jsou semiautomatické testy. Je to kombinace automatických i manuálních testů nebo také kompromis mezi oběma testy. (Selecký, 2012)
   - Je zde snaha o maximální využití výhod obou testů. (Selecký, 2012)

3.2.2 **Metodika penetračního testování**

1) Black-Box testing
    - Objednavatel v tomto případě neposkytne žádné informace nebo informace ve velmi malém množství. Tím pádem testování simuluje útočníka bez jakýchkoliv znalostí. (Selecký, 2012)
    - Tento případ, ale přináší i výhodu, a to je věrná simulace útočníka. Simuluje vnější přístup útočníka, ale nikoliv vnitřní infrastrukturu cíle. Proto se jedná o nejpoužívanější metodu testování. (Selecký, 2012)
    - Funkcionalita pro testera je takzvanou černou skříňkou (anglicky black-box). (Comguard, 2021)
    - Nevýhoda je pak taková že je vyšší pravděpodobnost nenalezení některého z cílů testování. (Comguard, 2021)
2) White-Box testing
    - Zde objednavatel poskytne dostatek informací a podkladů, které jsou během testování použity jako zdroj informací o cílech. (Comguard, 2021)
    - Zároveň tyto podklady mohou sloužit k oponentuře použité topologie z bezpečného pohledu. (Selecký, 2012)
    - Hlavní výhodou je, že znalost všech informací a podkladů jako například kódu nebo infrastruktury sítě, umožní celý test zvládnout během mnohem kratší doby. (Selecký, 2012) (Comguard, 2021)
    - Nevýhodou v případě aplikací je, že tester musí být znalý použitého programovacího jazyka, což vede k větší ceně a vyšší kvalifikaci. (Selecký, 2012) (Comguard, 2021)
3) Grey-Box testing
    - Tato metoda je kombinací obou předchozích, kde se snaží využít obou výhod výše uvedených testů. (Selecký, 2012) (Comguard, 2021)

3.2.3 **Fáze penetračního testování**

Penetrační testování se dělí do několika fází, které jsou rozhodující pro úspěšné naplánování a provedení penetračního testu:

1. Shromažďování informací
2. Modelování hrozeb
3. Analýza zranitelnosti
4. Exploitace
5. Po-exploitace
6. Vytvoření zprávy (Weidman, 2014)

3.2.3.1 Shromažďování informací¨

Před každým testováním je potřeba shromáždit určité množství informací. A pokud se testování provádí s nějakým klientem je potřeba předběžná komunikace. Rozhoduje se jaká metodika bude použita (black-box, white-box, grey-box), cílem je získat co nejvíc informacích je možné. (Weidman, 2014)

Mezi běžné techniky shromažďování informací patří např:

- Dotazy ve vyhledávači
- Vyhledávání názvů domén
- Sociální inženýrství
- Daňové záznamy
- Internet footprinting (emailové adresy, uživatelská jména, sociální sítě a další
- Interní footprinting - prověřování pomocí pingu, skenování portů, reverzní DNS, sniffing paketů.
- Dumpster Diving
- Tailgating (ciphersec, 2020)

3.2.3.2 Modelování hrozeb

Na základě získaných znalostí z přechozí fáze, lze přejít k modelování hrozeb. To spočívá v tom, že se tester snaží uvažovat jako útočník a vytváří plány útoků podle předem získaných informací, kdy tyto informace jsou pak použity pro způsob útoku během penetračního testu. (Weidman, 2014) (ciphersec, 2020)

3.2.3.3 Analýza zranitelnosti

V této fázi se začínají aktivně odhalovat zranitelnosti, aby se zjistilo, jakým způsobem mohou být jejich strategie zneužity. Neúspěšné exploity mohou způsobit zhroucení služeb, spustit výstrahy při detekci narušení a jinak zničit šance na úspěch. (Weidman, 2014)
Během této fáze se často spouštějí skenery zranitelností, které využívají databáze zranitelností a řadu aktivních kontrol k tomu, aby co nejlépe odhadli, které zranitelnosti jsou v systému klienta přítomny. I přestože jsou skenery zranitelností mocnými nástroji, nemohou plně nahradit kritické myšlení, takže se provádí také ruční analýza a ověřují se výsledky i v této fázi. (Weidman, 2014)
Mezi nejčastější oblasti, které pentester mapuje a identifikuje, patří např:

- Obchodní aktiva - identifikace a kategorizace aktiv s vysokou hodnotou
- Údaje o zaměstnancích
- Údaje o zákaznících
- Technická data
- Hrozby - identifikace a kategorizace interních a externích hrozeb.
- Interní hrozby - vedení, zaměstnanci, dodavatelé atd.
- Externí hrozby - porty, síťové protokoly, webové aplikace, síťový provoz atd. (ciphersec, 2020)

3.2.3.4 Exploitace

Zde se spouští exploity proti zranitelnostem, které tester objevil pomocí nástrojů a pokusí se získat přístup do systémů klienta. Cílem etického hackera je přesně zjistit, jak daleko se může dostat, v případě že nemá předem stanovený rozsah, jak daleko muže zajít. Identifikovat cíle s vysokou hodnotou a vyhnout se jakémukoli odhalení. Některé zranitelnosti se mohou pozoruhodně snadno zneužít, například přihlašování pomocí výchozích hesel. (Weidman, 2014) (ciphersec, 2020)
Mezi standardní taktiky zneužití patří např:

- Útoky na webové aplikace
- síťové útoky
- Útoky založené na paměti
- Útoky na Wi-Fi
- Zero-Day Angle

- Fyzické útoky
- Sociální inženýrství (ciphersec, 2020)

3.2.3.5 Po-exploitace

Pokud se proniklo do nezáplatovaného staršího systému, který není součástí domény a tento systém neobsahuje žádné informace, které by útočníka zajímaly, je riziko této zranitelnosti výrazně nižší, než kdyby se podařilo zneužít řadič domény nebo vývojový systém klienta. Při následném zneužití se shromažďují informace o napadeném systému, hledají se zajímavé soubory. Může se například vypisovat hashe hesel, aby se zjistilo, zda je to možné zvrátit nebo použít k přístupu do dalších systémů. Tester se také může pokusit využít zneužitý počítač k útoku na systémy, které nebyly dříve dostupné. (Weidman, 2014)
Po dokončení doporučení pro penetrační testování by měl tester vyčistit prostředí, překonfigurovat všechny přístupy, které získal pro průnik do prostředí, a zabránit budoucímu neoprávněnému přístupu do systému jakýmikoliv prostředky. (ciphersec, 2020)

Mezi typické úklidové činnosti patří např:

- Odstranění všech spustitelných souborů, skriptů a dočasných souborů z napadených systémů.
- Překonfigurování nastavení zpět na původní parametry před pentestem.
- odstranění všech rootkitů nainstalovaných v prostředí
- odstranění všech uživatelských účtů vytvořených pro připojení k napadenému systému (ciphersec, 2020)

3.2.3.6 Vytvoření zprávy

Poslední fází penetračního testování je takzvané reportování. Jedná se o nejkritičtější aspekt pentestu. V této fázi se sděluje zjištění buď se někam zaznamená nebo je sděleno klientovy, kterým je řečeno, co je správně a co nikoliv. Dále v čem potřebují zlepšit svou bezpečnostní pozici, jakým způsobem se tester dostal dovnitř, co zjistil, jak problémy odstranit atd. (Weidman, 2014) (ciphersec, 2020)
Napsat dobrou pentestovou zprávu je umění, jehož zvládnutí vyžaduje praxi, tak aby to pochopil expert i každý jí. Zpráva o pentestu by měla obsahovat shrnutí, tzv. technickou zprávu. (Weidman, 2014)

3.2.4 **Typy penetračních testů**

Aby bylo zajištěno, že pen testy mohou dosáhnout cílů a odhalit slabá místa, existují různé typy pen testů, které se zaměřují na různé oblasti IT infrastruktury:

3.2.4.1 Testy webových aplikací

Penetrační testy webových aplikací prověřují celkové zabezpečení a potenciální rizika webových aplikací, včetně chyb v kódování, porušeného ověřování nebo autorizace a zranitelností typu injection. Tento test využívá strategie útoků v reálném světě k odhalení chyb a slabin způsobených samotnou aplikací a jejím vztahem ke zbytku infrastruktury IT. (HelpSystems, 2021)

3.2.4.2 Testy zabezpečení sítě

Cílem penetračních testů sítě je zabránit škodlivým činům tím, že se najdou slabá místa dříve, než je najdou útočníci. Pentesteři se zaměřují na testování zabezpečení sítí tím, že využívají a odhalují zranitelnosti různých typů sítí, souvisejících zařízení (směrovače a přepínače, a další). Cílem tohoto typu je využít nedostatky v těchto oblastech, jako jsou slabá hesla nebo špatně nakonfigurovaná zařízení. Útok na síť může být zničující, protože aktér hrozby může snadno získat přístup ke každému zařízení v síti. (HelpSystems, 2021)

3.2.4.3 Testy zabezpečení cloudu

S rozvojem cloud computingu organizace rozšířily své možnosti a závislost na cloudových platformách. Přestože cloud nabízí efektivní a škálovatelný způsob poskytování přístupu k firemním datům, v mnoha organizacích se vytvořila slepá místa, pokud jde o zabezpečení cloudu. Výskyt chybných konfigurací a prostých lidských chyb v kombinaci s rostoucími hrozbami ze strany hackerů, kteří hledají zranitelná místa, znamená, že týmy IT bezpečnosti musí pravidelně vyhodnocovat a provádět testování zabezpečení cloudu, aby mohly proaktivně identifikovat a zmírňovat rizika v cloudovém prostředí. (HelpSystems, 2021)

3.2.4.4 Testy zabezpečení internetu věcí

V tomto typu se musí brát v úvaze nuance různých zařízení IoT tím, že se analyzují jednotlivé komponenty a interakce mezi nimi. Pomocí vrstevnaté metodiky, kdy se analyzuje každá vrstva, lze pak odhalit slabá místa, která by jinak mohla zůstat nepovšimnuta. Zařízení IoT jsou nyní všude, a to od zařízení v domácnosti až po zařízení integrovaná do kritické

infrastruktury organizace. Vzhledem k tomu, že mnoho těchto zařízení nemá tradiční operační systémy, není na nich běžně dostupný antivirus, takže jsou obzvláště zranitelná. (HelpSystems, 2021)

3.2.4.5 Sociální inženýrství

Sociální inženýrství je taktikou narušení, která spočívá v použití klamání s cílem získat přístup nebo informace, které mohou být použity ke škodlivým účelům. Nejčastější příklad tohoto postupu je u phishingových podvodů. Phishing se obvykle používá k jednomu účelu. Útočníci se snaží propašovat škodlivý kód přes perimetr. Cíl by mohl obdržet e-mail, který obvykle vypadá, že pochází odněkud nebo od někoho známého. Případně může uživatel obdržet e-mail, který se tváří, jako by pocházel z důvěryhodného místa, které vyžaduje přihlášení, například z banky. (HelpSystems, 2021)

Testování sociálního inženýrství napodobuje takovéto phishingové kampaně, aby bylo možné bezpečně zjistit, zda jsou zaměstnanci zranitelní vůči phishingu a jaké typy phishů je s největší pravděpodobností lze oklamat. Pen testeři by měli vytvořit různorodou kampaň a nasadit e-maily s různým stupněm obtížnosti. Některé mohou být podobné těm, které skutečně používají aktéři hrozeb v přírodě, jiné mohou být pečlivě prozkoumány a vytvořeny tak, aby cílily konkrétně na organizaci nebo osobu. Uživatelům, kteří kliknou nebo zadají přihlašovací údaje, není doručen malware, ale jsou sledováni a případně označeni pro další školení. Díky těmto testů se zaměstnanci stanou prozíravějšími a budou věnovat čas pečlivému prozkoumání e-mailu, než uvěří jeho pravosti. (HelpSystems, 2021)

3.3 Kybernetické útoky

V dnešní době dochází ke stále častějším útokům jak na počítače, tak i software, data či sítě. Útoky jsou stále účinnější a sofistikovanější a představují hrozbu v prostoru informačních sítí. (Kolouch, 2010)

Existují 4 základní skupiny hrozeb:

1. Únik informace – v této hrozbě dojde k vyzrazení chráněné informace
2. Narušení integrity – představuje poškození změnu nebo narušení dat nebo informací
3. Potlačení služby – úmyslné bránění v přístupu k informacím či systému
4. Nelegitimní použití – užití informace neoprávněným subjektem (Kolouch, 2010)

Mezi nejčastější útoky patří:

1. Hacking
2. Cracking
3. Phishing
4. Pharming
5. Racketeering (kybernetické výpalné)
6. Malware
7. SQL injection
8. Man-in-the-middle
9. Odepření služby (Kolouch, 2010)

3.3.1 Cracking

Protože hacking byl již zmíněn na začátku, přejdu hned na druhý a to cracking. Cracking znamená prolamování ochranných prvků systémů a dalších s cílem neoprávněného užití. Cracker zneužívá hackerských metod k obohacení sebe sama. (Kolouch, 2010)

3.3.2 Phishing

Phishing je způsob, jímž se dá spáchat trestný čin podvodu prostřednictvím informačních technologií. U tohoto útoku se útočník snaží získat přístup k peněžním účtům nějakého finančního ústavu, platebním kartám a následně z nich získat peněžní obohacení. Cílem jsou právě klienti, kterým jsou po prolomení a získání informací rozeslány e-maily s kontaktováním klientského centra a po kliknutí na odkaz je klient přesměrován na stejně

vypadající stránku s rozdílem, že už tomu tak není. Zde chtějí většinou přihlašovací údaje + čísla karty a PIN. Tím získají všechny potřebné informace a docílí jejich snažení. (Kolouch, 2010)

3.3.3 **Pharming**

Je sofistikovanější verze phishingu. Jedná se nebezpečnější verzi, kdy jde o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. Dochází k tomu, když se uživatel připojuje. V ten okamžik se totiž připojí na jinou IP adresu, podvrženou. Uživatel se tak dostane na stránku kopírující tu, kam se chtěl prvně dostat. Většinou se opět jedná o nějaké finanční instituce, kdy klient zadá přihlašovací údaje, které jsou pak následně ukradeny. (Kolouch, 2010)

3.3.4 **Racketeering**

V tomto případě se jedná o to, že útočník nějakým způsobem získá citlivá informace uživatele, u kterého se poté snaží vyvolat strach z možné penetrace sytému, zničení, odcizení dat anebo poškození. Zde se opět jedná o trestný čin kdy, ale nedochází k fyzickému kontaktu, proto se stává hůře dohledatelný. Útočník nebo spíše vyděrač využívá především neznalosti uživatele a požaduje za to finanční obnos. (Kolouch, 2010)

3.3.5 **Malware**

Neboli také škodlivý software. Jedná se jednu z nejčastějších hrozeb, který vytvořil nějaký kyberzločinec nebo hacker, s úmyslem narušit nebo poškodit počítač uživatele. Často se šíří prostřednictvím e-mailů nebo souborů ke stažení, které vypadají legitimně. Existuje několik možných typů malwaru a to například: (Kaspersky, 2021)

- Viry
    - Viry, které se vyskytují v různých oblastech
    - Například virus: Samo replikující se program, který se připojí k čistému souboru a šíří se po celém počítačovém systému, přičemž infikuje soubory škodlivým kódem. (Kaspersky, 2021)
- Trojský kůň
    - Jedná se o typ malwaru, který se tváří jako legitimní software
    - Kyberzločinci použijí lsti, aby dostali trojského koně do uživatelova zařízení, kde způsobuje škodu a shromáždí data (Kaspersky, 2021)

- Spyware
    - Program, který tajně zaznamenává, co uživatel na svém zařízení dělá.
    - Kyberzločinci se tak dostanou například údajům o platební kartě nebo jiných důležitých informací (Kaspersky, 2021)
- Ransomware
    - Software, který uzamkne soubory a data některého uživatele, kterým pak následně hrozí jejich smazáním nebo zveřejněním
    - Za vrácení požadují výkupné (Kaspersky, 2021)
- Adware
    - Je reklamní software, který se může použít k šíření škodlivého softwaru (Kaspersky, 2021)
- Botnety
    - Jsou sítě počítačů infikovaných malwarem
    - Kyberzločinci je tak používají k provádění úkolů bez souhlasů uživatelů (Kaspersky, 2021)

3.3.6 **SQL injection**

Typ kybernetického útoku, který slouží převzetí kontroly nad nějakou databází a převzetí tak jejich dat. Kybernetičtí zločinci využívají zranitelnosti v aplikacích založených na datech k vložení škodlivého kódu do databáze prostřednictvím škodlivého příkazu SQL. Tím získají přístup k citlivým informacím obsaženým v databázi. (Kaspersky, 2021)

3.3.7 **Man-in-the-middle**

Typ kybernetické hrozby, při níž útočník zachytí komunikaci mezi dvěma osobami a pokusí se ukrást jejich vzájemná data. Děje se tomu tak v nezabezpečené WiFi síti. Kde je jednoduché komunikaci zachytit. (Kaspersky, 2021)

3.3.8 **Odepření služby**

Nebo anglicky denial-of-service attack. Spočívá v tom, že zločinec zabrání počítačovému systému plnit legitimní požadavky tím, že zahltí sítě a servery provozem. Tím se systém stává nepoužitelným a organizace nemůže vykonávat důležité funkce. (Kaspersky, 2021)

3.4 Kybernetická bezpečnost

Zabývá se, jak už název napovídá ochranou počítačů, serverů, sítí a dalších před kybernetickými útoky. Čemu všemu hrozí riziko prolomení a mělo by být podrobeno penetračnímu testování:

- Veřejné webové stránky
- Interní firemní informace o klientech a zaměstnancích
- E-mailové servery a schránky,
- Přístupová hesla
- Uložiště dat
- FTP servery
- Softwarové aplikace
- Informační systémy (Integra, 2021)

Lze rozdělit do několika společných kategorií:

1. Zabezpečení sítě

   Je postup zabezpečení sítě před jakýmikoliv narušiteli, tedy ať už útočníky nebo malwarem. (Kaspersky, 2021)

2. Zabezpečení aplikací

   Tato kategorie se zaměřuje na ochranu softwaru a zařízení před hrozbami. Napadená aplikace by mohla poskytnout přístup k datům, která v ní mají být chráněna. Správné zabezpečení by mělo být již v rámci návrhu, tedy před tím, než je aplikace vydána. (Kaspersky, 2021)

3. Zabezpečení informací

   Chrání integritu a soukromí dat, a to jak v uložišti, tak při přenosu. (Kaspersky, 2021)

4. Provozní zabezpečení

   Zahrnuje procesy a rozhodnutí pro nakládání s daty a jejich ochranu. Do této oblasti spadají oprávnění, která mají uživatelé při přístupu k síti, a postupy, které určují, jak a kde mohou být data uložena nebo sdílena. (Kaspersky, 2021)

5. Obnova po havárii a kontinuita provozu

   Tato kategorie definuje, jak organizace reagují na incident způsobený kybernetickým útokem, který způsobil například ztrátu provozu nebo dat. Zásady obnovy po havárii určují, jak organizace obnoví své operace a informace, aby se vrátila ke stejné provozní kapacitě jako před událostí. (Kaspersky, 2021)

Kontinuita je pak plán, ke kterému se organizace vrací, když se snaží fungovat bez určitých zdrojů. (Kaspersky, 2021)

6. Vzdělávání koncových uživatelů

   Je jednou z nejdůležitějších kategorií, řeší nejvíce nepředvídatelnější faktor bezpečnosti a to lidi. Například kdokoliv v kterékoliv firmě nebo organizaci může nevědomky přivést nějaký vir do bezpečného systému. Je důležité naučit uživatele mazat podezřelé e-maily, nezapojovat neidentifikované USB disky a jiné jinak důležité lekce o bezpečnosti. (Kaspersky, 2021)

3.4.1 Jak se chránit proti kybernetickým útokům?

Důležitým aspektem v ochraně počítačů, telefonů, tabletů a dalších zařízení je prevence do které se řadí několik následujících bodů:

1. Pravidelná aktualizace softwaru a operačního systému. To znamená používat nejnovější ochrany, i když se zde doporučuje nejprve zjistit, zda tato verze neobsahuje nějaké chyby, které je potřeba stále opravit. (Kaspersky, 2021)
2. Používání antivirového softwaru. Antivirové ochrany odhalí nedostatky v zařízení uživatele a odstraní hrozby. Mnoho ale jejich funkcí je zpoplatněno a takzvaná free verze není dostačující. Proto se doporučuje zvážit koupi nějakého antivirového softwaru. Dále se doporučuje držet software a v nejnovější verzi, tedy ho stále aktualizovat. (Kaspersky, 2021)
3. Používání silných hesel. Hesla uživatele by měla být odlišná a pestrá ve výběru znaků. To znamená velká, malá písmena, čísla a speciální znaky. Čím je heslo složitější, tím je méně pravděpodobné, že útočník prolomí ochranu třeba brute force útokem. V případě že se útočníkovi podaří prolomit heslo uživatele otevírají se další možnosti, jak proniknout do dalších účtů. Proto pokud útočník pronikne do uživatelova emailu má téměř jistotu, že se dostane do dalších účtů uživatele přes možnost „zapomenuté heslo“ (Kaspersky, 2021) (Malwarebytes, 2021)
4. U e-mailů je dobré zkontrolovat odesílatele. Případě pochyby neotvírat přílohu e-mailu, mohlo by se jednat o nebezpečný malware. (Kaspersky, 2021)
5. Spojený s předešlým bodem, tak neklikat ani na odkazy. Zde by se opět mohlo jednat o malware nebo o jeho šíření. (Kaspersky, 2021)
6. Nepoužívat nezabezpečené Wi-fi sítě na veřejných místech. Nezabezpečené sítě činí uživatele zranitelnými vůči útokům typu man-in-the-middle. (Kaspersky, 2021)

7. Bezpečně vyhledávat na internetu. To spočívá v tom vyvarovat se návštěvy nebezpečných webových stránek a nikdy nestahovat neověřené přílohy. (Malwarebytes, 2021)
8. Jako poslední jsou tu aplikace na přenosná zařízení. Uživatel by nikdy neměl stahovat neověřené aplikace. Proto by se mělo stahovat pouze z legitimních tržišť, která si sama hlídají, zda neobsahují škodlivý software, například Google Play a Appstore. Dále se doporučuje i na těchto tržištích zkontrolovat její hodnocení recenze a počet stažení. Při negativním hodnocení nebo špatných recenzí je lepší se aplikaci vyhnout. (Malwarebytes, 2021)

3.4.2 **Jak chránit firmu proti kybernetickým útokům?**

Několik tipů, jak zůstat v bezpečí a ochránit tak organizaci před útoky hackerů

1. Zavedení segmentace sítě. Rozložení dat do menších dílčích sítí snižuje vaše vystavení riziku při útoku. To může pomoci omezit infekci pouze na několik koncových bodů namísto celé infrastruktury. (Malwarebytes, 2021)
2. Uplatňujte princip nejmenších oprávnění (PoLP). To znamená že uživatelům je poskytnuta pouze taková úroveň přístupu, kterou potřebují k výkonu své práce, a nic víc. Minimalizují se tím potenciální škody způsobené útoky ransomwaru. (Malwarebytes, 2021)
3. Záloha všech dat. To platí i pro všechny koncové body v síti a síťové sdílené soubory. Pokud jsou data archivována, je tu možnost vždy infikovaný systém vymazat a obnovit ze zálohy. (Malwarebytes, 2021)
4. Vzdělávat koncové uživatele o tom, jak rozpoznat malspam. Uživatelé by se měli mít na pozoru před nevyžádanými e-maily a přílohami od neznámých odesílatelů. Při manipulaci s přílohami. V dnešních firmách se provádí tajný test, kdy je všem zaměstnancům rozeslán falešný škodlivý email a pozoruje se kolik zaměstnanců na daný odkaz v mailu kliklo. (Malwarebytes, 2021)
5. Důležitým bodem je vzdělávat zaměstnance v oblasti vytváření silných hesel a informovat o možných činnostech, které by mohly vést k útoku. (Malwarebytes, 2021)
6. Více faktorového ověřování (MFA) - minimálně dvou faktorové ověřování. (Malwarebytes, 2021)

7. A jako poslední platí stejně jak u normálních uživatelů neustále aktualizovat svůj software. (Malwarebytes, 2021)

3.5 Nástroje na penetrační testování

Útočníci používají nástroje, aby byly jejich pokusy o narušení úspěšnější. Totéž platí pro pen testery. Software pro penetrační testování je určen k doplnění, nikoliv k nahrazení člověka - umožňuje pen testerům soustředit se na myšlení mimo rámec tím, že přebírá úkoly, které vyžadují čas, ale ne mozkovou kapacitu. Pokud jde o pen testování, nikdy není na výběr mezi nástroji pro penetrační testování a penetračními testery. Místo toho je to volba toho, jaké nástroje penetračního testování pomohou penetračnímu testerovi nejvíce. (HelpSystems, 2021)

3.5.1 Burp Suite

Burp nebo Burp Suite je sada nástrojů pro penetrační testování webových aplikací. Vyvinula ji společnost Portswigger. BurpSuite si klade za cíl být sadou nástrojů typu vše v jednom a jeho možnosti lze rozšířit instalací doplňků. Jedná se o nejoblíbenější nástroj mezi profesionálními výzkumníky zabezpečení webových aplikací a lovci chyb. BurpSuite je k dispozici v edicích: community edition, professional edition a enterprise edition. (awasthi7xenextt, 2019) (Portswigger, 2021)

3.5.2 Aircrack-ng

Sada nástrojů pro do zabezpečení WiFi sítě. Zaměřuje se na různé oblasti zabezpečení WiFi jako například na:

- Monitorování - Zachycení paketů a export dat do textových souborů pro další zpracování nástroji třetích stran.
- Útoky
- Testování – zachycení a injektování, kontrola wifi driverů a jejicj schopností
- Cracking: WEP a WPA PSK (WPA 1 a 2) (aircrack-ng, 2021) (Martin6, 2020)

3.5.3 THC Hydra

Jedná se o paralelní přihlašovací cracker, který podporuje četné protokoly k útoku. Tento nástroj především slouží k výzkumným účelům pracovníků. Ukazuje, jak snadné by bylo se dostat k neoprávněným informacím a získat tak přístup na dálku. (Martin6, 2020)

3.5.4 John the Ripper

Je open source nástroj pro zabezpečení hesel a jejich obnovu. Je dostupný pro mnoho operačních systémů a podporuje stovky typů hashů a šifer. Kombinuje několik režimů prolomení v jednom programu a je plně konfigurovatelný pro potřeby uživatele. (Martin6, 2020) (Openwall, 2021)

3.5.5 . Nmap

Bezplatný a otevřený nástroj pro zjišťování a auditování sítě. Využívá se také pro úkoly jako je inventář sítě správa plánů upgradu služeb a monitorování doby provozu hostitele nebo služby. Využívá IP pakety k určení, kteří hostitelé jsou v síti k dispozici, jaké služby nabízejí, jako operační systémy používají a další. (Martin6, 2020) (Nmap, 2006)

3.5.6 WireShark

Je analyzátorem síťových protokolů. To umožňuje vidět co se děje na mikroskopické úrovni. Jedná se o standart v mnoha průmyslových odvětví. Má bohatou sadu funkcí, která zahrnuje hloubkovou kontrolu stovek protokolů, přičemž je stále více přidáváno. Podporuje také živé zachycení a offline analýzu. (Martin6, 2020) (Wireshark, 2021)

3.5.7 Nikto

Zaměřuje se na shromažďování informací. Provádí komplexní testy webových serverů, kontroluje zastaralé verze a také položky konfigurace serveru, například přítomnost více souborů indexu, možnosti serveru HTTP a pokusí se identifikovat nainstalované webové servery a software. (Martin6, 2020)

3.6 Kritéria komparace

3.6.1 Cena a licence

Mnoho uživatelů a společností klade velký důraz na cenu produktu, proto je to jeden z důležitých faktorů, protože někteří uživatelé nebo společnosti mají stanovené určité náklady, které lze vymezit na tyto nástroje. I nástrojů pro penetrační testování se jejich velký počet vyskytuje v bezplatné verzi neboli také jako open source, a to kolikrát na omezenou časovou dobu, po jejíž uplynutí je uživateli odepřen přístup a je tu nutnost daný nástroj koupit. Jiné jsou už od začátku komerční a je nutnost za ně zaplatit. (Manoj, 2014) (HelpSystems, 2021)

3.6.2 Spolehlivost

Dalším důležitým faktorem je spolehlivost daného nástroje. Zda nástroj plní funkce, které má, popřípadě při jakých obtížích, pokud nějaké nastanou. (Manoj, 2014)

3.6.3 Čas

V této kategorii je důležitý čas, ve kterém nástroj splní svoji funkci. 4as je důležitý pro případy, kdyby se testy nebo skenování opakovalo. Může se totiž stát, že testování bude hardwarově obtížné a mohly tak přetížit nebo poškodit počítač na kterém jsou testy vykonávány. (Manoj, 2014)

3.6.4 Dokumentace

Dokumentace je nedílnou částí správného nástroje, proto je zde důležité, jestli se daná dokumentace vyskytuje, a jak obsáhlá je. Dokumentace je užitečná pro rychlou a efektivní práci. (Manoj, 2014)

3.6.5 Podpora a udržovanost

U těchto nástrojů je velmi důležité, aby byli co nejaktuálnější, protože vývoj dnešních aplikací a technologií jde stále kupředu. Tím pádem se vyskytují nové možnosti, jak dané problémy obejít a objevují si i nové problémy, které lze najít v starších aplikací. Proto je nutné stahovat nebo kupovat aktuální nástroje, které mají stále podporu a vychází na něj pravidelné aktualizace. Pro tuto kategorii je důležité uvádět datum poslední verze nebo stav vývoje. (Manoj, 2014) (HelpSystems, 2021)

3.6.6 **Automatizace**

Bonusem pro daný nástroj může být jeho určitá automatizace. Většinu aplikací je možné spouštět jinými aplikacemi na pravidelné bázi a s různými parametry. U některé nástrojů není potřeba dalších aplikací a mají určitou automatizaci zabudovanou již v sobě. V této kategorii se proto zaměřuje, zda se automatizace vyskytuje a jak se používá. (Manoj, 2014) (HelpSystems, 2021)

3.6.7 **Výstup**

Důležitým faktorem je výstup z daného nástroje. Zda se jedná o adekvátní výsledek či nikoliv. Kolik a co je možné s daným výsledkem dělat a zda se dá použít i dále na další postupy a zda je možná dodatečná manipulace s výsledky (HelpSystems, 2021)

3.6.8 **Přehled všech kritérií**

Název	Popis	Hodnoty
Cena a licence	Zda se u stažení nástroje vyskytuje nějaká cena nebo licence a jaká.	Částka/Zdarma/Cena licence
Spolehlivost	Zda nástroj plní funkce, které má, popřípadě při jakých obtížích.	0-100 %
Čas	Doba, po kterou běží požadovaný test	Čas v sekundách
Dokumentace	Jak kvalitní je dokumentace a jak je popsáno použití nástroje.	ANO - kvalita (výborná, dobrá, dostačující) / NE
Podpora a udržovanost	Zda je nástroj podporovaný a udržovaný a zda se stále pokračuje na jeho vývoji či nikoliv.	ANO - Datum poslední verze/NE - Datum poslední verze
Automatizace	Zda nástroj má možnosti nějaké automatizace, či nikoliv	ANO/NE
Výstup	Použití výsledků.	ANO - formát exportu/NE

Tabulka 1: Přehled všech kritérií

4 Vlastní práce

V teoretické části byly popsány základy o penetračním testování, útoky a ochrana. V praktické části je rozvedena ochrana a provádí se útoky danými nástroji, kde nakonec je vyhodnocení a určení nejvhodnějšího nástroje. Dále v praktické části probíhají testy nejpoužívanějších nástrojů pro penetrační testovaní dostupných z prostředí Kali Linux, respektive výhradně z nástrojů, které jsou již předinstalovaný v samotném operačním systému. Následuje určení, který z těch nejlépe hodnocených je doopravdy ten nejlepší.
Testy se zaměřuje na způsoby získání přihlašovacích údajů různými způsoby a zjišťování zranitelností.

4.1 Testovací prostředí

Samotné penetrační testování je nelegální činnost, a proto se budou používat nástroje, weby a webové aplikace k tomu předem určené, tak aby nedošlo k nezákonné aktivitě. Z důvodu bezpečí mého zařízení jsou všechny testy prováděny ve virtuálním prostředí, tak aby se nedošlo k újmě mého zařízení.

4.1.1 VirtualBox

4.1.1.1 Popis a instalace

VirtualBox je univerzální plnohodnotný virtualizátor pro hardware x86 určený pro použití na serverech, stolních počítačích a vestavěných zařízeních.
Instalace proběhla z oficiální stránky oraclu pro stažení VirtualBoxu. kde jsem stáhl nejnovější verzi 6.1.32, pro Windows.

4.1.2 Kali Linux

4.1.2.1 Popis

Kali Linux je open-source distribuce Linuxu založená na Debianu, která je určena pro různé úkoly v oblasti informační bezpečnosti, jako je penetrační testování, bezpečnostní výzkum, počítačová forenzní analýza a reverzní inženýrství.

4.1.2.2 Instalace

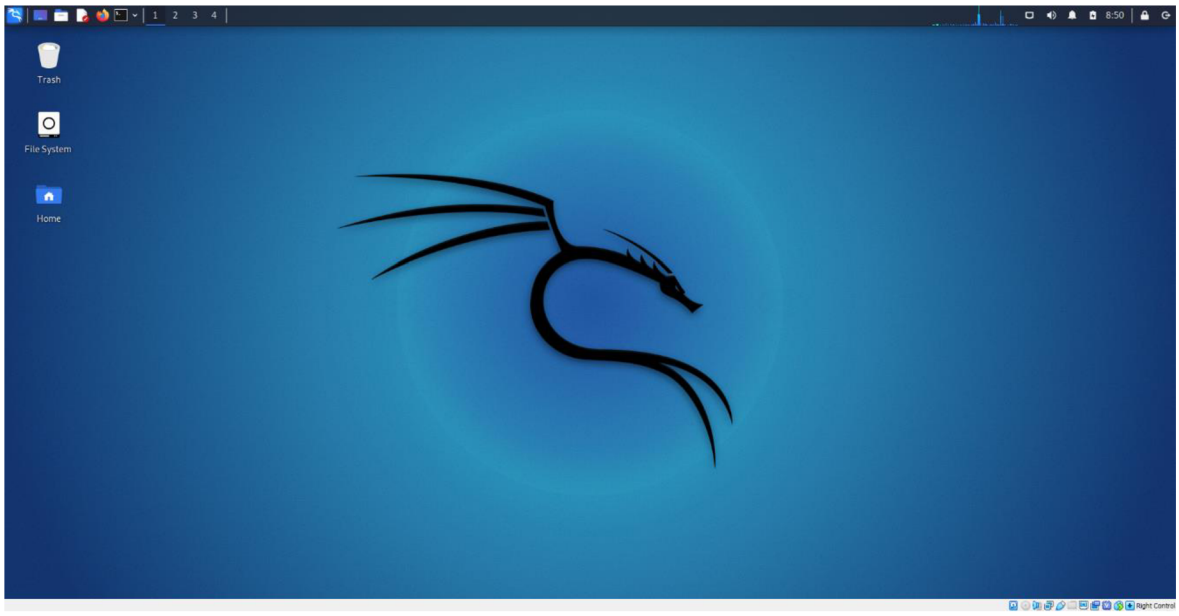
Výběr operačního systému je prostý. Kali Linux je totiž designován na penetrační testování a má tak vše potřebné k této činnosti, včetně předinstalovaných nástrojů. Stažení systému

bylo provedeno z oficiálních stránek Kali pro virtuální prostředí a virtualbox. Následně ve virtualboxu bylo vybráno: Počítač → přidat → a následně vybrán stažený soubor s kali - Kali-Linux-2021.4a-virtualbox-amd64.vbox

Přihlášení:

- Uživatelské jméno: kali
- Heslo: kali

Samotné prostředí po přihlášení vypadá následovně jak je na obrázku 2.



Obrázek 2: Plocha Kali linux, zdroj vlastní

4.1.3 **DVWA**

4.1.3.1 Popis

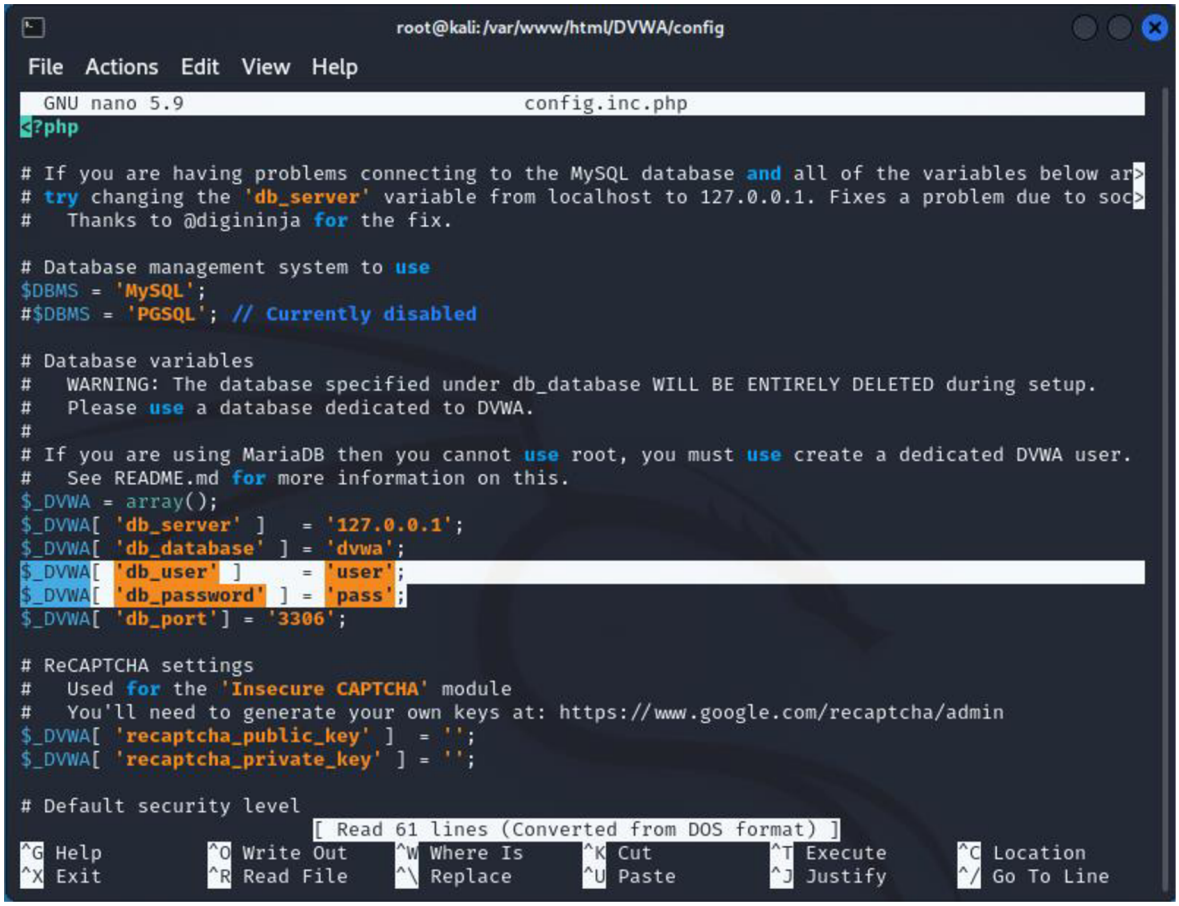
Damn Vulnerable Web App (DVWA) je webová aplikace PHP/MySQL, která je zatraceně zranitelná (Damn Vulnerable). Jejím hlavním cílem je pomoci bezpečnostním profesionálům otestovat své dovednosti a nástroje v legálním prostředí, pomoci webovým vývojářům lépe pochopit procesy zabezpečení webových aplikací a pomoci učitelům a studentům vyučovat a učit se zabezpečením webových aplikací.

4.1.3.2 Instalace a zapínání

V této práci byla nainstalována aplikace DVWA do operačního systému Kali Linux ve VirtualBoxu. Další potřebnou části je databáze a v tomto případě byla vybrána databáze MySQL. Jako poslední je potřeba lokální server, který je v této práci APACHE server.

Postup instalace:

1. Veškerá instalace již nyní probíhá v prostředí Kali Linux. DVWA se stahuje ze stránek GitHubu odkud je zkopírováno url.
2. Instalace pokračuje v terminálu Root Terminal Emulator příkazem: git clone https://github.com/digininja/DVWA.git následuje příkazem chmod -R 777 DVWA pro nastavení práv
3. Jako poslední je třeba nastavit heslo, což se provede příkazem nano config.inc.php kde se změní heslo na jakékoliv možné. V tomto případě na user a pass, jak je zobrazeno na obrázku 3.



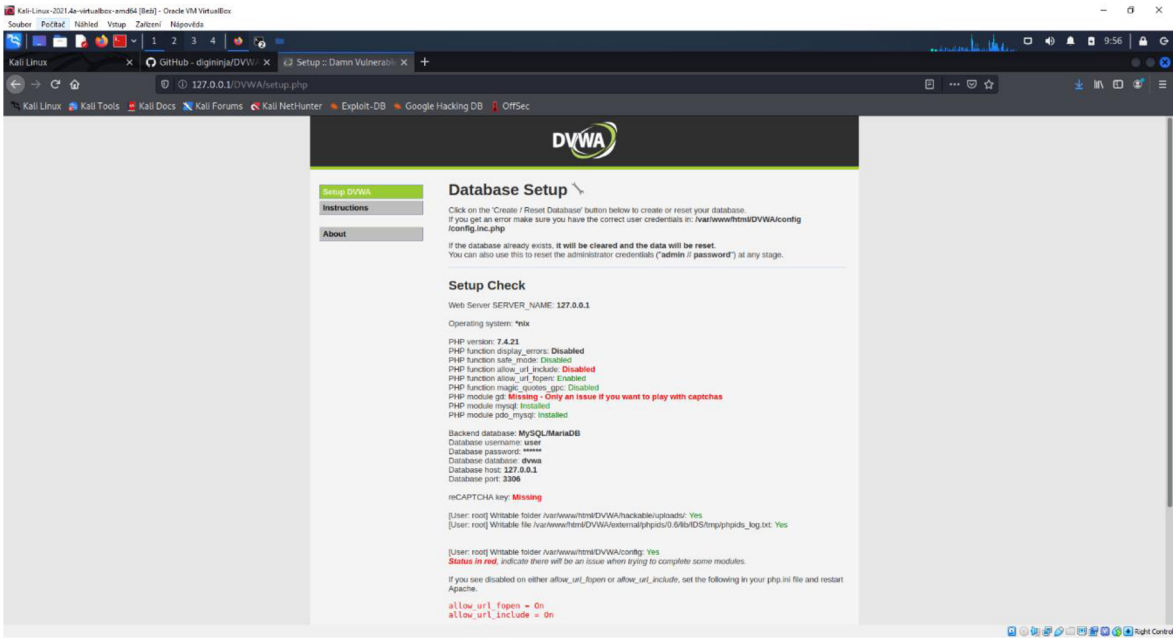
Obrázek 3: Kali - nastavení uživatelského jména a hesla, zdroj vlastní

Dále byla provedena konfigurace mysql, kde se vytvořil uživatel a kde mu jsou dána všechna potřebná práva. Dále byla provedena konfigurace apache serveru, kde bylo potřeba v souboru php.ini povolit url a to allow_url_fopen a allow_url_include.

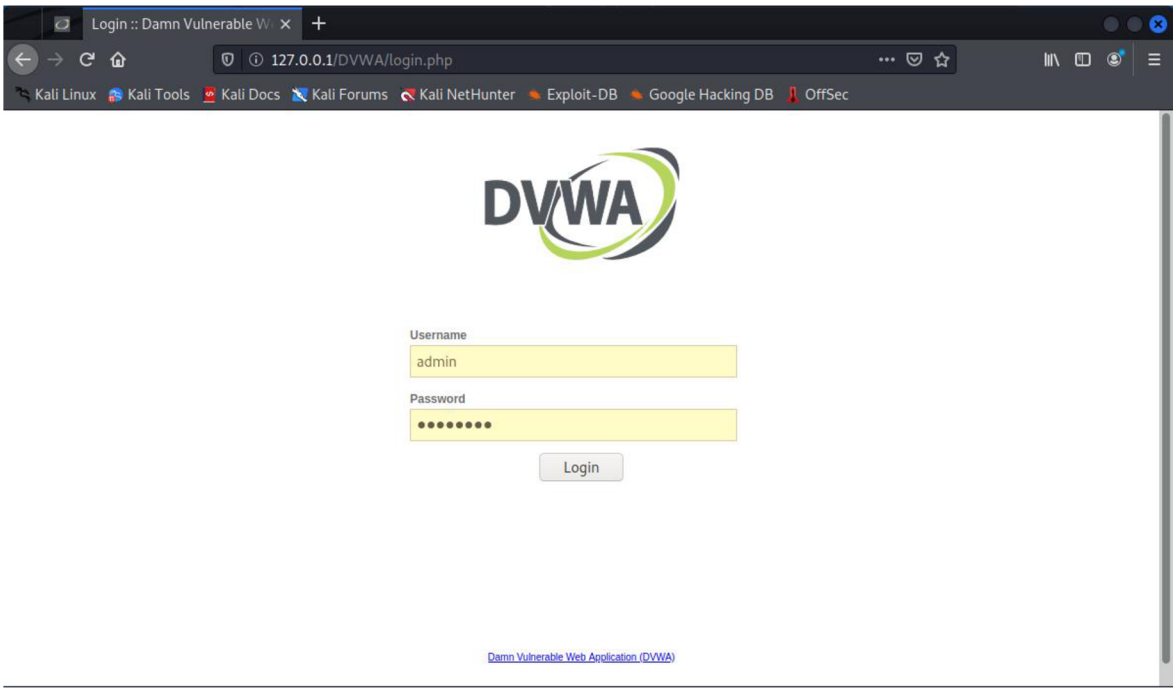
Postup zapnutí:

1. První příkaz: service mysql start
2. Druhý příkaz: service apache2 start

3. Do prohlížeče je zadána adresa 127.0.0.1/DVWA, která po prvním zapnutí přenese uživatele do setupu DVWA jak je na obrázku 4. Po příštím nebo opětovném spuštění je uživatel přesunut již na přihlášení, jak je na obrázku 5., kde přednastavené přihlášení je:
    - Uživatelské jméno: admin
    - Heslo: password

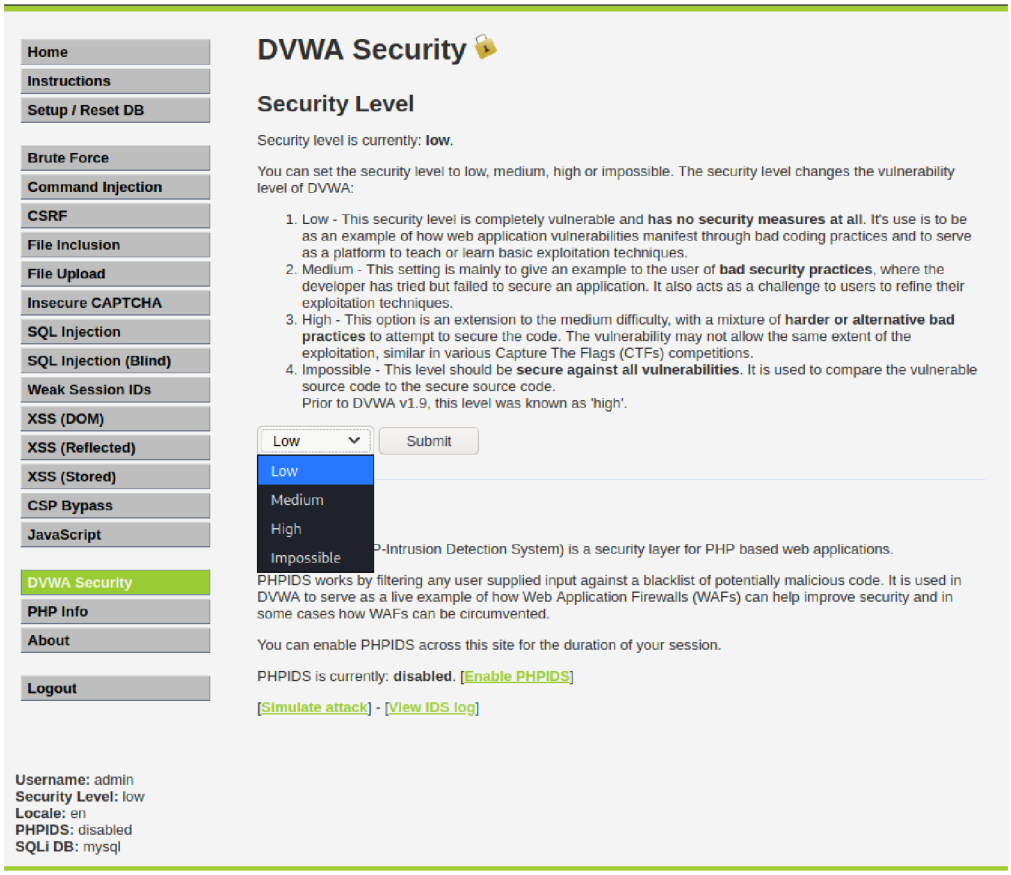


Obrázek 4: DVWA - první zapnutí, zdroj vlastní



Obrázek 5: DVWA - další zapnutí, zdroj vlastní

Po přihlášení je pro účely této práce je zvoleno zabezpečení úrovně low – nízké. Tak aby šlo patřičně otestovat každý nástroje.



Obrázek 6: DVWA - nastavení úrovně zabezpečení, zdroj vlastní

4.2 Průběh testování

V této kapitole je popsáno, jak každý test probíhal včetně postupů a informací o nástrojích. Testované nástroje jsou Burp Suite, Sqlmap, Nmap, John the Ripper, Wireshark.

4.2.1 Burp Suite

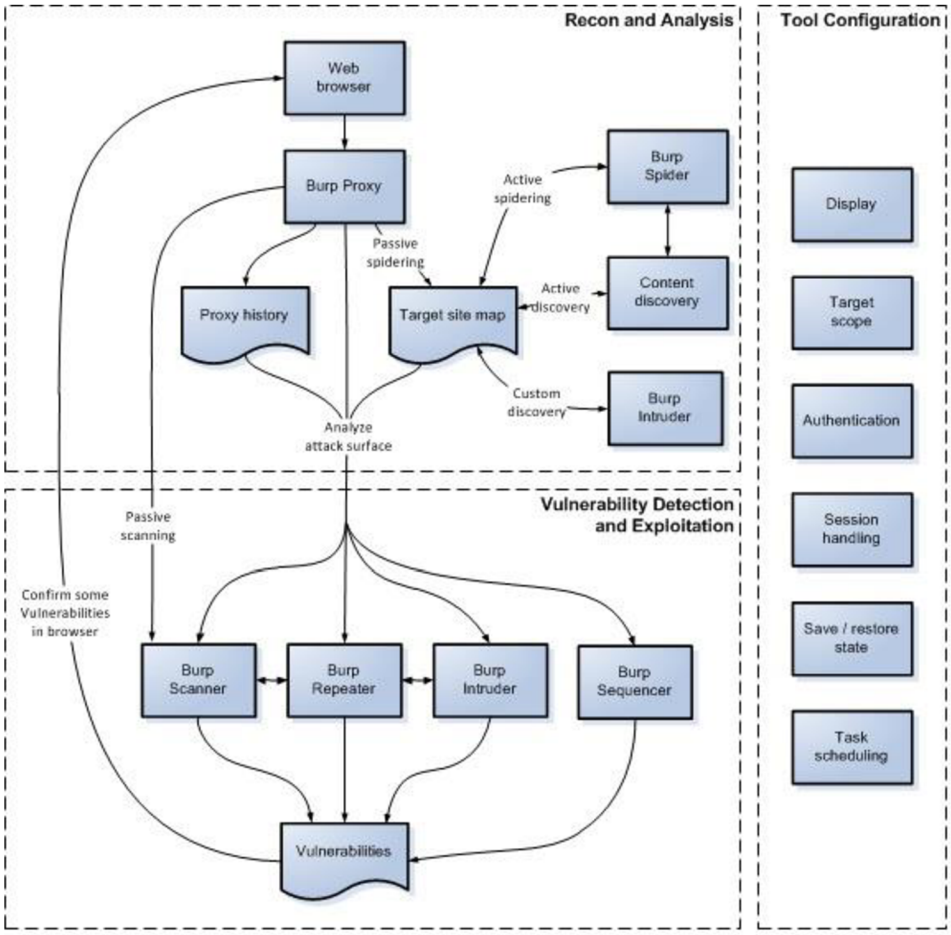
Jedná se jeden z nejpoužívanějších nástrojů a o velice komplexní nástroj, který je rozdělen do několika částí.

- Intruder, ten umožňuje provádět automatizované útoky na míru a provádět nejrůznější testovací úlohy.
- Repeater, který slouží k ruční úpravě a opakovanému zadávání jednotlivých požadavků HTTP.
- Sequencer, ten slouží k analýze kvality náhodnosti v tokenech relací aplikace.

- Decoder umožňuje transformovat bity dat aplikace pomocí běžných schémat kódování a dekódování.
- Comparer, který slouží k vizuálnímu porovnávání bitů dat aplikace s cílem najít zajímavé rozdíly.

V placených verzí profesional a enterprise existují další části jako například scanner, který slouží k automatickému skenování webových stránek na obsah a zranitelnosti zabezpečení. Burp umožňuje efektivně kombinovat manuální a automatizované techniky, poskytuje úplnou kontrolu nad všemi činnostmi, které Burp Suite provádí, a poskytuje podrobné informace a analýzy o testovaných aplikacích.

Schéma uvedené na obrázku 7. představuje přehled klíčových částí pracovního postupu penetračního testování Burp Suite na vysoké úrovni:



Obrázek 7: Burp Suite schéma, (Portswigger, 2021)

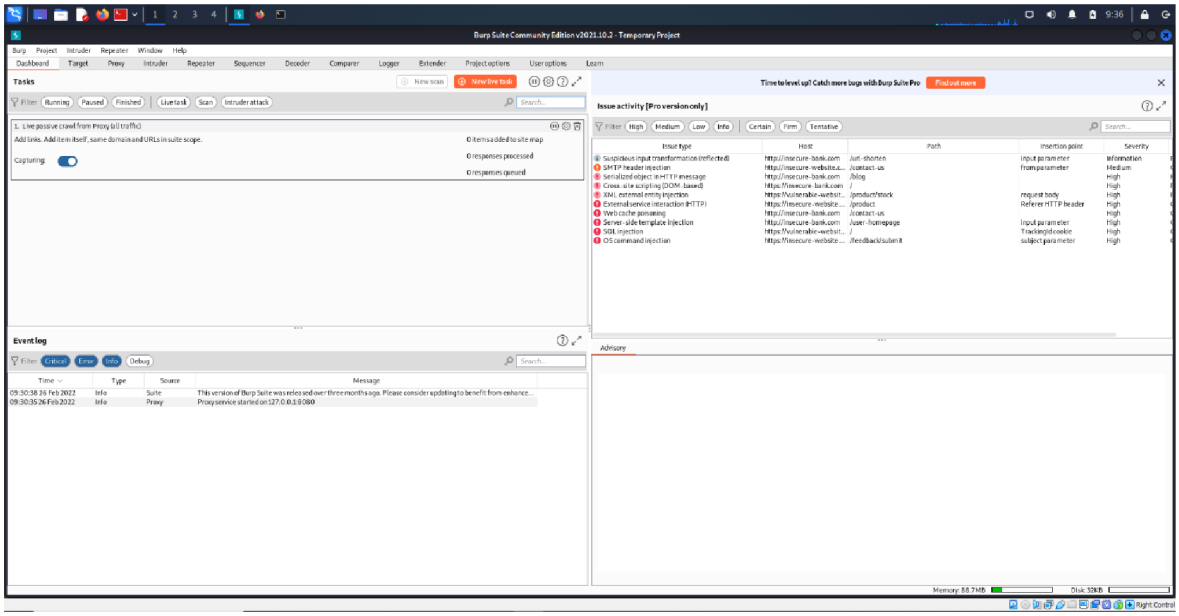
Burpsuite obsahuje obsáhlou dokumentaci která je dostupná na oficiálních stránkách https://portswigger.net/burp/documentation ,kde je volně přístupná ke čtení. Je rozdělena do

několika částí a to především na edice nástroje. Tím pádem kritérium pro podporu a udržovanost splňuje.

Licence a cena se u nástroje Burpsuite rozděluje podle vlastněné edice a to buď:

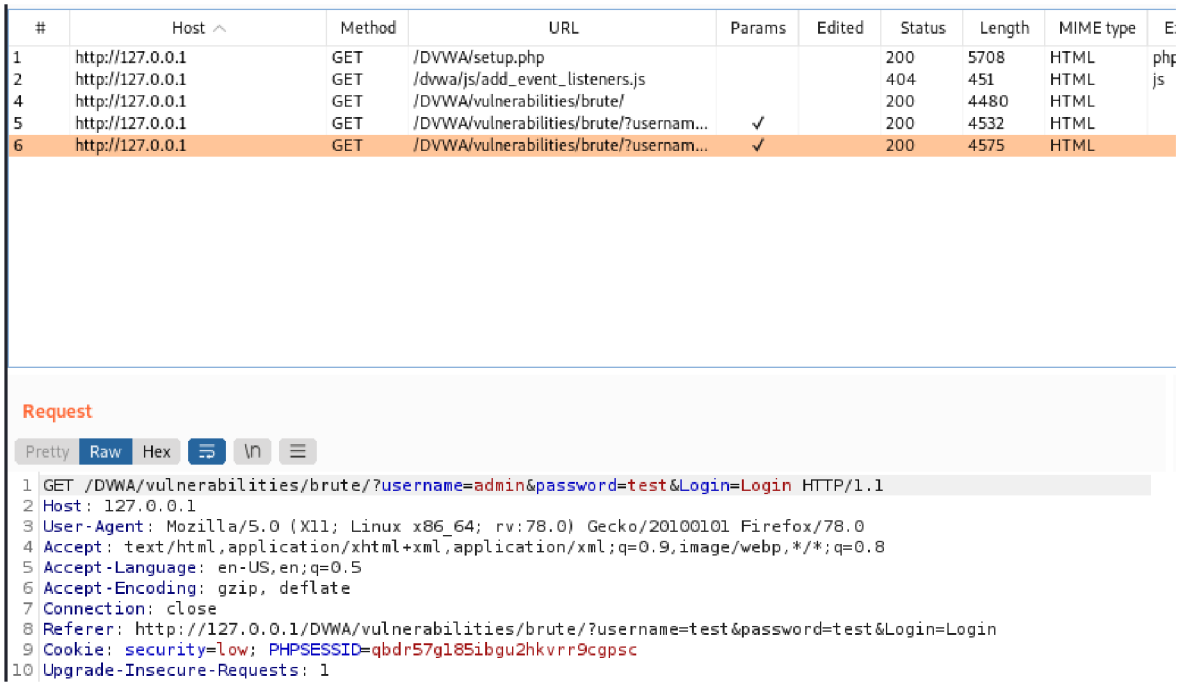
- Commmunity je základní verze volně dostupná a zcela zdarma. Obsahuje základní funkce s možnostmi ručního testování.
- Professional je pokročilejší verze, která je rozšířena o další pokročilejší nástroje, možnosti rozšíření a automatizace. Cena nástroje je staovena na 349€ s možností stáhnutí trial verze zadarmo.
- Enterprise je nejlepší z nich a jeho určení je pro větší společnosti, neboť jeho cena je nejprve rozdělena do tří možností a to dle počtu skenovacích agentů (1 skenovací agent = 1 sken v jeden okamžik):
    - Nejlevnější možnost a to možnost pro 5 je za cenu 6 015€
    - Verze pro 20 je za cenu 12,450€
    - A pro 50+ je cena stanovena na 25,320€

Pro demostraci nástroje je v této verzi jako první možné udělat brute-force attack pomocí části intruder.



Obrázek 8: Burp Suite, zdroj vlastní

Nejprve je potřeba aplikaci DVWA proklikat a udělat jakýkoliv pokus o přihlášení. Tím se v záložce proxy objeví http historie a je potřeba jen vybrat přihlášení, které se pošle do další části intruder.



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	E
1	http://127.0.0.1	GET	/DVWA/setup.php			200	5708	HTML	php
2	http://127.0.0.1	GET	/dvwa/js/add_event_listeners.js			404	451	HTML	js
4	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/			200	4480	HTML	
5	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/?usernam...	✓		200	4532	HTML	
6	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/?usernam...	✓		200	4575	HTML	

Obrázek 9: Burp Suite proxy, zdroj vlastní

V části intruder je potřeba ověřit cíl, následně pozici, na které se bude provádět útok a jako poslední je potřeba vyplnit payload. Tedy to místo odkud se budou brát hesla. Samotný test pak trvá na dle závislosti velikosti payloadu. V práci bylo vybráno 100 nejpoužívanějších dostupných přímo v systému kali linux. Nalezené heslo se dá po skončení nalézt podle velikosti žádosti, protože jako jediná se liší od ostatních svojí délkou, tedy že došlo k nějaké odpovědi, jak je vidět na obrázku 10.

Request	Payload	Status	Error	Timeout	Length	Comment
72	555555	200			4532	
73	liverpool	200			4532	
74	abc	200			4532	
75	whatever	200			4532	
76	11111111	200			4532	
77	102030	200			4532	
78	123123123	200			4532	
79	andrea	200			4532	
80	pepper	200			4532	
81	nicole	200			4532	
82	killer	200			4532	
83	abcdef	200			4532	
84	hannah	200			4532	
85	test	200			4575	
86	alexander	200			4532	
87	andrew	200			4532	
88	222222	200			4532	

Obrázek 10: Burp Suite výsledek, zdroj vlastní

4.2.2 Výsledky nástroje Burb Suite

Název	Hodnoty	Poznámky
Cena a licence	0-25,320€	Cena se odvíjí od verze nástroje
Spolehlivost	100 %	
Čas	4m 56s	Závislý na velikosti paylodu
Dokumentace	Ano - Výborná	
Podpora a udržovanost	Ano, v2021.10.2	
Automatizace	Ano	
Výstup	Ano – html, xml	

Tabulka 2: Výsledky nástroje Burp Suite

4.2.3 Sqlmap

Sqlmap je automatizuje proces detekce a využití chyb SQL injection a převzetí databázových serverů. Je vybaven výkonným detekčním enginem, mnoha výklenkovými funkcemi pro dokonalé penetrační testery a širokou škálou přepínačů. Podporuje velké množství databází jako například MySQL, Oracle, PostgreSQL, Microsoft SQL a spoustu dalších.

Samotný software je zdarma a lze jej šířit anebo upravovat za podmínek GNU General Public License, jak ji vydala Free Software Foundation.

Aplikace je stále udržována. Aktuální a používaná verze při testech je 1.5.11#stable, která byla vydána 3. ledna 2021.

Celá dokumentace je dostupná na stránkách GitHubu na adrese https://github.com/sqlmapproject/sqlmap/wiki/Usage, kde je i nástroj dostupný ke stažení, proto kritérium pro podporu a udržovanost splňuje.

Výstup je během nebo po průběhu testu dostupný na /home/kali/.local/share/sqlmap/output/127.0.0.1 ve formátu .txt a výstupy jsou uloženy v users.csv. Jako výstup dokáže poskytnout získané hashe hesel pro zpracování crackovacími nástroji.

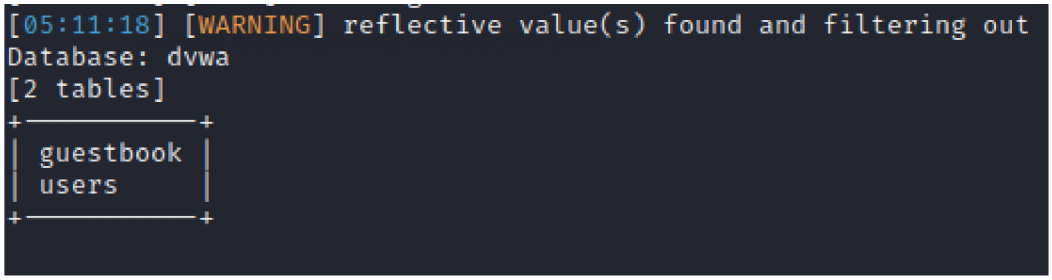
Cílem demonstrace nástroje je cracknout hesla uložené v databázi aplikace DVWA. Sqlmap má přesně stanovené parametry které je nutné dodržet při SQL injection Cíl je uveden parametrem – u, který následuje jeho hodnota – URL. URL musí obsahovat cíl s parametry obsahující možnou zranitelnost (zde je zranitelností id). Následuje parametr session získaný z předešlého nástroje Burpsuite, který umožní přihlášení do aplikace DVWA.

Příkazem:

Sqlmap -u https://127.0.0.1/DVWA/vulnerabilities/sqli/?id=aaa&Submit=Submit# --cookie="security=low; PHPSSESSID=8288m3chbrrrfb7co1tdrdrl9p"

Doplněním o další parametr dbs lze najít databáze v aplikaci, zde je důležitá pouze databáze DVWA. Následujícím příkazem tedy smazáním –dbs a nahrazením -D (Direct) jsou zobrazeny dvě databáze:

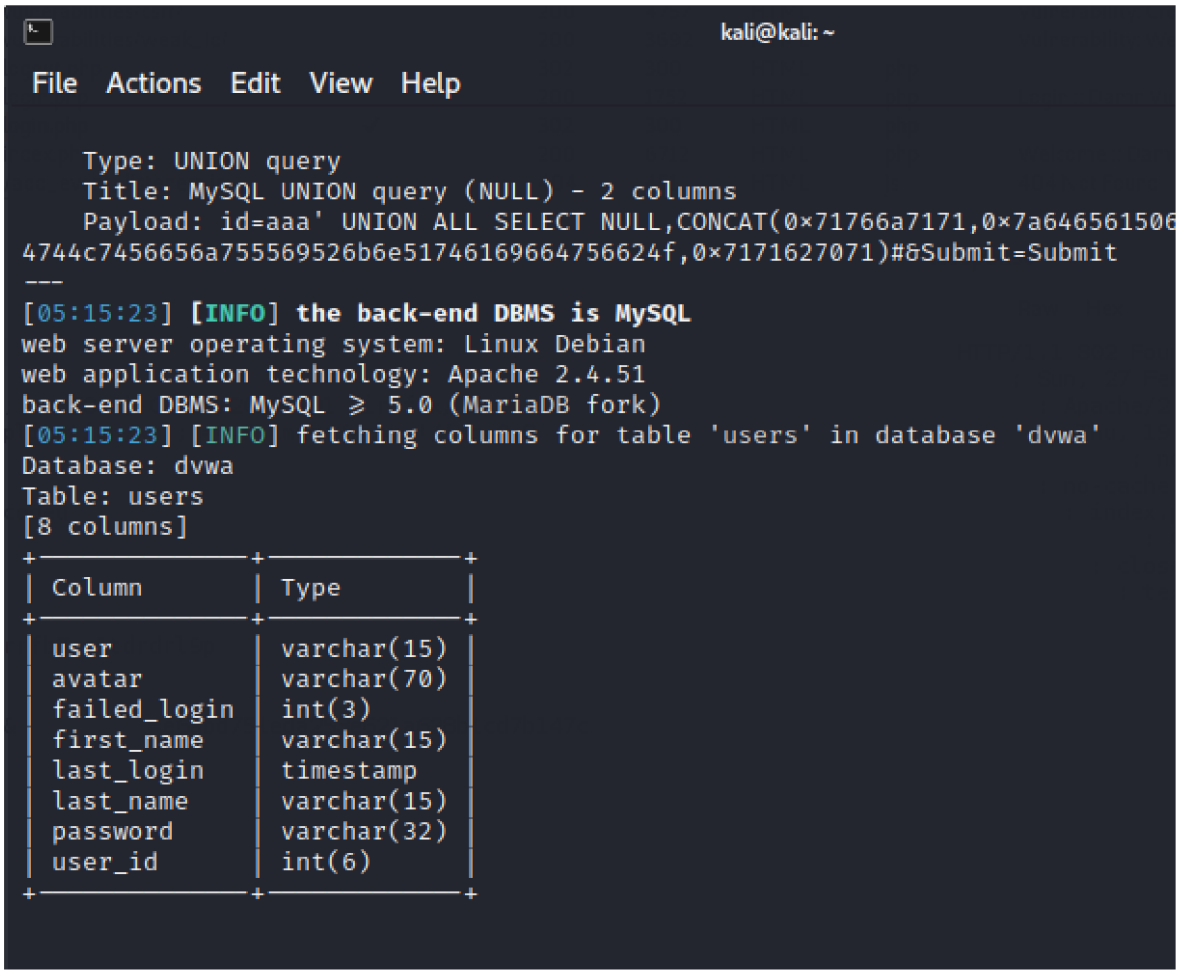
Sqlmap -u https://127.0.0.1/DVWA/vulnerabilities/sqli/?id=aaa&Submit=Submit# --cookie="security=low; PHPSSESSID=8288m3chbrrrfb7co1tdrdrl9p" -D dvwa -tables



Obrázek 11: Sqlmap tables, zdroj vlastní

Následuje příkaz pro databázi users kde se hledají položky user a password:

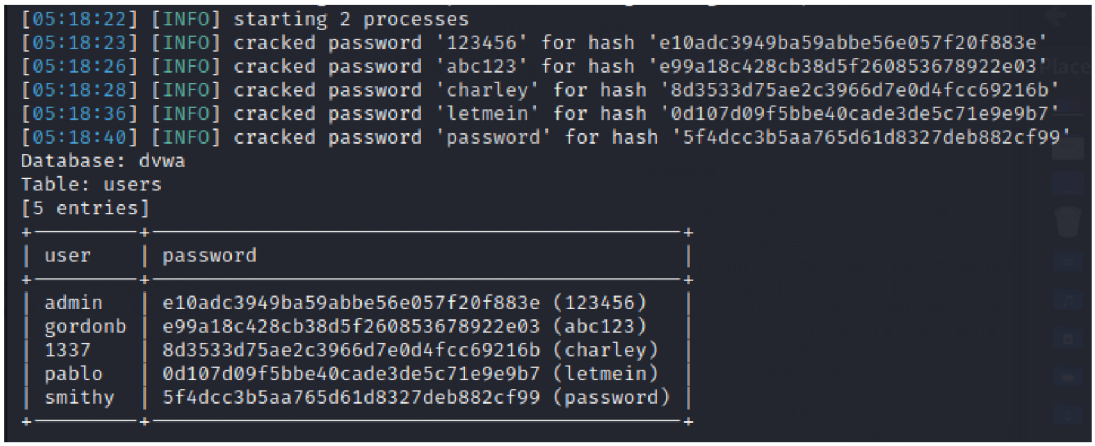
Sqlmap -u https://127.0.0.1/DVWA/vulnerabilities/sqli/?id=aaa&Submit=Submit# --cookie="security=low; PHPSSESSID=8288m3chbrrrfb7co1tdrdrl9p" -D dvwa -T users --columns



Obrázek 12: Sqlmap users, zdroj vlastní

A posledním příkazem došlo ke cracknutí hesel, jak je vidět na obrázku 13.

Sqlmap -u https://127.0.0.1/DVWA/vulnerabilities/sqli/?id=aaa&Submit=Submit# --cookie="security=low; PHPSSESSID=8288m3chbrrrfb7co1tdrdrl9p" -D dvwa -T users -C user,password --dump



Obrázek 13: Sqlmap cracked passwords, zdroj vlastní

4.2.4 **Výsledky nástroje Sqlmap**

Název	Hodnoty	Poznámky
Cena a licence	Zdarma	GNU GPL version 2
Spolehlivost	100 %	
Čas	9 minut 39 sekund	
Dokumentace	Ano - Dobrá	
Podpora a udržovanost	Ano 1.5.11#stable	
Automatizace	Ano	Z příkazového řádku
Výstup	Ano – Plain text	V podobě hashů hesel

Tabulka 3: Výsledky nástroje Sqlmap

4.2.5 **.Nmap**

Nmap je určen pro zjišťování sítě a audit zabezpečení. Mnoho správců systémů a sítí jej také považuje za užitečný pro úkoly, jako je inventarizace sítě, správa plánů aktualizace služeb a sledování provozuschopnosti hostitelů nebo služeb. Nmap využívá surové pakety IP novými způsoby ke zjištění, jací hostitelé jsou v síti k dispozici, jaké služby apod.

Licence a cena nástroje je zdarma. Nmap je distribuován za podmínek Nmap Public Source License. Tato licence je založena na licenci GNU GPLv2, ale obsahuje další důležité podmínky, upřesnění a výjimky.

Nmap obsahuje obsáhlou dokumentaci na stránkách https://nmap.org/docs.html i s možností výběru několika jazyků, nicméně databáze nemá pravidelné aktualizace.

Nástroj je stále podporován a jeho aktuální verze je 7.92 vydaná 7.8.2021 proto kritérium pro podporu a udržovanost splňuje.

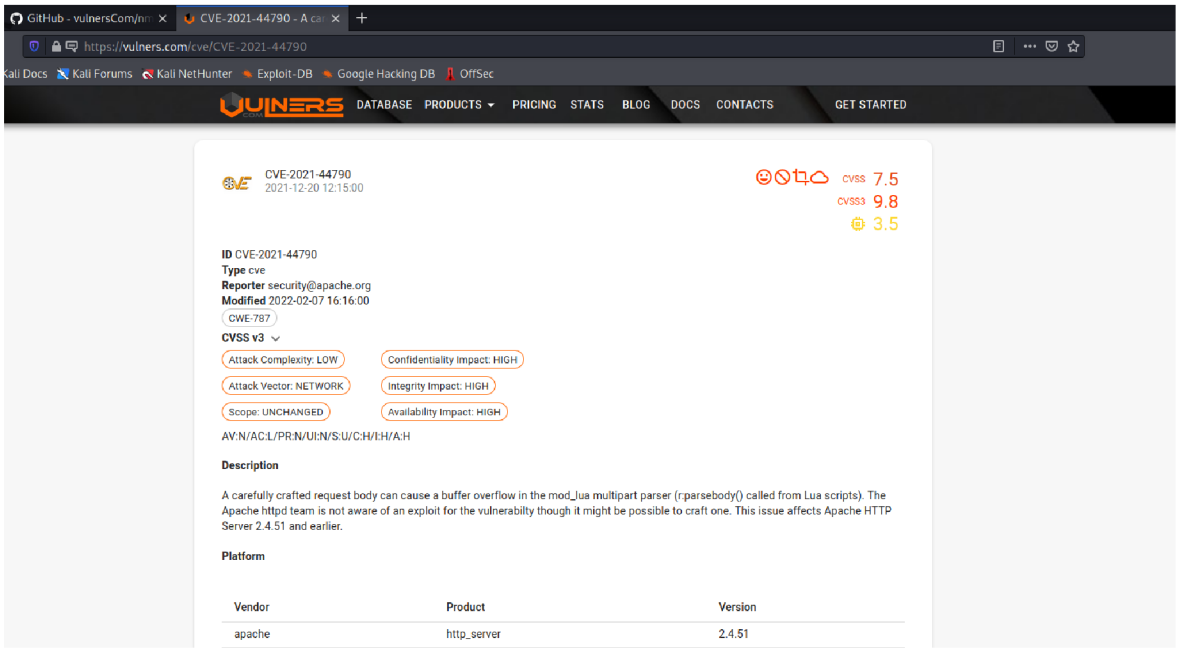
Pro demonstraci testu nástroje je zjištění zranitelností webové aplikace DVWA

Pro zjištění zranileností je použit příkaz: Sudo nmap -sV -p21-8080 --script vulners 127.0.0.1

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 8058 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.51 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.51:
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|_      CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|_http-server-header: Apache/2.4.51 (Debian)
3306/tcp open  mysql   MySQL 5.5.5-10.5.12-MariaDB-1
| vulners:
|   MySQL 5.5.5-10.5.12-MariaDB-1:
|_      NODEJS:602      0.0     https://vulners.com/nodejs/NODEJS:602
```

Obrázek 14: Nmap zranitelnosti

Po skončení testu se objeví všechny nalezené zranitelnosti s určitým skóre zranitelnosti a odkazem na podrobný výpis, jak je znázorněno na obrázku číslo 15.



Obrázek 15: Výsledek zranitelnosti

4.2.6 Výsledky nástroje .Nmap

Název	Hodnoty	Popis
Cena a licence	Zdarma	GNU GPL version 2
Spolehlivost	100 %	
Čas	12 sekund	

Dokumentace	Ano - Dobrá	
Podpora a udržovanost	Ano - 7.92	
Automatizace	Ano	Z příkazového řádku
Výstup	Ano – xml, xsl, xslt, html	Dostupný v několika formátech

Tabulka 4: Výsledky nástroje Nmap

4.2.7 John the Ripper

John the Ripper je rychlý program pro prolamování hesel, který je v současné době k dispozici pro mnoho verzí systémů Unix, MacOS, Windows, DOS, BeOS a OpenVMS. Jeho hlavním účelem je odhalovat slabá hesla Unixu. Kromě několika typů hashů hesel crypt, které se nejčastěji vyskytují v různých systémech Unixu.

Licence tohoto nástroje je zdarma za podmínnek GNU General Public License, které definovala společnost Free Software Foundation. Tato licence neomezuje užívání nástroje, ale říká, jak se zachovat v případě distribuce nástroje, jakým způsobem pracovat s přidáváním úprav nástroje.

Nástroj je momentálně stále udržovaný. Jeho poslední verze je 1.9.0, která byla vydaná 2.11.2021.

Dokumentace nástroje obsáhla a dostupná na adrese https://www.openwall.com/john/doc/

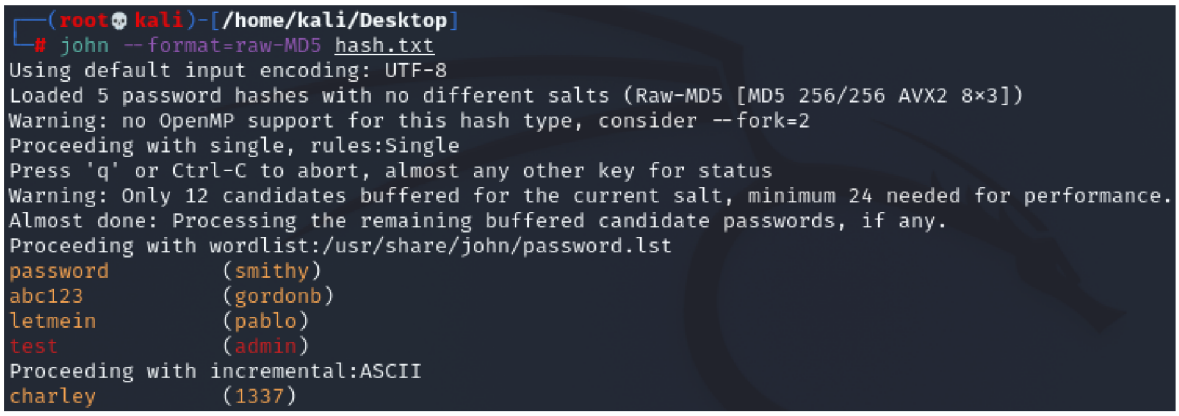
K tomu, aby bylo možné crackovat hesla bylo zapotřebí provést SQL injection. Je tu několik možností, jak ji provést, buď pomocí nějakého dalšího nástroje jako třeba sqlmap použitý výše anebo manuálně. Pro tento nástroj jsem se rozhodl pro manuální možnost, kdy lze danými příkazy, a nakonec finálním příkazem:

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

získat hashe hesel v databázi aplikace DVWA jak je vidět na obrázku 16.

Obrázek 16: Zjištění hashů hesel, zdroj vlastní

Z těch je pak zapotřebí udělat hash soubor s kterým pak příkazem --format=raw-MD5 hash.txt lze cracknout hesla, která jsou vypsána níže na obrázku 17.



Obrázek 17: Cracknutá hesla, zdroj vlastní

4.2.8 Výsledky nástroje John the Ripper

Název	Hodnoty	Poznámky
Cena a licence	Zdarma	GNU GPL version 2
Spolehlivost	70 %	Během testu došlo ke třem potížím, a to především s přetížením RAM
Čas	7 minut 11 sekund	

Dokumentace	Ano – Dostačující	
Podpora a udržovanost	Ano - 1.9.0	
Automatizace	Ne	
Výstup	Ne	

Tabulka 5: Výsledky nástroje John the Ripper

4.2.9 **Wireshark**

Wireshark je celosvětově nejpoužívanějším analyzátorem síťových protokolů. Umožňuje sledovat dění v síti na mikroskopické úrovni.

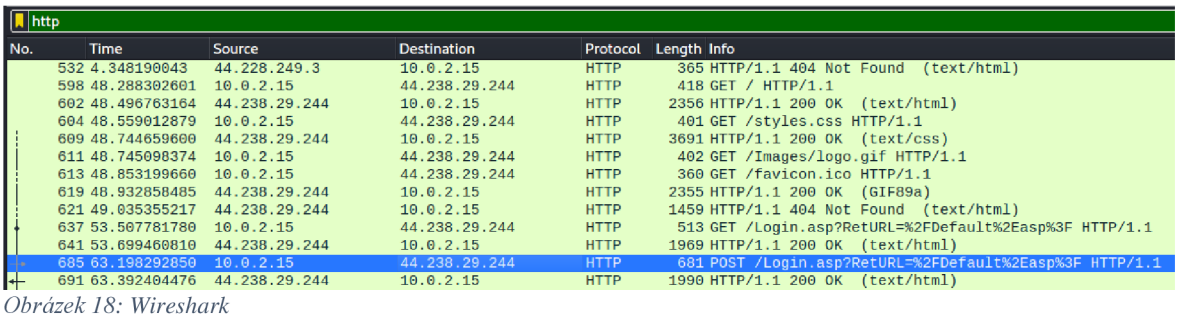
Nástroj je zdarma a lze si jej stáhnout bez placení licenčních poplatků. Licence, pod kterou je Wireshark vydáván, je GNU General Public License verze 2.

Dokumentace včetně dostupných video tutoriálů je dostupná online na webové stránce https://www.wireshark.org/docs/ anebo ke stažení ve formátu ePub a PDF na stejné adrese.

Nástroj je stále udržovaný, verze použitá při testování byla 3.4.9 vydaná 6.10.2021

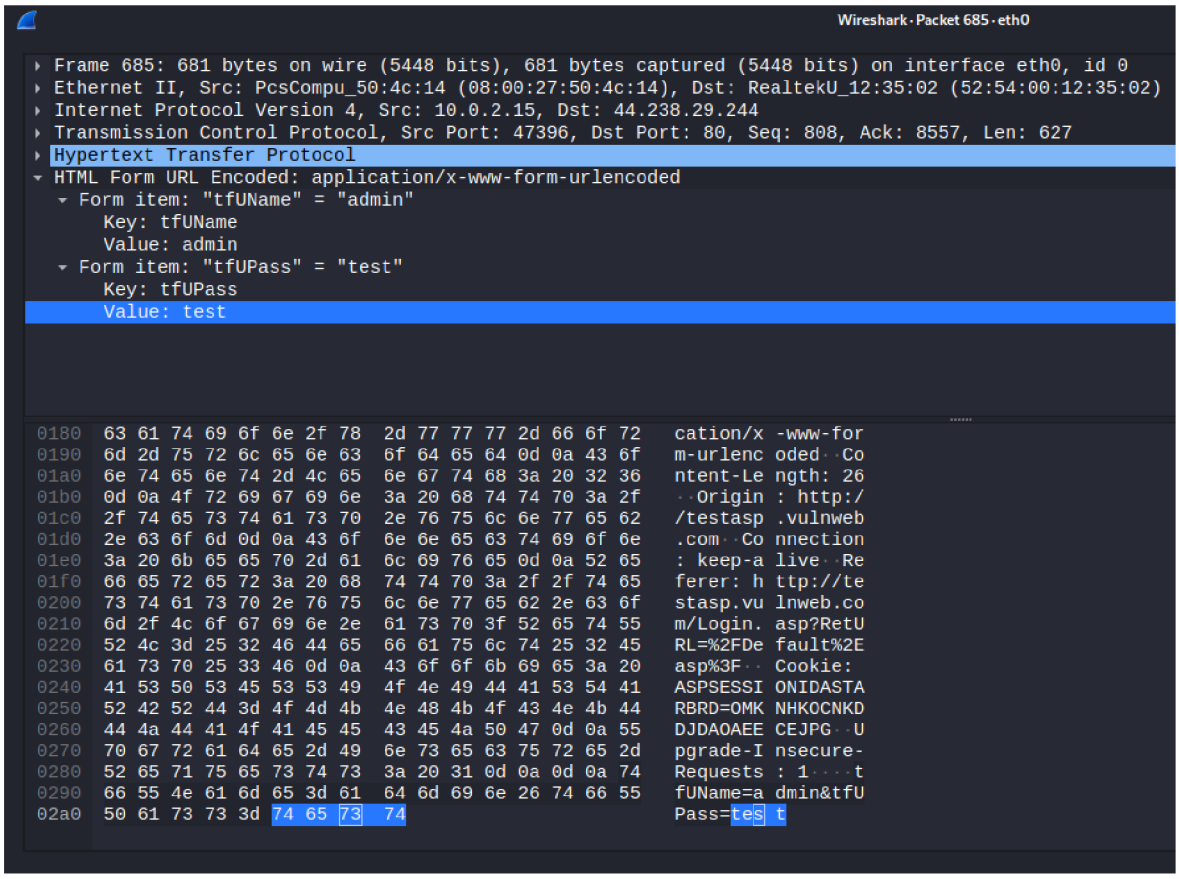
Rozsáhlý výstup výsledku. Export možný do několika různých souborů.

K otestování tohoto nástroje byla použitá webová stránka určená k tomuto testu dostupná na adrese: http://testasp.vulnweb.com/ . Wireshark má své vlastní rozhraní a po zapnutí začne snímat jakoukoliv aktivitu. K zjištění přihlašovacích údajů byl použit sniffing, již dříve zmiňovaný v kapitole o kybernetických útocích. Po pokusu o přihlášení je v programu zachyceno samotné přihlašovaní. Pro rychlejší nalezení lze vyfiltrovat výsledky pouze na protokol http, kde pak následně vyhledat přihlášení, jak je vidět na obrázku číslo 18.



Obrázek 18: Wireshark

Po patřičném prozkoumání, lze nalézt samotné přihlášení v části „hypertext transfer protocol“, jak je vidět na obrázku 19.



Obrázek 19: Wireshark výsledek, zdroj vlastní

4.2.10 **Výsledky nástroje Wireshark**

Název	Hodnoty	Poznámky
Cena a licence	Zdarma	GNU GPL version 2
Spolehlivost	100%	
Čas	1 minuta 14 sekund	
Dokumentace	Ano - Výborná	
Podpora a udržovanost	Ano - 3.4.9	
Automatizace	Ano	
Výstup	Ano - Plain text, csv, json	

Tabulka 6: Výsledky nástroje Wireshark

5 Výsledky a diskuse

5.1 Souhrnné vyhodnocení dle kategorií

V této kapitole je nejprve vyhodnocení nástrojů v daných kritérií a následně celkové vyhodnocení dle všech kritérií.

5.1.1 Cena a licence

Nástroje Sqlmap, Nmap, John the Ripper a Wireshark jsou zdarma s omezením distribuce a všechny zmíněné jsou licencovány pod licencí GNU General Public licence verze 2. Nástroj Burp Suite je komerční produkt s minimálně ročním licencování a jeho cena se pohybuje v rozmezí od 0 do 25 320 € dle verze.

5.1.2 Spolehlivost

Všechny nástroje dosáhly ve finále výsledku, kterých jejich demonstrace měla dosáhnout, nicméně s nástrojem John the Ripper docházelo k zatížení procesoru na maximum a dostával se do fáze nečinnosti a nutného restartu.

5.1.3 Čas

Zde je potřeba rozdělit nástroje na 2 skupiny, a to na komplexnější nástroje Burp Suite a wireshark a pan na ty ostatní. Čas Wireshraku je o pár minut rychlejší, ale musí se brát v potaz, že stojí na sniffingu bez kterého by nedošlo k úspěšnému zjištění.

5.1.4 Dokumentace

Dokumentace u všech nástrojů byla velmi důležitá při práci s aplikaci DVWA a byla tak její nedílnou součástí. U nástroje John the Ripper, sqlmap a nmap dokumentace obsahovala popisovala základní funkcionality a došlo i na chvíle kdy byla potřeba některé informace dohledávat. Naproti tomu Burp Suite a Wireshark mají dokumentace o něco lepší, protože se jedná o mnohem komplexnější nástroje a jejich přítomnost je potřeba. Proto mají oba nástroje dokumentace zakomponované již ve svých aplikacích.

5.1.5 Podpora a udržovanost

K období, kdy probíhali testy byly všechny nástroje stále podporované. U většiny nástrojů je patrná s porovnáním předešlých verzí pouhá udržovanost bez nějaké inovace nebo nových

funkcí. Namísto toho nástroj Burp Suite se v pohledu zpět na předchozí verze mění a přidává nové funkce. To ale může být k neprospěchu, protože v případě placeného nástroje jako je Burp Suite dochází k ochuzení o některé funkce u verzi zdarma. I přes to se Burp Suite jeví jako ta nejlepší možnost

5.1.6 **Výstup**

Export výsledků je možný u všech kromě až na nástroj John the Ripper, kdy se jedná o jednoduchý nástroj a je zde pochopitelné jeho absence. U ostatních nástrojů je export možný v několika formátech.

5.2 Vyhodnocení

Při porovnání všech kategorií, které jsou vidět v tabulce x. Vyhodnocení všech nástrojů, si vedly nejlépe nástroje Burp Suite a Wireshark, kde oba nástroje jsou velmi podrobné, mají své vlastní rozhraní, mnoho dalších funkcí a velmi dobře zpracovanou dokumentaci. Nicméně při porovnání všech jejich možností, funkcí a vzaní v potaz ostatní verze Burp Suite i přes jejich ohromné ceny, Burp Suite svojí komplexitou převyšuje Wireshark a jedná se o nejlepší nástroj, který v této práci byl otestován.

V průběhu práce došlo i na testy dalších nástrojů, a to nástroj THC Hydra a Nikto. Nicméně u prvního zmíněného nebylo možné test dokončit z důvodu zahlcení procesoru i v momentech jednoho dotazu. Nejspíše se jednalo o možný bug, který souvisel s nainstalovanou verzí v operačním systému Kali linux. Z toho důvodu byly z práce vyloučeny a nebyly porovnávány.

Jako další tu jsou menší nástroje, kdy nejhůře z nich si vedl John the Ripper z důvodu menších obtíží při testování. I přes to se jedná o velmi dobrý a účinný nástroj, který je velmi oblíbený u ostatních uživatelů, ale je vhodný pro menší manuální testy.

Následuje Nmap, který není určen pro zjišťování přihlašovacích údajů ale pro nalezení zranitelnosti. I přes to si vedl velmi dobře a je dobrý pro menší testy na zjišťování zranitelností.

A jako poslední je Sqlmap, který by se v případě zařazení zařadil na třetí místo. Je podobný nástroji Burp Suite, je zdarma a jeho funkce se zaměřené na zranitelnosti. Nástroj je výborný a na 100 % plní svojí funkci, ale určitými vlastnostmi zaostává. I přes to se jedná o dobrý nástroj pro manuální testy.

	Cena a licence	Spolehlivost	Čas	Dokumentace	Podpora a udržovanost	Auto.	Výstup
Burpsuite	0-25 120€	100 %	4m 56s	Výborná	Ano	Ano	Ano
Sqlmap	Zdarma	100 %	9m 39s	Dobrá	Ano	Ano	Ano
Nmap	Zdarma	100 %	14s	Dobrá	Ano	Ano	Ano
John the Ripper	Zdarma	70 %	7m 11s	Dostačující	Ano	Ne	Ne
Wireshark	Zdarma	100 %	1m 14s	Výborná	Ano	Ano	Ano

Tabulka 7: Vyhodnocení nástrojů

6 Závěr

Obsahem práce bylo vyhodnocení několika nejlépe hodnocených nástrojů pro penetrační testování mezi uživateli dle kritérií, které byly v práci vybrány a definovány.

V teoretické části bylo definováno, co je to hacking, jeho důležité aspekty jako například white hat, black hat hacker. Dále pak bylo definováno samotné penetrační testování jeho dělení, metodika, fáze a typy. Pokračovalo se kybernetickými útoky, a to se zaměřením na ty nejběžnější s daným důrazem na útoky použité při testování. Útoky byly následovány kybernetickou bezpečností, kde bylo popsána ochrana jak pro běžné uživatele, tak i pro společnosti.

Dále se práce zaměřila na analýzu nástrojů pro penetrační testování, které byly použity pro zhotovení praktické části. A jako poslední došlo na stanovení hodnotících kritérií, které byly vytvořeny na základě použitých publikací.

V praktické části bylo vytvořeno prostředí pro bezpečné testování a popsána aplikace DVWA a operační systém Kali linux, aby v případě potřeby bylo možné toto prostředí znovu vytvořit.

Dále byly popsány demonstrace samotných útoků, které se zaměřovaly na způsoby získání přihlašovacích údajů a vyhledávání zranitelnosti dle dostupných dokumentací nástrojů. Jednalo se útoky brute force, sql injection, cracking a nalezení zranitelností. Při Sql injection bylo zapotřebí prozkoumat databázi, a to buď manuálně nebo za použití nástroje Burp Suite.

Demonstrace testování nebyly prováděny na reálných systémech z důvodu omezení zákona. Vše bylo prováděno na místech tomu plně určené, a to na zmíněné webové aplikaci nebo webové stránce k tomu určené.

V poslední kapitole bylo uzavřeno testování a došlo ke komparaci nástrojů mezi sebou, kdy jako nejlépe hodnocený i přes jeho možnost vysoké ceny, vyšel nástroj Burp Suite.

7 Seznam použitých zdrojů

aircrack-ng. 2021. aircrack-ng. *aircrack-ng.* [Online] 2021. https://www.aircrack-ng.org/.

awasthi7xenextt. 2019. What is Burp Suite? *geeksforgeeks.* [Online] 26. 8 2019. https://www.geeksforgeeks.org/what-is-burp-suite/.

ciphersec. 2020. A Complete Guide to the Phases of Penetration Testing. *Cipher.* [Online] 8. 9 2020. https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/.

Cloudflare. 2021. What is penetration testing? *Cloudflare.* [Online] 2021. https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/.

Comguard. 2021. Penetrační testování. *comguard.cz.* [Online] 2021. https://www.comguard.cz/penetracni-testovani.

Dizdar, Admir. 2021. What is Penetration Testing? Process, Types, and Tools. *Bright.* [Online] 1. 6 2021. https://brightsec.com/blog/penetration-testing/.

DVWA. 2021. Damn Vulnerable Web Application (DVWA). *DVWA.* [Online] 2021. https://dvwa.co.uk/.

Engebretson, Patrick. 2011. *The Basics of Hacking and penetration testing.* Waltham : Elsevier, 2011. 978-1-59749-655-1.

HelpSystems. 2021. How to Select the Right Third-Party Pen Testing Service. *coresecurity.* [Online] 2021. https://www.coresecurity.com/blog/how-select-right-third-party-pen-testing-service.

—. 2021. What Is Penetration Testing? *coresecurity.* [Online] 2021. https://www.coresecurity.com/penetration-testing.

Integra. 2021. typy pemetračních testů. *zabezpecujem.net.* [Online] 2021. https://zabezpecujeme.net/typy-penetracnich-testu.

Kali. 2021. Kali Tools. *Kali.org.* [Online] 2021. https://www.kali.org/tools/.

Kali Linux. 2021. Get Kali. *kali.org.* [Online] 2021. https://www.kali.org/.

Kaspersky. 2021. What is a Black-Hat hacker? *Kaspersky.* [Online] 13. 1 2021. https://www.kaspersky.com/resource-center/threats/black-hat-hacker.

—. 2021. what is cyber security. *Kaspersky.* [Online] 2021. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.

Kaspersky.com. 2021. White Hat Hackers: The Good, the Bad, or the Ugly? *kaspersky.* [Online] 2021. https://www.kaspersky.com/resource-center/definitions/white-hat-hackers.

KOLOUCH, Jan, BAŠTA, Pavel a kol. 2019. *CYBERSECURITY.* Praha : CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8.

Kolouch, JUDr. Jan. 2010. kybernetické útoky. *csirt.cesnet.cz.* [Online] 11. 1 2010. https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf.

Kovalčík, Marek. 2020. Etický hacking – laicky a jednoduše. *bdo.* [Online] 8. 12 2020. https://www.bdo.cz/cs-cz/blog/it-security/12-2020/eticky-hacking-%E2%80%93-laicky-a-jednoduse.

Malwarebytes. 2021. [Online] 29. 11 2021. https://www.malwarebytes.com/hacker.

Manoj, Rai. 2014. Choosing the Right Penetration Testing Tool. *happiestminds.* [Online] 20. 8 2014. https://www.happiestminds.com/blogs/choosing-the-right-penetration-testing-tool/.

Martin6. 2020. Nejlepší Kali Linux Nástroje 2019 - 10 Nejlepší Kali Linux penetrační testovací nástroje. *websetnet.* [Online] 5. 8 2020. https://websetnet.net/cs/best-kali-linux-tools-2019-10-best-kali-linux-penetration-testing-tools/.

Mitnick, Kevin. 2017. *The art of invisibility.* New York : Little, Brown and Company, 2017. ISBN 978-0-316-38049-2.

Nmap. 2006. Documentation. *nmap.* [Online] 2006. https://nmap.org/docs.html.

OCCUPYTHEWEB. 2019. *LINUX BASICS FOR HACKERS: Getting Started with Networking, Scripting, and Security in Kali.* San Francisco : No Starch Press, Inc., 2019. ISBN: 978-1-59327-855-7.

Openwall. 2019. Documentation. *Openwall.* [Online] 11. 4 2019. https://www.openwall.com/john/doc/.

—. 2021. john. *openwall.* [Online] 2021. https://www.openwall.com/john/.

Oracle. 2021. VirtualBox – Oracle VM VirtualBox. *https://www.virtualbox.org/.* [Online] 2021. https://www.virtualbox.org/wiki/VirtualBox.

Portswigger. 2021. Burp Suite documentation. *portswigger.* [Online] 21. 12 2021. https://portswigger.net/burp/documentation.

—. 2021. Burp Suite is the choice of security professionals worldwide. *portswigger.* [Online] 2021. https://portswigger.net/burp.

—. 2021. How to use Burp Suite for penetration testing. *portswigger.* [Online] 11. 11 2021. https://portswigger.net/burp/documentation/desktop/penetration-testing.

Rafter, Dan. 2021. What is the difference between black, white and gray hat hackers? *Norton.* [Online] 25. 2 2021. https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html.

Redlegg Blog. 2019. PEN TESTING: INTERNAL VS EXTERNAL AND WHY BOTH ARE IMPORTANT. *Redlegg.* [Online] 1. 9 2019. https://www.redlegg.com/blog/penetration-testing-internal-vs-external-and-why-both-are-important.

Sabih, Zaid . 2018. *Learn Ethical Hacking from Scratch: Your stepping stone to penetration testing.* Birmingham : Packt Publishing Ltd., 2018. ISBN 978-1-78862-205-9.

Sarangam, Ajay. 2021. different types of hackers. *jigsawacademy.* [Online] 3. 8 2021. https://www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/#White-Hat-Hackers.

Selecký, Matúš. 2012. *Penetrační testy a exploitace.* Brno : Computer Press, 2012. 978-80-251-3752-9.

Sobers, Rob. 2020. What Does it Take to Be an Ethical Hacker? *Varonis.* [Online] 17. 6 2020. https://www.varonis.com/blog/white-hat-hacker/.

Stampar, Miroslav. 2021. Usage. *github.* [Online] 20. 12 2021. https://github.com/sqlmapproject/sqlmap/wiki/Usage.

Varghese, Jinson. 2021. What, Why, and How of Penetration Testing. *Astra.* [Online] 3. 3 2021. https://www.getastra.com/blog/security-audit/penetration-testing/.

wallarm.com. 2021. Gray Hat Hacker. *wallarm.com.* [Online] 2021. https://www.wallarm.com/what/gray-hat-hacker.

Weidman, Georgia. 2014. *Penetration testing: A Hands-On Introducton to hacking.* San Francisco : No Starch Press, Inc., 2014. ISBN: 978-1-59327-564-8.

Wireshark. 2021. Documentation. *Wireshark.* [Online] 2021. https://www.wireshark.org/docs/.