EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

TESTOVÁNÍ BEZPEČNOSTI

Etický hacking

Metodický list

Autor: doc. Ing. Jaroslav Dočkal, CSc., Metodik: Bc. Jaroslav Tihlařík

Recenzent: Martin Žember

Rok vydání: 2023

Obsah

Cíle

V rámci této úlohy bude dosaženo následujících cílů:

- Objasnit žákům základní pojmy a terminologii v oblasti kybernetické bezpečnosti
- Poskytnout přehled nástrojů aktérů ohrožení
- Seznámit s dvěma nejznámějšími modely v oblasti kybernetické bezpečnosti a rozdíly mezi nimi
- Nalézt základní zdroje pro procvičování znalostí v oblasti etického hackingu
- Procvičit použití technik etického hackingu

Dovednosti

Žáci by si měli osvojit následující dovednosti:

- Osvojit základní pojmy v oblasti kybernetické bezpečnosti
- Porozumět použití nejznámějších nástrojů etického hackingu
- Aplikovat principy etického hackingu v rámci blue týmů
- Analyzovat útoky red týmu
- Hodnotit dostupné zdroje informací na téma etického hackingu
- Používat MITRE ATT&CK Navigátor při analýze komplexních penetrací

Pracovní prostředí

Úlohu lze realizovat v prostředí:

- Cylab JCEKB
- Offline Security Classroom

Pro práci budeme potřebovat následující nástroje:

- MITRE ATT&CK Navigátor

Protože jde o úvodní téma celé problematiky kybernetické bezpečnosti, nevyžaduje se zde speciální technické vybavení.

Průběh výuky

1 Teoretická část

Na tomto místě by se měl nacházet nutný teoretický podklad pro správné pochopení problematiky. Nemusí nutně obsahovat mnoho řádek textu. Spíše je vhodné se zaměřit na nezbytné teoretické minimum, které žák musí bezpodmínečně zvládnout.

1.1 Základní pojmy oblasti kybernetické bezpečnosti

Pro pochopení procesů zabezpečení sítě je důležité znát následující základní pojmy uvedené v tabulce 1.

Tabulka 1.1.1: Základní pojmy v oblasti kybernetické bezpečnosti (Cisco Module 13 2020)

TERMÍN	VYSVĚTLENÍ
Aktiva	Cokoliv, co má pro danou firmu či organizaci cenu.
Ohrožení	Potenciální nebezpečí pro aktiva, jako jsou data nebo samotná síť.
Hrozba	Vyjádření úmyslu způsobit zlo, zranění nebo škodu.
Zranitelnost	Slabina v systému nebo jeho návrhu, kterou by mohla zneužít hrozba.
Riziko	Pravděpodobnost, že konkrétní hrozba využije konkrétní zranitelnost aktiva a povede k nežádoucímu důsledku.
Plocha útoku (attack surface)	Plocha útoku je celkový součet zranitelností v daném systému, které jsou přístupné útočníkovi. Plocha útoku popisuje různé body, přes které by se útočník mohl dostat do systému a odkud by mohl dostat data ze systému. Attack Surface je celkový počet vektorů útoku, které může útočník použít k manipulaci se sítí nebo počítačovým systémem nebo k extrakci dat.
Vektor hrozby (threat vector) a vektor útoku (attack vector)	Vektor hrozby je způsob, jak s využitím některé slabiny potencionálně získat přístup k nezabezpečené ploše útoku (např. otevřený port nebo neopravená zranitelnost softwaru). Vektory útoků jsou záměrné hrozby (spíše než neúmyslné), protože vyžadují určité plánování a analýzu.
Exploatace	Mechanismus, který se používá k využití zranitelnosti ke kompromitaci aktiva.
Dopad	Potenciální poškození organizace způsobené hrozbou.
Protiopatření	Opatření přijatá k ochraně aktiv zmírněním hrozby nebo snížením rizika.

Máme také klíčové pojmy, které přeložit neumíme, například Proof of Concept (PoC), což je v obecné rovině zjišťování, jestli je produkt realizovatelný a zda má naději uplatnit se na trhu. Vývojáři tento termín používají jako výchozí v posloupnosti PoC – prototyp – MVP (Minimum Value Product). V oblasti kybernetické bezpečnosti se termín PoC používá k popisu kódu, který byl vyvinut k demonstraci bezpečnostních chyb. Označuje simulaci útoků sloužící k identifikaci zranitelností a jejich opravě. PoC kód lze také použít k určení úrovně hrozby. Pokud je kód PoC publikován před opravou bezpečnostní díry, může dojít k explozi nultého dne (Zero-day), kdy k útoku dochází po zjištění bezpečnostního rizika, ale před jeho opravou.

Další termín, který do oblasti kybernetické bezpečnosti přišel zvenčí, je řízení rizik. Řízení rizik je proces, který vyvažuje provozní náklady na poskytování ochranných opatření se zisky dosaženými ochranou aktiva. Existují čtyři způsoby, jak řídit rizika – viz tabulka 1.1.2.

Tabulka 1.1.2: Způsoby řízení rizik (Cisco Module 13 2020)

STRATEGIE ŘÍZENÍ RIZIK	VYSVĚTLENÍ
Přijetí rizika	Když náklady na možnosti řízení rizik převáží náklady na riziko, je riziko přijato a nejsou podniknuty žádné kroky.
Vyhýbání se riziku	To znamená vyhnout se jakémukoli vystavení riziku vyloučením činnosti, což má za následek ztrátu veškerých výhod z činnosti.
Snížení rizika	To snižuje vystavení riziku. Je to nejpoužívanější strategie zmírňování rizik. Tato strategie vyžaduje pečlivé vyhodnocení nákladů na ztráty, strategie zmírňování a přínosů získaných z operace nebo činnosti, která je ohrožena.
Přenos rizika	Některá nebo všechna rizika jsou převedena na dobrovolnou třetí stranu, jako je např. pojišťovna.

Běžné podmínky zabezpečení sítě vyžadují:

- Protiopatření – Opatření přijatá k ochraně majetku zmírněním hrozby nebo snížením rizika.
- Analýzu dopadů – Potenciální škoda pro organizaci, která je způsobena hrozbou.

Poznámka: Místní exploit vyžaduje vnitřní síťový přístup, jako je uživatel s účtem v síti. Ke zneužití zranitelnosti této sítě nevyžaduje účet v síti.

„Hacker“ je běžný termín používaný k popisu aktéra hrozby. Termín má různé významy, které jsou následující:

1 Chytrý programátor schopný vyvíjet nové programy a provádět změny v kódování stávajících programů, aby byly efektivnější.

2 Síťový profesionál, který využívá sofistikované programovací dovednosti, aby zajistil, že sítě nebudou zranitelné vůči útokům.

3 Jednotlivec, který spouští programy k zabránění nebo poškození dat na serverech.

Rozlišujeme tři typy hackerů: **White Hat, Grey Hat a Black Hat**. White Hat jsou etičtí hackeři, kteří své programátorské dovednosti využívají pro dobré, etické a právně obhajitelné účely. Grey Hat jsou jednotlivci, kteří páchají zločiny a neetické věci, ale ne pro osobní zisk nebo způsobit škodu. Black Hat jsou neetičtí zločinci, kteří porušují zabezpečení počítače a sítě pro osobní zisk.

Co je to etické hackování?

Podstatou definice etického hackingu je, že zahrnuje autorizovaný pokus o získání neoprávněného přístupu k počítačovému systému, aplikaci nebo datům. Provádění etického hacku zahrnuje duplikování strategií a akcí škodlivých útočníků. Tento postup pomáhá identifikovat slabá místa zabezpečení, která pak lze vyřešit dříve, než má útočník příležitost je zneužít.

Co je to etický hacker?

White Hat, neboli etičtí hackeři, jsou bezpečnostní experti, kteří s předchozím souhlasem organizace nebo vlastníka IT aktiv provádějí bezpečnostní hodnocení organizace a tím zlepšují bezpečnostní pozici organizace. Podmínkou legálnosti je určení rozsahu prací tak, aby nepřekročily schválené hranic organizace. Organizaci je informována o všech zranitelnostech zjištěných během hodnocení a zároveň obdrží rady k nápravě pro vyřešení těchto zranitelností. V závislosti na citlivosti dat mohou etičtí hackeři kromě jiných požadovaných podmínek posuzovanou organizací souhlasit i se smlouvou o mlčenlivosti.

Poznámka: Termín „aktér hrozby“ se používá, když se odkazuje na jednotlivce nebo skupiny, které by mohly být klasifikovány jako hackeři Grey Hat nebo Black Hat.

Aktéři hrozeb jsou následujících čtyř kategorií:

- Script kiddies – termín se vztahuje na teenagery a nezkušené osoby, kteří používají existující skripty, nástroje a exploity, aby způsobili škodu, ale obvykle ne za účelem zisku.
- Brokeři (makléři) zranitelnosti – Týká se to Grey Hat hackerů, kteří se pokoušejí objevit exploity a nahlásit je prodejcům, aby získali ceny nebo odměny.
- Hacktivisté – odkazuje opět na Grey Hat hackery, kteří se shromažďují a protestují proti různým politickým a společenským myšlenkám.
- Kyberzločinci – označuje Black Hat hackery, kteří jsou buď samostatně výdělečně činní, nebo pracují pro velké organizace zabývající se kyberzločinem.

Státem sponzorovaní hackeři jsou aktéři hrozeb, kteří kradou vládní tajemství, shromažďují zpravodajské informace a sabotují sítě zahraničních vlád, teroristických skupin a korporací.

Kybernetická bezpečnost má v současnosti následující rysy:

- Aktéři hrozeb se zaměřují na domácí uživatele, malé a střední podniky i velké veřejné a soukromé organizace.
- Kybernetická bezpečnost je tedy sdílená odpovědnost, kterou musí všichni uživatelé praktikovat, aby byl internet a sítě bezpečnější a bezpečnější.
- Organizace musí jednat a chránit svá aktiva, uživatele a zákazníky. Musí vyvinout a procvičit úkoly v oblasti kybernetické bezpečnosti, jako jsou důvěryhodné dodavatelé, aktuální bezpečnostní software, penetrační testy, zálohování na disk nebo do cloudu, periodické změny WiFi hesel, aktuální bezpečnostní politika, vynucování použití silného hesla, dvoufaktorová autentizace atd.

Indikátory kompromitace (IOC)

- Jsou důkazem, že k útoku došlo, a každý útok má jedinečné identifikovatelné atributy.
- Mohou být funkce, které mimo jiné identifikují soubory malwaru, IP adresy serverů, které se používají při útocích, názvy souborů a charakteristické změny provedené v softwaru koncového systému.
- Pomáhají pracovníkům kybernetické bezpečnosti identifikovat, co se stalo při útoku, a rozvíjet obranu proti útoku.

Indikátory útoku (IOA)

- více se zaměřuje na motivaci a strategie za útokem a na útočníky, aby získali přístup k aktivům,
- pomáhají vytvářet proaktivní přístup k zabezpečení, který lze znovu použít v různých kontextech a při více útocích. Obrana proti strategii tedy může zabránit budoucím útokům.

Sdílení hrozeb a budování povědomí o kybernetické bezpečnosti přineslo řadu pozitivních momentů:

- Vlády nyní aktivně podporují kybernetickou bezpečnost.
- Americká Agentura pro kybernetickou bezpečnost a infrastrukturu (CISA – Cybersecurity Infrastructure and Security Agency) vede úsilí o automatizaci bezplatného sdílení informací o kybernetické bezpečnosti s veřejnými a soukromými organizacemi.
- CISA používá systém nazvaný Automated Indicator Sharing (AIS), který umožňuje sdílení indikátorů útoku mezi americkou vládou a soukromým sektorem, jakmile jsou hrozby ověřeny.
- Agentura Evropské unie pro kybernetickou bezpečnost (ENISA – European Union Agency for Cybersecurity) poskytuje rady a řešení pro výzvy členských států EU v oblasti kybernetické bezpečnosti.
- CISA a National Cyber Security Alliance (NCSA) pořádají každý říjen každoroční kampaň s názvem National Cybersecurity Awareness Month (NCASM) s cílem zvýšit povědomí o kybernetické bezpečnosti.

1.2 Nástroje aktérů ohrožení

Pro nástroje aktérů ohrožení platí:

- Aby mohl aktér hrozby využít zranitelnost, musí mít techniku nebo nástroj.
- V průběhu let se útočné nástroje staly sofistikovanějšími a vysoce automatizovanými.
- Implementace těchto nových nástrojů vyžaduje méně technických znalostí.
- Etické hackování zahrnuje použití mnoha různých typů nástrojů k testování sítě a koncových zařízení.

- Pro ověření bezpečnosti sítě a jejích systémů bylo vyvinuto mnoho nástrojů pro testování průniku do sítě a mnohé z těchto nástrojů mohou také využít aktéři hrozeb ke zneužití.
- Aktéři hrozeb také vytvořili různé hackerské nástroje. Pracovníci kybernetické bezpečnosti musí také vědět, jak tyto nástroje používat při provádění testů pronikání do sítě.

Poznámka: *Většina těchto nástrojů je založena na systému UNIX nebo Linux; proto by bezpečnostní profesionál měl mít dobré zázemí pro UNIX a Linux. Podle by také měl být schopen číst programy v jazycích C, Python a Assembleru.*

V tabulce 1.2.1 jsou uvedeny některé kategorie běžných nástrojů pro testování penetrace sítí.

Tabulka 1.2.1: Vybrané kategorie běžných nástrojů pro testování penetrace sítí (Cisco Module 13 2020)

Kategorie nástrojů	Popis
Prolomení hesel	Používá se k prolomení nebo obnovení hesla. Např. pro offline crackování hashů hesel John the Ripper, Ophcrack, pro online hádání hesel Hydra, Medusa, Patator
Nástroje pro bezdrátové hackování	Používá se k záměrnému nabourání se do bezdrátové sítě za účelem zjištění slabých míst zabezpečení. Např. Aircrack-ng a jeho nadstavba wifite, bettercap, Kismet
Nástroje pro skenování a hackování sítě	Používá se k testování síťových zařízení, serverů a hostitelů na otevřené porty TCP nebo UDP. Např. Nmap, Masscan, Unicornscan, SuperScan
Nástroje pro tvorbu paketů	Používají se k testování a testování odolnosti firewallu. Např. Hping3, Scapy
Sniffery paketů	Používá se k zachycení a analýze paketů v tradičních ethernetových LAN nebo WLAN. Např. Wireshark, Tcpdump, Molo.ch, NetworkMiner, Zeek, Snort
Detektory rootkitů	Jedná se o kontrolu integrity adresářů a souborů, kterou používají White Hat k detekci nainstalovaných zadních vrátek . Např. AIDE, Netfilter, Tripwire, chkrootkit, rkhunter
Fuzzery pro vyhledávání zranitelností	Používají j e aktéři hrozeb při pokusu odhalit slabá místa zabezpečení počítačového systému vyzkoušením mnoha různých vstupů. Např. pro weby Burp Suite, ZAProxy , Wapiti
Forenzní nástroje	White Hats používají tyto nástroje k vyčmuchání jakýchkoli stop důkazů existujících v konkrétním počítačovém systému. Např. Sleuth Kit, Helix

Debuggery a disassemblery	Používají je Black Hat k reverzní analýze binárních souborů při psaní exploitů a White Hat při analýze malwaru. Např. GDB, WinDbg, ImmunityDbg, IDA Free/IDA Pro, radare2, GHIDRA
Hackovací operační systémy	Ty jsou předinstalované nástroji a technologiemi optimalizovanými pro hackování. Např. Kali Linux, Parrot
Šifrovací nástroje	Tyto nástroje používají schémata algoritmů ke kódování dat, aby se zabránilo neoprávněnému přístupu k datům. Např. VeraCrypt, GPG, CipherShed
Nástroje pro zneužívání zranitelnosti	Tyto nástroje identifikují, zda je vzdálený hostitel zranitelný vůči bezpečnostnímu útoku. Např. Metasploit, Core Impact, RouterSploit, FuzzBunch
Skenery zranitelnosti	Tyto nástroje skenují síť nebo systém a identifikují otevřené porty. Lze je také použít ke skenování známých zranitelností a skenování virtuálních počítačů, zařízení BYOD a klientských databází. Např. Nuclei, Nessus, Greenbone Vulnerability Manager, Nmap NSE skripty, Nipper, Securia PSI

Aktéři hrozeb využívají k vytváření různých útoků výše zmíněné nástroje nebo kombinaci nástrojů. Je důležité pochopit, že aktéři hrozeb používají k provádění těchto útoků různé bezpečnostní nástroje. V následující tabulce 1.2.2 jsou uvedeny běžné typy útoků.

Tabulka 1.2.2: Vybrané kategorie útoků používaných při testování penetrace sítí (Cisco Module 13 2020)

Kategorie útoku	Popis
Útok využívající odposlech	Útok na bázi odposlechu probíhá tak, že aktér zachytí hrozbu a následně naslouchá síťovému provozu. Říká se tomu také čichání nebo slídění.
Útok na úpravu dat	K útokům na úpravu dat dochází, když aktér hrozby zachytil podnikový provoz a změnil data v paketech bez vědomí odesilatele nebo příjemce.
Útok falšováním (spoofingem) IP adres	K útoku falšování IP adresy dochází, když aktér hrozby sestrojí paket IP, který vypadá, že pochází z platné adresy v podnikovém intranetu.
Útoky cílené na hesla	K útokům na hesla dochází, když aktér hrozby získá pověření pro platný uživatelský účet.

Denial-of-service (DoS) útok (útok záplavou)	Útok DoS brání normálnímu používání počítače nebo sítě platnými uživateli. Tento útok může blokovat provoz, což má za následek ztrátu přístupu k síťovým zdrojům.
Man-in-the-middle útok (MiTM)	K útoku MiTM dochází, když se aktéři hrozby umístí mezi zdroje a cíl.
Kompromitovaný útok na klíč	K útoku na kompromitovaný klíč dochází, když aktér hrozby získá tajný klíč. Kompromitovaný klíč lze použít k získání přístupu k zabezpečené komunikaci bez odesílatele nebo příjemce.
Sniffing	Sniffing je aplikace nebo zařízení, které může číst, monitorovat a zachycovat síťové výměny dat a číst síťové pakety. Pokud pakety nejsou zašifrovány, sniffer má úplný pohled na data uvnitř paketu.

Engines najdeme na google.com, Shodan.io, Censys.io, Hunter.io, redhuntlabs.com, fullhunt.io, onyphe.io, fofa.so, socradar.io, synapsint.com, binaryedge.io, ivre.rocks, crt.sh.

1.3 Proces penetračního testování metodou Cyber Kill Chain

Cyber Kill Chain, také známý jako Cyber Attack Lifecycle, je série fází kybernetického útoku, od průzkumu až po exfiltraci dat a aktiv. Díky pochopení modelu kybernetického „zabíjení“ mohou organizace lépe identifikovat, předcházet a zmírňovat ransomware, narušení bezpečnosti a pokročilé perzistentní hrozby (APT – Advanced Persistent Threats).

Termín „Kill Chain“ pochází z vojenského konceptu a struktury fázovaného útoku. Jeho struktura je následující: Identifikace cíle, vyslání síly na cíl, rozhodnutí a příkaz k útoku na cíl, Zničení cíle.

Lockheed Martin[1] byl první, kdo vzal tento koncept, aplikoval jej na informační bezpečnost a použil jej jako metodu pro modelování průniku do počítačové sítě. Počítačoví vědci z Lockheed Martin zjistili, že kybernetické útoky se často vyskytují ve fázích a mohou být narušeny prostřednictvím kontrol zavedených v každé fázi. Při reakci na bezpečnostní incident je cílem detekovat a zastavit útok co nejdříve v průběhu řetězce zabíjení, aby se zabránilo dalším škodám. Pokud je útočník v jakékoli fázi zastaven, zabijácký řetězec je přerušen a obránce úspěšně zmaří průnik aktéra hrozby.

Popišme si jednotlivé fáze a v jejich rámci taktiky útoku a obrany z hlediska SOC (Security Operation Centre) v souladu s výkladem v (CyberOps 2021).

[1] jedna z vedoucích mezinárodních společností s pokročilou technologií a rovněž výrobce letadel.

1.3.1 Průzkum

Průzkumem je, když aktér hrozby shromažďuje informace a vybírá cíle. Přednostně si vybírá cíle, které byly zanedbávány nebo nechráněny, protože bude mít vyšší pravděpodobnost, že budou proniknuty a kompromitovány.

Taktika protivníka spočívá ve sběru e-mailových adres, identifikaci zaměstnanců na sociálních sítích, shromažďujte všechny informace o vztazích s veřejností (tiskové zprávy, ocenění, účastníci konference atd., vyhledávání serverů orientovaných na internet, skenování sítě k identifikaci IP adres a otevřených portů.

Obrana SOC spočívá v odhalení záměru protivníka, zkoumání webového protokolu a vyhledávání v historických záznamech, v analýza prohlížeče datového dolu (mining) a ve vytvářejte příručky pro detekci chování, které naznačuje aktivitu průzkumu. Obrana musí být zaměřena na technologie a lidi, na které se průzkumná činnost útočníka zaměřuje.

1.3.2 Ozbrojování

Taktika útočníka spočívá ve využití informací z průzkumu k vývoji zbraně proti specifickým cíleným systémům nebo jednotlivcům v organizaci. Často je efektivnější použít zero-day útok[2], aby se útočník vyhnul detekčním metodám.

Útočník připraví a uspořádá operaci, během které:

- Získá automatizovaný nástroj pro doručení užitečné zátěže (payload) malwaru (weaponizer).
- Vybere nebo vytvoří falešný dokument, který předhodí oběti.
- Vybere nebo vytvoří zadní vrátka a infrastrukturu velení a řízení (C&C – command and control).

Obrana SOC detekuje a sbírá artefakty zbraní, kontroluje aktuálnost pravidel řízení přístupu a signatur IDS, provádí úplnou analýzu odchyceného malwaru, nastavuje detekce chování firewallů a dalších zařízení, zkoumá, zda je malware starý nebo nový, sbírá soubory a metadata pro budoucí analýzu. Úkolem je i určit, které artefakty jsou společné pro které kampaně.

1.3.3 Doručení

Během tohoto kroku je zbraň přenesena na cíl pomocí vektoru dodávky. Pokud zbraň není doručena, útok bude neúspěšný. Aktér ohrožení použije různé metody ke zvýšení šancí na doručení užitečného zatížení, jako je šifrování komunikace, vytvoření legitimního kódu nebo zamlžení (obfuscating) kódu. Bezpečnostní senzory jsou dnes tak pokročilé, že mohou detekovat kód jako škodlivý, pokud není pozměněn, aby se zabránilo detekci.

Taktika útočníka musí zajistit spuštění malwaru v cíli buď přímo na webové servery anebo nepřímo prostřednictvím škodlivého e-mailu, malwaru na USB klíčence, interakce na sociálních sítích či kompromitované webové stránky.

Obrana SOC spočívá v blokování doručení malwaru: Analýzou cesty infrastrukturou použitou pro doručení, sledování cílených serverů, osob a dat, která jsou vystavena pro útok, předvídání záměrů protivníka na základě jeho předpokládaných cílů, sběru e-mailových a webových protokolů pro forenzní rekonstrukci.

[2] zero day útok – hrozba či útok, který využívá fakt, že daný software je zranitelný, tj. ještě pro něj neexistuje obrana. „zero“, neboli nula, značí, že uživatel se až do té doby, dokud nebude vydána aktualizace, nachází ve výchozím postavení, tj. v nultém dni.

1.3.4 Exploatace (vytěžování)

Poté, co byla zbraň doručena, aktér hrozby ji použije k prolomení zranitelnosti a získání kontroly nad cílem. Nejčastějšími objekty vytěžování informací jsou aplikace, zranitelnosti operačního systému a uživatelé.

Taktika útočníka je založena na využití zranitelnosti k získání přístupu. Útočník využívá software, hardware nebo lidskou zranitelnost a, získá nebo rozvíjí exploit. Ideální je, když si obránce sám spustí exploit např. díky otevřené příloze e-mailu nebo škodlivému webovému odkazu.

Obrana SOC je založena na školení zaměstnanců na téma bezpečnosti, zabezpečení kódu a posílení zařízení, pravidelném testování e-mailů, školení webových vývojářů pro zabezpečení kódu, pravidelném skenování zranitelnosti a penetračním testování, opatřeních pro zodolnění koncových zařízení a jejich Auditu pro forenzní určení původu exploitu.

1.3.5 Instalace

Během tohoto kroku si aktér hrozby vytvoří zadní vrátka do systému, aby si vytvořil nepřetržitý přístup k cíli. Aby se tato zadní vrátka zachovala, vzdálený přístup by neměl upozorňovat analytiky nebo uživatele kybernetické bezpečnosti. Aby byla přístupová metoda účinná, musí přežít antimalwarové skenování a restarty počítače.

Taktika útočníka spočívá v instalaci perzistentních (stálých) zadních vrátek, např. v nainstalování webového shellu na webový server pro trvalý přístup či vytvořte bod stálosti (point of persistence) přidáním služeb, klíčů AutoRun atd. Někteří protivníci upravují časové razítko malwaru, aby se jevili jako součást operačního systému.

Obrana SOC je založena na detekci, protokolování a analýze aktivity instalace: HIPS musí upozorňovat nebo blokovat běžné instalační cesty. Pídit se je třeba po tom, zda malware vyžaduje zvýšená oprávnění nebo uživatelská oprávnění, je třeba auditovat koncové body pro zjištění abnormálních vytváření souborů a zjistit, zda je malware známou hrozbou nebo novou variantou.

1.3.6 Velení a řízení (C&C, C2)

Cílem je vtvoření zabezpečené komunikace s cílovým systémem. Kompromitovaní hostitelé obvykle odhlašují od sítě ke controlleru směrem k internetu. Aktéři hrozeb používají kanály C&C k vydávání příkazů softwaru, který nainstalovali do cíle. Analytik kybernetické bezpečnosti musí být schopen tuto komunikaci detekovat, aby odhalil kompromitovaného hostitele.

Taktika útočníka je založena na otevření kanálu pro manipulaci s cílem otevření obousměrných komunikačních kanálů do infrastruktury (nejběžnější C&C kanály vedou přes web, DNS a e-mailové protokoly). Infrastruktura C&C přitom může být vlastněna protivníkem nebo sítí jiných obětí.

Obrana SOC má poslední šanci zablokovat operaci a objevit infrastrukturu C&C pomocí analýzy malwaru, případně provádět výzkum možných nových C&C infrastruktur. Po jejich zjištění izoluje provoz DNS na podezřelých serverech

DNS, zejména na dynamických DNS[3], blokováním kanálu chrání před dopady na aktiva, konsoliduje počet míst připojení do internetu (points of presence) a nastavuje pravidla blokování protokolů C&C na webových serverech proxy.

1.3.7 Akce na cílech

Jde o poslední krok Cyber Kill Chain, který popisuje, jak aktér hrozby dosahuje svého původního cíle. V tomto okamžiku je aktér hrozby již hluboce zakořeněn v systémech organizace, skrývá své pohyby a zakrývá stopy. Nyní je už extrémně obtížné odstranit aktéra hrozby ze sítě.

Taktika útočníka spočívá ve sklízení plodů úspěšného útoku: sběru přihlašovacích údajů uživatele, eskalaci privilegií, vnitřním průzkumu, laterálním (bočním) pohybu prostředím, sběru a extrakci dat, zničení systému či přepisu, úpravě či poškození dat.

Obrana SOC už může jen odhalit útok pomocí forenzních důkazů: detekovat exfiltraci dat, boční pohyb a neoprávněné použití přihlašovacích údajů. Analytik musí na všechna upozornění okamžitě reagovat. Probíhá forenzní analýza koncových bodů pro rychlé třídění, zachycují se síťové pakety pro obnovení aktivity a provádí posouzení poškození. Na závěr lze vytvořit příručku reakce na incidenty či ji doplnit o nové pravidlo.

1.3.8 Varianty Cyber Kill Chain

Existují i poněkud odlišné etapy koncepce Cyber Kill Chain, např. v (Hospelhorn 2016), je název 2. fáze místo Weaponization Intrusion, ale to je spíše formální rozdíl. Jako samostatné fáze jsou rozlišovány Privilege Escalation, Lateral Movement a Denial of Service, neboli jde o fáze více orientované na techniky, ale zase jde o 7 fází: Reconnaissance, Intrusion, Exploitation, Privilege Escalation, Lateral Movement, Denial of Service, Exfiltration).

Od svého vzniku se řetězec zabíjení vyvíjel, aby lépe předvídal a porozuměl moderním kybernetickým hrozbám, a byl přijat organizacemi a odborníky na zabezpečení dat, aby pomohl definovat fáze útoku. Ačkoli mnohé firmy z oblasti kybernetické bezpečnosti přijali Cyber Kill Chain, přijetí stále není univerzální a existuje mnoho kritiků, kteří poukazují na to, co považují za základní nedostatky.

1.3.9 Kritika Cyber Kill Chain

Současné kritiky lze rozdělit do dvou hlavních kategorií: zabezpečení perimetru a zranitelnosti útoku.

Zabezpečení perimetru: Jednou z největších kritik modelu kybernetického zabíjení společnosti Lockheed je skutečnost, že první fáze (průzkum, zbrojení) útoku probíhají mimo cílovou síť, což ztěžuje pochopení nebo obranu proti akcím, ke kterým v těchto fázích dochází.

Útok na zranitelnosti: Někteří kritici se domnívají, že metodika také posiluje tradiční obranné strategie založené na perimetru a prevenci malwaru, které v dnešním klimatu kybernetické bezpečnosti nestačí.

Jedna závěrečná kritika uvádí (Hospelhorn 2016), že tradiční řetězec kybernetického zabíjení není vhodným modelem při přemýšlení o hrozbách zevnitř. Z tohoto důvodu jsou organizace potenciálně více ohroženy, vzhledem k pravděpodobnosti úspěšných útoků, které naruší perimetr vnitřní sítě cíle.

[3] DDNS naboptnaly u Windows.

1.3.10 Budoucnost Cyber Kill Chain

Vzhledem k neustále se vyvíjející povaze kybernetických hrozeb je budoucnost Cyber Kill Chain ve vzduchu. Vzhledem k tomu, že koncepce XDR (eXtended Detection and Response) je pro moderní strategii kybernetické bezpečnosti stále důležitější, mnozí autoři se domnívají, že je třeba vytvořit nový rámec.

Kontrolní otázky

- Do které fáze popsané metodiky byste umístili phishing?
- V které fázi byste použili kompresi a šifrování?
- V které fázi byste použili PowerShell, skripty, makra v dokumentech ?

1.4 MITRE ATT&CK

1.4.1 Rámec MITRE ATT&CK

Rámec MITRE ATT&CK (dále jen stručně ATT&CK) je globální centrum znalostní báze pro dokumentaci různých taktik a technik, které hackeři používají v různých fázích kybernetického útoku. Společnost MITRE začala databázi vyvíjet v roce 2013 a v průběhu let se stala klíčovým zdrojem pro týmy kybernetické obrany při posuzování zranitelností a bezpečnostních protokolů.

ATT&CK je zkratka pro *Adversarial Tactics, Techniques a Common Knowledge*. Rámec je maticí různých technik kybernetického útoku seřazených a organizovaných podle různých taktik. Navíc existují různé matice pro Windows, Linux, Mac a mobilní systémy. Použití matice MITRE ATT&CK je mimořádně užitečným nástrojem pro zjištění, jaké útočné vektory mohou hackeři použít proti vaší společnosti a jak optimalizovat váš plán reakce na incidenty a penetrační testování.

Primárním cílem rámce ATT&CK je zlepšit detekci škodlivých aktérů, kteří se zaměřují na podnikové sítě, systémy a data. Při používání ATT&CK organizace získají přehled o akcích, které by útočník mohl podniknout. Zkoumá cesty vstupu útočníka do systému, jak se pohybuje a na jaké oblasti míří.

Znalostní databáze je navržena tak, aby zodpověděla klíčové otázky o tom, jak by se hackeři mohli zaměřit na konkrétní společnost, a také přispěla k celkovému stavu zabezpečení organizace. Použití ATT&CK pomáhá identifikovat díry a zranitelnosti a pomáhá společnostem je pak upřednostňovat na základě celkového rizika.

Security Operations Center (SOC) a Red týmy používají rámec ATT&CK pro:

- Plánování strategie kybernetické bezpečnosti. Sestavení obrany proti známým technikám a nastavení monitorování tak, aby detekovalo důkazy o technikách ATT&CK.
- Sestavení referencí pro reakci týmů na incidenty (Incident Response – IR). IR tým může použít ATT&CK k určení povahy potenciálních hrozeb a metod potřebných k jejich eliminaci.
- Reference budoucího IR plánování. IR tým může použít ATT&CK jako referenci pro nové hrozby kybernetické bezpečnosti a vstřícné plánování.

- Celkové ohodnocení kybernetické obrany. ATT&CK může napomoci při hodnocení celkovou strategii kybernetické bezpečnosti a při odstraňování bezpečnostních hrozeb.

ATT&CK Group reprezentuje pojmenovaný klastr aktivit útočníka, zatímco Software reprezentuje nástroje malwaru používané těmito aktéry. ATT&CK poskytuje popisy a aliasy pro Groups a Software, stejně tak jako techniky pozorované při těchto hrozbách. Techniky jsou mapovány na Groups a Software prostřednictvím příkladů těchto hrozeb, případně popisem specifických způsobů vykonávání těchto technik.

1.4.2 MITRE ATT&CK vs. CYBER KILL CHAIN

Obecně řečeno, oba systémy se řídí stejným vzorem – vstupte, nenechte se chytit, ukradněte věci. Primární rozdíl mezi těmito dvěma je v tom, že matice ATT&CK je spíše seznamem technik podle taktiky a nenavrhuje konkrétní pořadí operací.

Cyber Kill Chain je dobře definovaný sled událostí: Červený tým se pohybuje od průzkumu k narušení a tak dále v tomto pořadí. Přitom používá techniky ATT&CK z různých taktik v různých časech scénáře v závislosti na situaci. Scénář ATT&CK by mohl např. začít u Hardware Addition z taktiky Initial Access, poté přejít na Bypass User Account Control z taktiky Privilege Escalation a vrátit se k Execution tactic a spustit PowerShell.

1.4.3 Nejpoužívanější techniky útoků

Nejpoužívanější techniky útoků jsou uvedeny v tabulce 1.4.1. Rozdíly jsou dány různými metodami testování a různými zkušebními příklady.

Tabulka 1.4.1 Nejpoužívanější techniky útoků

	PICUS	CROWDSTRIKE	Recorded Future	red canary
1	Process Injection	Masquerading	Security Software Discovery	Process Injection
2	PowerShell	Command-line Interface	Obfuscated Files or Information	Scheduled Task
3	Credential Dumping	Credential Dumping	Process Injection	Windows Admin Shares
4	Masquerading	PowerShell	System Information Discovery	PowerShell
5	Command-line Interface	Hidden Files and Directories	Process Discovery	Remote File Copy
6	Scripting	Process Injection	Software Packing	Masquerading
7	Scheduled Task	Registry Run Keys / Startup Folder	DLL Side-Loading	Scripting
8	Registry Run Keys / Startup Folder	System Owner/User Discovery	Data Encrypted	DLL Search Order Hijacking
9	System Information Discovery	Account Discovery	Execution Through API	Domain Trust Recovery
10	Disabling Security Tools	Scripting	Standard Cryptographic Protocol	Disabling Security Tools

Nejčastěji používané techniky dle Picus Security (v roce 2019 byla provedena analýza 48813 malwarů):

Nejběžnější technikou byla **T1055 Process Injection**, která umožňuje vyhnout se bezpečnostním kontrolám (Defense Evasion) a získat oprávnění vyšší úrovně (Privilege Escalation) spuštěním kódu v rámci legitimního procesu.

Nejrozšířenější taktikou byly **Defence Evasion and Execution**, což naznačuje zájem útočníků zůstat pod radarem bezpečnostních kontrol. Neustále jsou vyvíjeny nové techniky úniku a vyhýbání se bezpečnostním opatřením.

Útočníci často používají nativní příkazový řádek Windows a skriptovací nástroje ke spouštění příkazů, jako je PowerShell, cmd.exe a VBScript. Tyto nástroje umožňují útočníkům provádět složitější akce a vyhýbat se bezpečnostním kontrolám přímou interakcí s operačním systémem Windows.

Jako třetí nejběžnější techniku používají útočníci **Credential Dumping** k získání pověření z operačního systému a softwaru pro provádění laterálního pohybu (Lateral Movement) a přístup k omezeným informacím a softwaru.

Nejpoužívanější dílčí techniky dle firmy SOPHOS jsou dány tabulkou 1.4.2:

Tabulka 1.4.2: Nejpoužívanější dílčí techniky dle firmy SOPHOS

TA0001	Initial access
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1566	Phishing
T1078	Valid Accounts
T1195	Supply Chain Compromise

TA0002	Execution
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
T1053	Scheduled Task/Job
T1569	System Services
T1204	User Execution

TA0003	Persistence
T1543	Create or Modify System Process
T1547.001	Registry Run Keys / Startup Folder
T1546.007	Netsh Helper DLL
T1547.010	Port Monitors
T1098	Account Manipulation

TA0004	Privilege escalation
T1059	Process Injection
T1047	Process Hollowing
T1053	SID-History Injection
T1569	.bash_profile and .bashrc
T1204	Security Support Provider

TA0005	Defense evasion
T1036	Masquerading
T1218	Signed Binary Proxy Execution
T1070	Indicator Removal on Host
T1562.001	Disable or Modify Tools
T1112	Modify Registry

TA0006	Credential access
T1552.002	Credentials in Registry
T1040	Network Sniffing
T1110	Brute Force
T1552.004	Private Keys
T1003	OS Credential Dumping

TA0007	Discovery
T1033	System Owner/User Discovery
T1007	System Service Discovery
T1016	System Network Configuration Discovery
T1046	Network Service Scanning
T1082	System Information Discovery

TA0008	Lateral movement
T1021.001	Remote Desktop Protocol
T1021.002	SMB/Windows Admin Shares
T1570	Lateral Tool Transfer
T1550.003	Pass the Ticket
T1550.002	Pass the Hash

TA0009	Collection
T1560.001	Archive via Utility
T1074	Data Staged
T1005	Data from Local System
T1039	Data from Network Shared Drive
T1409	Access Stored Application Data

TA00011	Command and control
T1105	Ingress Tool Transfer
T1090	Proxy
T1572	Protocol Tunneling
T1008	Fallback Channels
T1043	Commonly Used Port

TA0010	Exfliration
T1041	Exfiltration Over C2 Channel
T1048	Exfiltration Over Alternative Protocol
T1567.002	Exfiltration to Cloud Storage
T1567.001	Exfiltration to Code Repository
T1537	Transfer Data to Cloud Account

TA0040	Imapact
T1490	Inhibit System Recovery
T1486	Data Encrypted for Impact
T1485	Data Destruction
T1489	Service Stop
T1496	Resource Hijacking

1.5 Model Threat-informed defense (TID)

Obránci sítě tradičně zaměřovali své obranné strategie o dodržování základních osvědčených postupů v oblasti kybernetické bezpečnosti: náprava chybné konfigurace, administrace záplat a nasazení nejlepších komerčních produktů ve své třídě. Současně se defenzivní modré týmy zaměřily na obranu domácího terénu. Zároveň organizace utrácely peníze na výstavbu nebo zaměstnávání červených týmů k otestování obrany modrého týmu.

Názvy „červené“ a „modré“ týmy vykreslují obrázek vyrovnaných soupeřících týmů, což není ani zdaleka přesné. Modré týmy jsou mnohem větší a utrácejí mnohem více než červené týmy. Testování červeného týmu je epizodické a pokrytí je rozsáhlé menší než měřítko obrany modrého týmu.

Pokud se obrana nezaměřuje na nejdůležitější hrozby, může dojít k plýtvání zdrojů a protivník proklouznout bokem. Úkolem je dát dohromady a kombinovat to nejlepší z červeného a modrého týmu – píše se o fialové konstrukci – modelu TID (Model Threat-informed defense) anebo (Bergeron Dec 2020) (AttackIQ 2021).

Při zvažování důležitosti TID pro profesionály v oblasti kybernetické bezpečnosti a stejně tak týmů má smysl začít pochopením investičních podmínek typického zabezpečení.

Týmy pro kybernetickou bezpečnost obvykle investují do potřebných technologií a lidských zdrojů ad hoc tak, že osoby s rozhodovací pravomocí v oblasti kybernetické bezpečnosti naslouchají radám odborníků a poskytují finanční podporu při vzniku projektu (řekněme v reakci na konkrétní ohrožení nebo pro vznikající řešení). Druhou možností jsou srovnávací testy s partnery: Procento vynaložené na IT rozpočet technologie kybernetické bezpečnosti je ovlivněno tím, jak ostatní utrácejí.

Tyto přístupy nevedou k efektivní operační kybernetické bezpečnosti. K té vede programové sladění služeb zabezpečení a rizik s podnikáním, které umožní se racionálně rozhodovat a zlepšit efektivnost práce bezpečnostního týmu při plnění úkolů vyplývajících ze standardů a z nich vyplývajících bezpečnostních směrnic. Zde se postupuje ve třech krocích:

KROK 1: Obrana na bázi informací o hrozbách (Threat-informed defense – TID). Provádí se identifikace pravděpodobných hrozeb, se kterými se organizace setká, a výběr technologií, které nabídnou adekvátně účelnou ochranu. Obrana informovaná o hrozbách je kritickým prvkem strategie kybernetické bezpečnosti, klíčem k získání potřebného přehledu pro stanovení priorit a optimalizaci bezpečnostních rozhodnutí. Jeho hodnota přesahuje získávání znalostí a provádění změn.

KROK 2: Optimalizace zabezpečení, kdy je třeba identifikovat a kvantifikovat rizika kybernetické bezpečnosti prostřednictvím sběru přesných údajů o provádění stávajících bezpečnostních kontrol proti skutečným hrozbám. Dále je třeba upřednostnit investice do bezpečnosti na základě kvantifikovaného odhadu potenciálního rizika pro výsledky byznysu.

KROK 3 Sladění hrozeb a řízení rizik: Za poslední dekádu se však situace v oblasti kybernetické bezpečnosti staly se stále složitější. Některé bezpečnostní rámce se staly de facto standardy a ovlivňují další předpisy a shodu rámců, včetně

NIST[4] 800-53. Pouhé dodržování standardů nezaručuje úspěch, pokud kybernetická obrana není testována proti známým hrozbám. Proto v roce 2020 Center for Threat-Informed Defense MITRE Engenuity mapovala bezpečnostní kontroly uvedené v NIST 800-53 k chování protivníka v MITRE ATT&CK.

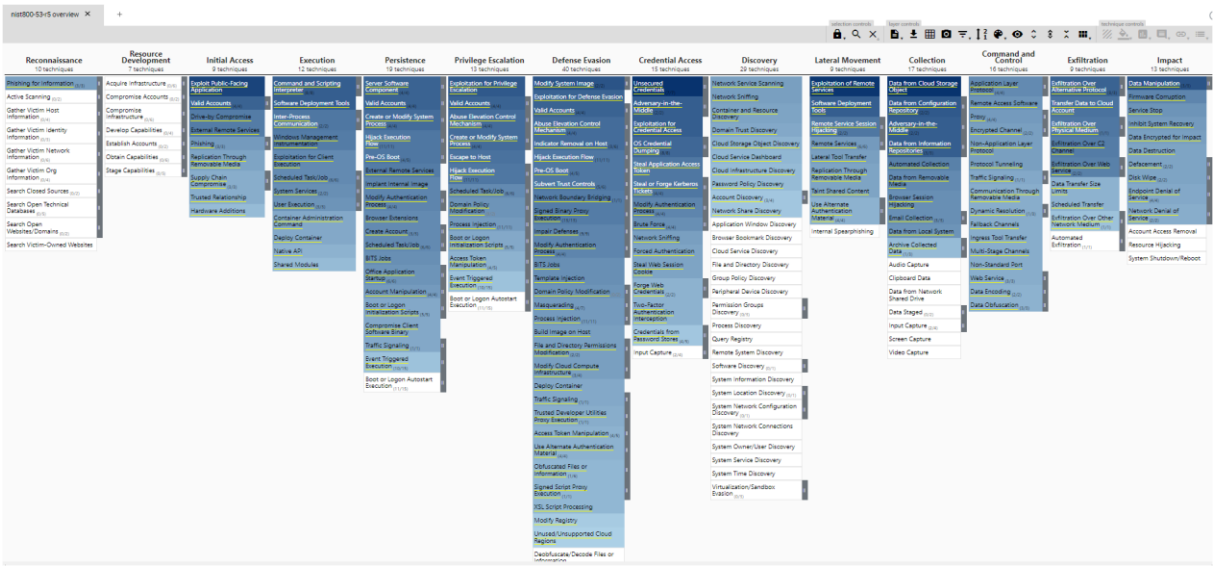
S tímto sladěním rámce hrozeb a rizik pak organizace mohou použít platformu pro simulaci narušení a útoku, aby otestovaly a ověřily, zda bezpečnostní kontroly v rámci dodržování předpisů fungují efektivně. Neboli jde o zajištění, aby ověřování shody reality s normami probíhalo spíše rutinně než prostřednictvím příležitostných auditů nebo interních bezpečnostních kontrol

1.5.1 Mapování rámce kontrol zabezpečení NIST 800–53 do MITRE ATT&CK

Center for Threat-Informed Defense v roce 2020 vydalo sadu mapování mezi MITRE ATT&CK a NIST Special Publication 800–53 s podpůrnou dokumentací a zdroji. Tato mapování poskytují organizacím kriticky důležitý zdroj pro posouzení jejich pokrytí bezpečnostní kontrolou proti reálným hrozbám popsaných ve znalostní bázi ATT&CK, a poskytují základ pro integraci informací o hrozbách založených na ATT&CK do procesu řízení rizik.

Mapování NIST 800–53 stejně jako jakéhokoliv jiného rámce kontroly zabezpečení (security control frameworks) na ATT&CK je pracný a často subjektivní úkol[5]. Navíc kvůli velkému počtu bezpečnostních kontrol v jakémkoli daném rámci a vyvíjející se povaze kybernetických protivníků jsou tato mapování často náchylná k chybám a obtížně se udržují.

Aktuální vydání poskytuje mapování z NIST 800–53 Revize 4 a Revize 5 na MITRE ATT&CK Techniques. Obrázek 1.5.1 jako příklad znázorňuje pokrytí mapováním NIST 800–53 Rev. 5 všech technik ATT&CK – čím tmavší je technika, tím více kontrol NIST 800–53 mapují tuto techniku.



[4] National Institute of Standards and Technology SP 800-53 je sada dokumentů, které podporují vývoj bezpečných a odolných federálních informačních systémů USA. Především definuje minimální sadu bezpečnostních kontrol.

[5] Center for Threat-Informed Defense spolupracuje s Center for Internet Security na aplikaci metodiky MITRE ATT&CK na kontroly CIS (Critical Security Controls).

Obrázek 1.5.1: Přehled mapování NIST 800–53 Rev. 5

Řešení je vymezeno těmito způsoby:

- Rozsah ATT&CK: Tato práce je zaměřena na techniky ATT&CK zahrnuté v doméně Enterprise; mobilní techniky nejsou zahrnuty.
- Ovládací prvky (controls) vs. vylepšení ovládacích prvků: Mapování se provádějí na úrovni řízení zabezpečení a nikoli na konkrétní vylepšení ovládání.
- Kontroly zásad a postupů: Kontroly spojené výhradně se zásadami a postupy jsou mimo rozsah, protože se mapování zaměřuje na technické a provozní prvky NIST 800–53.
- Zaměřeno na techniku: Mapování se provádí pro systémově specifická technická zabezpečení a protiopatření (např. blokování USB zařízení), nikoli pro netechnické způsoby zmírnění (např. ochrana fyzického prostoru).

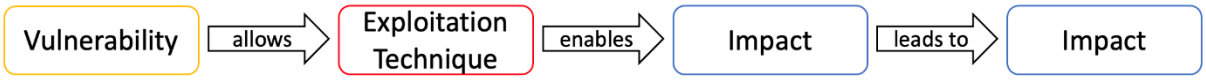
Reprezentace STIX 2.0[6] umožňuje snadno generovat různé vizualizace a reprezentace mapování. Jsou také generovány tabulky aplikace Excel, které obsahují všechna mapování pro každý rámec v tabulkovém formátu.

1.5.2 Integrace zranitelností do MITRE ATT&CK

Další projekt (Baker Nov 2021) definuje metodiku MITRE ATT&CK k charakterizaci dopadu zranitelností uvedených v seznamu CVE (*Common Vulnerabilities and Exposures)*. Techniky ATT&CK poskytují standardní způsob popisu metod, které protivníci používají ke zneužití zranitelnosti, a toho, čeho mohou protivníci zneužitím zranitelnosti dosáhnout. Použití technik ATT&CK k popisu zranitelnosti usnadňuje obráncům integraci zranitelností do jejich modelování hrozeb.

Cílem je umožnit prodejcům, výzkumníkům, databázím zranitelnosti a dalším producentům informací o zranitelnosti standardizovat způsob popisu dopadu zranitelnosti. CVE s referencemi technik ATT&CK mají umožnit obráncům lépe porozumět jejich kompenzačním kontrolám pro daný CVE. V konečném důsledku je tato metodika zaměřena na vytvoření kritického spojení mezi správou zranitelnosti a modelováním hrozeb.

Konkrétní zranitelnost umožňuje útočníkovi použít využívanou techniku k získání primárního dopadu, což zase vede k sekundárnímu dopadu (viz obrázek 1.5.2):



Obrázek 1.5.2: Struktura řetězce od konkrétní zranitelnosti přes použitou techniku k finálnímu dopadu

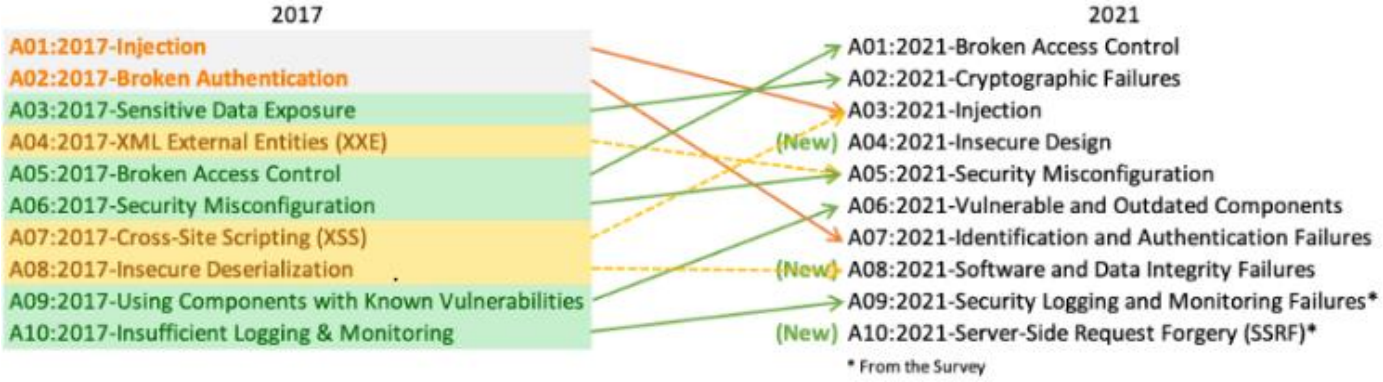
[6] Structured Threat Information Expression (STIX) je jazyk a formát používaný k výměně informací o kybernetických hrozbách.

1.6 Bug Bounty a CTF

1.6.1 Lov na odměny alias Bug Bounty

Zranitelnosti BAC (Broken Access Control – prolomeného řízení přístupu) jsou v dnešních aplikacích běžné, protože programátor musí zajistit fungování programů v rámci různých obchodních, ale i organizačních a právních logik, které si často navzájem odporují. Detekce chyb by v těchto podmínkách musela být nepřetržitá a automatická, což není. Záleží na tom, kdo kontroluje výsledný program pečlivěji, proto se hledají chyby i cestou Bug Bounty.

Téměř o každém nasazení webového serveru a aplikace je známo, že je náchylný k alespoň jedné nefunkční zranitelnosti řízení přístupu. V závislosti na tom, ke kterým zdrojům útočníci získají oprávnění k přístupu, mohou být dopady úspěšného útoku škodlivé. Podle (OWASP 2021) se BAC v rámci TOP 10 OWASP přesunulo v roce 2021 na 1. místo z 5. místa v roce 2017 – viz obr. 1.6.1. Využívá těchto slabin webových aplikací.



Obr. 1.6.1: Posun Broken Access Control z 5. na 1. místo TOP 10 OWASP slabin webových aplikací.

- Porušení zásady nejmenšího privilegia nebo jeho odepření ve výchozím nastavení, kdy by měl být přístup udělen pouze konkrétním schopnostem, rolím nebo uživatelům, ale je dostupný komukoliv.
- Vynechání kontrol řízení přístupu úpravou adresy URL (neoprávněná manipulace s parametry nebo vynucené procházení), vnitřního stavu aplikace nebo stránky HTML nebo pomocí útočného nástroje upravujícího požadavky rozhraní API.
- Povolení zobrazení nebo úpravy účtu někoho jiného poskytnutím jeho jedinečného identifikátoru (nezabezpečené přímé odkazy na objekt).
- Přístupové rozhraní API s chybějícím řízením přístupu pro POST, PUT a DELETE.
- Zvýšení privilegia. Vystupovat jako uživatel bez přihlášení nebo jednat jako admin, když jste přihlášeni jako uživatel.
- Manipulace s metadaty, jako je přehrání nebo manipulace s tokenem řízení přístupu JSON Web Token (JWT), nebo se souborem cookie nebo skrytým polem manipulovaným za účelem zvýšení oprávnění nebo zneužití zrušení platnosti JWT.
- Nesprávná konfigurace CORS (Cross-origin resource sharing, sdílené zdroje odjinud) umožňuje přístup k API z neautorizovaných/nedůvěryhodných zdrojů.

- Vynutit procházení ověřených stránek jako neověřený uživatel nebo privilegovaných stránek jako standardní uživatel.

(Sengupta 2021) odlišuje vertikální a horizontální eskalaci řízení přístupu. Vertikální řízení přístupu se používá k omezení přístupu ke klíčovým funkcím, které nejsou dostupné pro ostatní uživatele v organizaci. Například lze prozkoumat nefunkční ovládací prvky vertikálního přístupu pro přístup k funkcím, ke kterým běžní uživatelé nemají přístup, jako je úprava a mazání uživatelských účtů. Příklady útoků s vertikální eskalací oprávnění z nefunkčních vertikálních řízení přístupu zahrnují: Nechráněné citlivé funkce, útoky založené na parametrech, špatné konfiguraci platformy.

Horizontální řízení přístupu umožňuje různým uživatelům aplikací přistupovat k podobným typům prostředků. Tyto mechanismy omezují přístup ke zdrojům pouze na skupinu uživatelů, kterým je přístup ke zdroji povolen. Například bankovní aplikace umožňuje klientům prohlížet záznamy o jejich transakcích, ale ne o transakcích jiných uživatelů. Poškozené horizontální kontroly přístupu umožňují útočníkům přístup ke zdrojům patřícím jiným uživatelům a jsou způsobeny nesprávnými kontrolami ID daného záznamu v databázi.

Útočníci často kompromitují privilegované uživatele, aby změnili horizontální útoky s eskalací oprávnění na vertikální eskalaci oprávnění. Hackeři mohou například použít poškozené horizontální ovládací prvky k získání přihlašovacích údajů jiného uživatele. Útočníci se pak mohou zaměřit na účty správců, což jim dává práva správce eskalovat vertikálně. Kontextově závislé útoky eskalace oprávnění zahrnují: nezabezpečený přímý odkaz na objekt, vícestupňové útoky, útoky na mechanismy založené na refererech, útoky na mechanismy založené na geografické poloze.

Pro lovce je nejlépe začít registrací na @BugCrowd, @Hacker0x01, @intigriti. Pro zachycení a úpravu požadavků je užitečným nástrojem @Burp_Suite Community Edition, které je zdarma, nejlépe s doplňkem Logger++. Dále je třeba sledovat youtube kanál Bug Bounty Reports Explained na *https://www.youtube.com/c/BugBountyReportsExplained*.

Podle (Anton 2021) je v průběhu testování webu nebo aplikace na chyby BAC užitečné zvýraznit všechny požadavky GET na kritické akce, např. /delete_user?id=1. Požadavky s kritickými akcemi, které lze přímo odeslat uživateli, jsou považovány za chybu zabezpečení CSRF (Cross-Site Request Forgery). Požadavky POST lze také použít k provedení útoku CSRF, ale obvykle mají ochranný mechanismus CSRF (Cross-Site Request Forgery) coby csrf_tokens nebo kontrola odkazujícího zdroje. Ochranu CSRF lze někdy obejít, např. lze přepnout metodu POST na GET nebo odebrat hodnotu tokenu z klíče — csrf_token=

S ochranou referreru[7] se lze pokusit připojit svoji vlastní doménu k referreru v podobě http://example.com.yourdomain.com.

Jako další užitečné opatření při provádění bug bounty huntingu je vložit základní užitečné zatížení do všech možných vstupů: qwe'"<X</. Stačí pak sledovat reflexi textu na webové stránce. Pokud se někde objeví qwe'" (bez lomených závorek) — to by mohla být šance pro XSS.

[7] HTTP referer, resp. referer stránky či referrer, je speciální HTTP záhlaví, ve které webový prohlížeč posílá serveru při vyžádání stránky adresu, ze které se návštěvník na danou stránku dostal. Tj. referer říká, z jaké stránky odkázal na aktuálně zobrazenou stránku.

Kromě toho lze vyhledat text qwe ve zdrojovém kódu stránky. Pro tento úkol lze v prohlížeči použít nástroje pro vývojáře. Některé vstupní užitečné zatížení se mohou projevit v parametrech tagu: <a class="qwe’"<x</"> nebo v samotném prvku <script>: <script> let a = “qwe’”<x</” <script>

Aktuální přehled Bug Bountry programů a webových stránek lze nalézt na *https://www.guru99.com/bug-bounty-programs.html*.

1.6.2 CTF

Události Capture-the-Flag jsou soutěže v počítačové bezpečnosti. Účastníci soutěží ve výzvách s bezpečnostní tématikou za účelem získání nejvyššího skóre. Od soutěžících se očekává, že „zachytí vlajky“, aby zvýšili své skóre, odtud název akce. Vlajky jsou obvykle náhodné řetězce vložené do výzev.

CTF v poslední době stoupla popularita popularitě, protože každý rok přitahují vyšší počet mladých talentů. Pomáhají rozvíjet základní dovednosti potřebné pro kariérní cestu v oblasti kybernetické bezpečnosti. Tyto soutěže mohou mít mnoho podob, ale nejběžnější jsou Jeopardy a Attack-Defence. Zpráva se konkrétně zaměřuje na tyto dva typy CTF. Pro každý z nich je vypracován výklad a analýza formátu, bodování, diskuse a variant. Attack-Defence je více podobný formátům válečných her a je vhodnější pro profesionální tréninková cvičení. Díky dostupnosti a nižším nákladům na nasazení je naopak formát Jeopardy vhodnější pro neprofesionální účastníky.

Jeooardy (ohrožení) zahrnuje výzvy založené na kategoriích. Kategorie jsou následující:
1. OSINT — Open Source Intelligence
2. Kryptografie
3. Využívání webu
4. Forenzní a steganografie
5. Binární využití (PWN)
6. Reverzní inženýrství
7. Různé
8. Hardware

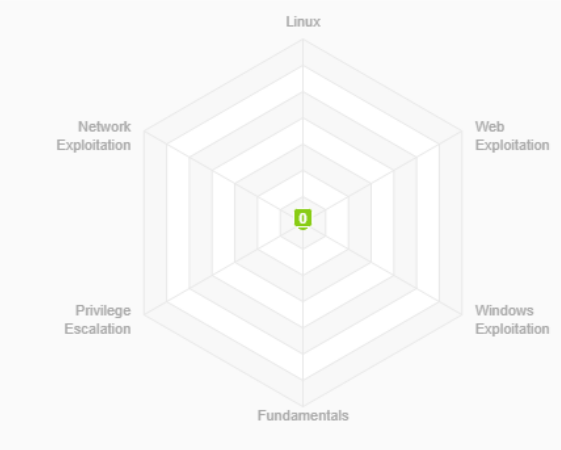
Jednotlivé CTF se liší podle druhu analýzy a použité metodologie. Prvky soutěže jsou:

- vstupní požadavky: údaje o věku, stavu, kvalifikaci, umístění atd.;
- rozmanitost a začlenění: vyvážené zastoupení žen a mužů, socioekonomické zázemí nebo etnické poměrné zastoupení atd.;
- Formát výzvy: zkoumá kategorie výzev, bodování, použitou platformu, ceny, délku soutěže atd.;
- formát soutěže: analyzuje informace o velikostech týmů, mentorech a trenérech, kvalifikacích nebo paralelních soutěžích;
- organizace akce: zabývá se dalšími organizovanými aktivitami, jako je stravování a doprava nebo poskytovaná ubytovací zařízení;
- akce po události: zkoumá akce provedené po události, jako je distribuce výzev a řešení, zveřejnění dat o výsledcích nebo následné publikace.

V souvislosti se zkoumanými tématy a oblastmi jsou uvedena doporučení. Například formáty by měly být vybrány podle publika, pro které je soutěž určena.

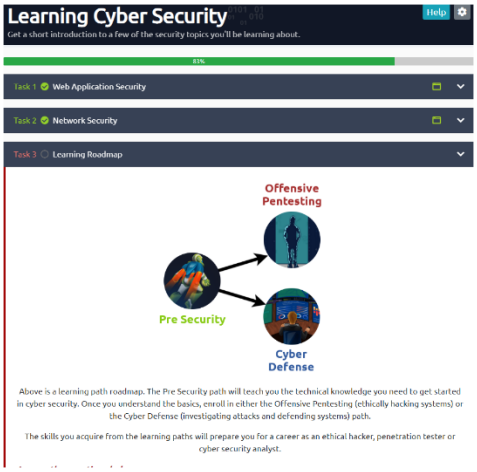
1.6.3 TryHackMe

Tryhackme funguje na úrovni systému. To se také přenese na Discord server[8] (pro členy). Úrovně se získávají hraním místností na webu. Za každou otázku, kterou vyplníte, získáte určitý počet bodů. Výzvové místnosti dávají více bodů než průchozí místnosti a nedávné místnosti stále dávají více bodů. V současné době existuje 13 úrovní a šest oblastí působnosti – viz obr. 1.6.3.1.



Obr. 1.6.3.1: Šest oblastí Skill Matrix TryHackMe

Z hlediska bezpečnosti si je po Pre security třeba vybrat mezi dvěma zaměřeními – viz obr. 1.6.3.2.



Obr. 1.6.3.2: Bezpečnostní rozcestí oblasti Cyber Security

Poslední novinkou je Výuková cesta Jr Penetration Tester, již bude věnována další podkapitola.

Výuková cesta Jr Penetration Tester

Jde o způsob, jak se naučit základy (a některé pokročilé koncepty) etického hackingu a penetračního testování. Tato výuková cesta se skládá ze sedmi sekcí místností, z nichž každá se specializuje na vlastní oblast

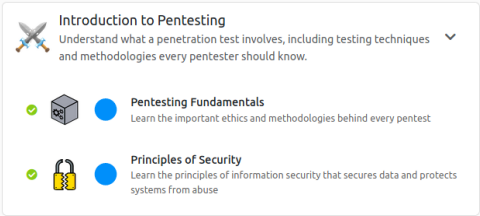
[8] Servery jsou prostory na Discordu. Vytvářejí je konkrétní komunity a skupiny přátel. Každý uživatel může zdarma spustit nový server a pozvat na něj své přátele. Discord servery jsou organizovány do textových a hlasových kanálů, které se obvykle věnují konkrétním tématům a mohou mít různá pravidla.

penetračního testování. Lze se zaregistrovat FREE, ale ne všechny místnosti jsou zdarma (viz https://tryhackme.com/why-subscribe):

	Free	Premium
Personal hackable instances	✓	✓
Hacking challenges	✓	✓
Learning content	Free Rooms Only	All Rooms
Full access to learning paths	✗	✓
Web-based AttackBox & Kali	1 hour a day	Unlimited
Access to Networks	✗	✓
Faster Machines	✗	✓
Private OpenVPN Servers	✗	✓
Private King of the Hill Games	✗	✓

Kurz vyžaduje jedinou předběžnou znalost, a to Základy Javascriptu. Blbé je, že to bez varování zjistíte až když uváznete v 8. místnosti 2. sekce, pak musíte postup přerušit a pustit se do kurzu JavaScripts Basics (*https://tryhackme.com/room/javascriptbasics*). Tedy kdo to čte, tak už ne.

Sekce 1: Pentesting



Pentesting

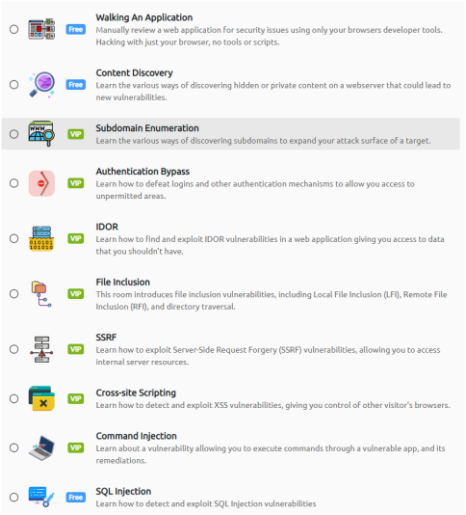
První sekce místností slouží jako stručný úvod do světa penetračního testování. Na konci budete rozumět tomu, co penetrační test zahrnuje, včetně testovacích technik a metodik, které by měl znát každý pentester.

První místnost, **Pentesting Fundamentals** (*https://tryhackme.com/room/ pentesting fundamentals*), poskytuje přehled o důležité etice a metodice každého pentestu. Než se ponoříte do technických věcí, musíte pochopit povinnosti, které máte jako penetrační tester, a procesy, které musíte dodržovat.

Charakterizovány jsou různé typy hackerů, důležitost pravidel zapojení, typy penetračního testování a formální rámce, které skuteční penetrační testeři každodenně používají.

Druhá místnost, **Principles of Security** (*https://tryhackme.com/room/principlesofsecurity*), žáky probírá principy informační bezpečnosti a způsoby, jak jsou systémy zabezpečeny. Žáci si zopakují, co je triáda CIA, principy soukromí a dva hlavní bezpečnostní modely, kterými se řídí informační systémy: model Bell-LaPadula a model Biba. Také pochopí, jak to souvisí s modelováním hrozeb a reakcí na incidenty, když se podíváte na STRIDE a PASTA, které se používají k nastínění různých metod útoku, a CSIRT, který je často označován jako šest fází reakce na incidenty.

Sekce 2: Introduction to Web Hacking



Web Hacking

Nyní se přejde od teorie do praktických místností. Ve 2. sekci tvořené deseti místnosti se žáci dozví o (a zneužijete) některé z nejpopulárnějších zranitelností webu v dnešním světě.

První místnost 2. sekce **Walking an Application** (*https://tryhackme.com/room/ walkinganapplication*) naučí, jak ručně kontrolovat webovou aplikaci a hledat potenciální bezpečnostní problémy. K tomu slouží pouze nástroje, které jsou k dispozici v prohlížeči, jako je například View Source, a nástroje pro vývojáře (Inspector, Debugger, Network atd.).

Druhá místnost 2. sekce **Content Discovery** (*https://tryhackme.com/room/contentdiscovery*) naučí způsoby odhalování skrytého/soukromého obsahu uloženého na webovém serveru, který by mohl vést k potenciálním bezpečnostním problémům. To zahrnuje prohlížení souborů Robots.txt, Sitemap.xml, záhlaví HTTP pro ruční zjišťování a používání různých zdrojů s otevřeným zdrojovým kódem pro OSINT (Open-Source Intelligence), jako jsou Google Dorks, Wappalyzer (*https://www.wappalyzer.com/*), Wayback Machine (*https://archive.org /web/)* a další. Také vás seznámí s automatickým objevováním pomocí ffuf, dirb a gobuster.

Pomocí těchto nástrojů se pak ve třetím místnosti **Subdomain Enumeration** (*https://tryhackme.com/why-subscribe* – dosud bylo vše free, nyní již jsme v placené verzi) seznámíte s Enumerací subdomén, což je proces hledání platných subdomén pro danou doménu. Je to proto, abyste mohli rozšířit svou útočnou sféru a najít další potenciální zranitelnosti. Proberou se zde tři hlavní způsoby, jak toho dosáhnout: OSINT, Bruteforce a virtuální hostitelé.

Pokud chcete vyčíslit a shromáždit informace o dané doméně, musíte vědět, jak ji využít a přimět ji, aby dělala věci, k nimž nebylo zamýšleno. Čtvrtá (placená) místnost **Authentication Bypass** naučí, jak lze obejít metody ověřování webových stránek pomocí ffuf a curl. Tyto chyby zabezpečení jsou často kritické a vedou k úniku osobních údajů.

Dále se naučíte, jak lokalizovat a zneužít zranitelnosti **IDOR** (Insecure Direct Object Reference) (5., zase placená místnost). Tyto chyby zabezpečení umožňují přístup k datům, která byste neměli mít. To se někdy stává, když webový server obdrží uživatelsky dodaný vstup pro příjem objektů, jako jsou soubory nebo dokumenty. V těchto případech se

příliš důvěřuje datům dodaným uživatelem, a proto nejsou na straně serveru řádně ověřena, což vede k chybám zabezpečení.

Tato místnost pěkně vede do placené 6. místnosti **File Inclusion**. Poskytuje příklady jak Local File Inclusion (LFI) tak Remote File Inclusion (RFI) a umožňuje vám prokázat tyto znalosti prostřednictvím speciálně vytvořené virtuální laboratoře.

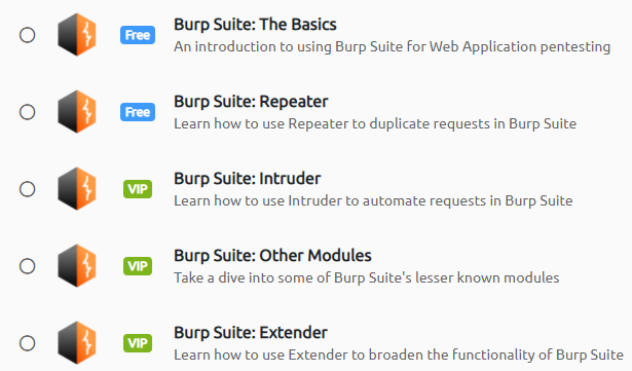
Poté se v sedmé místnosti 2. sekce (také placený) dozvíte o **SSRF** (Server-Side Request Forgery – 7. (opět placená) místnost 2. sekce, které vám umožní přimět webový server, aby provedl další nebo upravený HTTP požadavek na zdroj útočníka. Poskytuje vám znalosti o tom, jak najít tato zranitelná místa a jak porazit běžné obranné mechanismy.

Poté přejdete na placené informace o **Cross-Site Scripting** (XSS) – 8. místnost 2. sekce. Tato místnost vyžaduje základní znalosti JavaScriptu, je to stále skvělá místnost pro začátečníky, aby se naučili, jak lze tyto chyby zabezpečení použít k převzetí kontroly nad prohlížeči jiných uživatelů. Chce to hluboce se ponořit do každého typu XSS a do toho, jak vyvinout své užitečné zatížení XSS, a umožní vám předvést své dovednosti proti zranitelné webové aplikaci.

Dále se dozvíte v deváté místnosti (placené) dozvíte o **Command Injection**, který vám umožňuje spouštět příkazy prostřednictvím zranitelné webové aplikace. Tato místnost vás naučí, jak tyto zranitelnosti odhalit a otestovat, a také jak zabránit výskytu tohoto typu zranitelnosti. Nakonec si tuto teorii procvičíte provedením injekce proti zranitelné aplikaci.

Nakonec se dozvíte, jak detekovat a zneužít zranitelnost SQL Injection (SQLi) – je to od první free room, viz *https://tryhackme.com/room/sqlinjectionlm* (od třetí do deváté místnosti šlo o placené přístupy). Tento útok zahrnuje odesílání škodlivých dotazů, které jsou prováděny na webovém serveru. Jedná se o velmi běžnou zranitelnost vyskytující se ve většině webových aplikací a může vést ke ztrátě a/nebo krádeži citlivých dat. Naučíte se různé typy SQLi, včetně in-band a blind, stejně jako techniky nápravy, které vývojáři používají k ochraně svých aplikací.

Sekce 3: Burp Suite



BurpSuite

Ve třetí sekci se dozvíte, jak používat Burp Suite pro penetrační testy webových aplikací. Burp Suite je nástroj, který se v průmyslu široce používá k testování bezpečnostních mechanismů webových aplikací.

V prvním místnosti, **Burp Suite: The Basics** (*https://tryhackme.com/module/learn-burp-suite*), se seznámíte se základy nástroje, včetně toho, jak jej nainstalovat a nastavit, jeho funkce a jak se provádějí základní útoky.

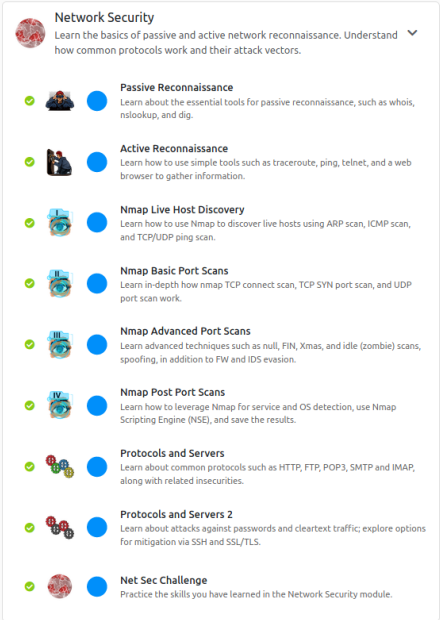
Dále se naučíte, jak používat **The Repeater** (https://tryhackme.com/room/burpsuiterepeater) k duplikování požadavků. Tímto způsobem vytvoříte a/nebo přenesete zachycené požadavky do webové aplikace. Běžně se to například používá k testování zranitelností SQL Injection, obcházení filtrů brány firewall nebo ke změně parametrů při odesílání formuláře.

Poté třetí místnost 3. sekce **Burp Suite: Intruder** (jsme už zase až do konce u placené verze) probírá, jak používat Intruder k automatizaci požadavků. Intruder je vestavěný nástroj Burp Suite pro fuzzing a lze jej použít k fuzz pro subdomény, koncové body nebo virtuální hostitele a k brutálnímu vynucení přihlašovacích formulářů výměnou uživatelských jmen a hesel pomocí seznamu slov.

4. místnost 3. sekce **Burp Suite: Other Modules** poskytne stručný přehled dalších funkcí sady Burp Suite. Konkrétně se zaměřuje na Decoder, Comparer a Sequencer, které umožňují kódovat a porovnávat sady textu, analyzovat zachycené tokeny.

Nakonec se v 5. místnosti sekce naučíte používat **Extender**, který vám umožní rozšířit stávající funkčnost Burp Suite prostřednictvím různých modulů.

Sekce 4: Network Security



Network Security

Přejdeme-li od webových aplikací, v této další části se naučíte základy pasivního a aktivního shromažďování síťových informací. Na konci budete dobře rozumět sítím, jejich protokolům, jak fungují a jak jsou napadány.

V první místnosti 4. sekce se dozvíte o **Passive Reconnaissance**. Tato místnost pokrývá různé nástroje, jako je whois, nslookup a dig, a jak se každý používá ke shromažďování informací o cíli.

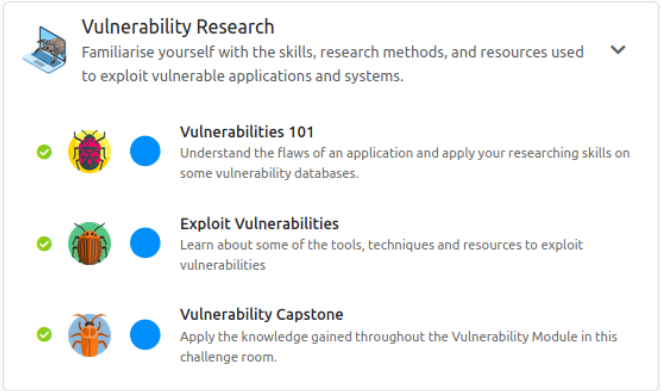
V návaznosti na to pochopíte, jak používat jednoduché nástroje, jako je traceroute, ping, telnet, a dokonce i webový prohlížeč k provádění aktivního průzkumu v druhé místnosti 4. sekce **Active Reconnaissance**.

Další čtyři místnosti (3.–6.) pokrývají Nmap. První vás naučí, jak provádět zjišťování hostitele pomocí skenování ARP, skenování ICMP a skenování ping TCP/UDP. Druhý vám řekne, jak provést základní skenování portů, a poskytne vám podrobné znalosti o tom, jak funguje skenování TCP connect, TCP SYN port a UDP port. Dále se naučíte různé pokročilé skenování portů, jako je null, FIN, Xmas a nečinné (zombie), stejně jako pokročilé techniky, jako je spoofing a vyhýbání se systému IDS (Intrusion Detection System). Nakonec se naučíte různé funkce Post Port Scans, včetně toho, jak používat Nmap pro detekci služeb a OS a také používat vestavěný skriptovací modul Nmap k výčtu konkrétních hostitelů a služeb.

V návaznosti na to vám další dvě místnosti (7. až 8.) poskytnou důkladné pochopení běžných protokolů, běžných síťových útoků a technik zmírňování. Konkrétně první **Protocols and Servers 1** vás naučí o HTTP, FTP, POP3, SMTP a IMAP a také o jejich příslušných zranitelnostech. Druhá část **Protocols and Servers 2** pokrývá běžné útoky na hesla a jak provádět útoky typu Man-in-the-Middle (MITM) a pokrývá také Transport Layer Security (TLS) a Secure Shell (SSH).

Nakonec tuto část uzavírá **Net Sec Challenge**. V této místnosti budete muset použít své dovednosti, které jste se naučili, k vyjmenování hostitele a nalezení skrytých informací v záhlavích zpráv HTTP a SSH a využít FTP server k nalezení příznaků.

Sekce 5: Vulnerability Research



Vulnerability Research

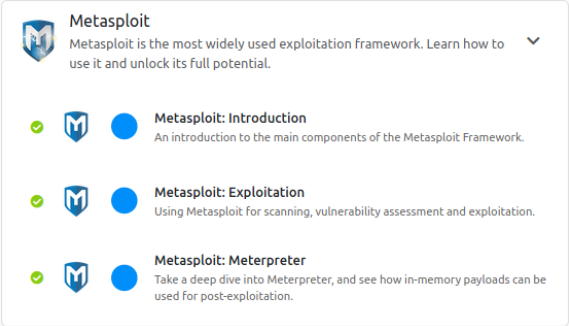
Poté, co si osvojíte zabezpečení sítě, můžete se seznámit se zdroji, které se používají ke zneužití zranitelných systémů a aplikací.

V první místnosti 5. sekce, **Vulnerabilities 101**, budete mít obecný přehled o tom, co je zranitelnost, jak jsou hodnoceny a jaké existují zdroje/rámce, které přispívají k výzkumu zranitelnosti. Konkrétně tato místnost pokrývá CVSS (Common Vulnerability Scoring System) a VPR (Vulnerability Priority Rating) – dvě běžné metody používané k hodnocení zranitelností. Pojednává také o online databázích zranitelnosti, jako je NVD (National Vulnerability Database) a Exploit-DB.

Další místnost, **Exploit Vulnerabilities**, vás naučí o některých nástrojích a technikách používaných ke zneužití zranitelností. Dozvíte se o automatizovaných a manuálních výzkumných technikách a také o tom, jak ručně využít cílovou webovou aplikaci prostřednictvím dříve zmíněných online zdrojů.

Nakonec tyto znalosti uplatníte v místnosti **Vulnerability Capstone**. V této místnosti vyjmenujete zranitelnou webovou aplikaci a najdete zranitelnost na základě informací o verzi spuštěné aplikace. Tuto chybu zabezpečení pak použijete ke vzdálenému spuštění kódu v systému a získání příznaku.

Sekce 6: Metasploit



Metasploit

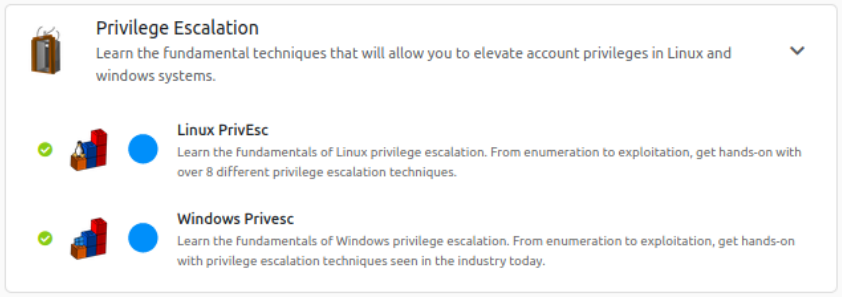
Nyní se dozvíte o Metasploitu a o tom, jak jej používat pro exploataci a po exploataci.

Metasploit: Introduction vám poskytne obecný přehled o hlavních komponentách Metasploit, jako je msfconsole, její moduly a nástroje. Poskytuje vám praktické zkušenosti s interakcí s moduly a s tím, jak je nakonfigurovat pro konkrétní cíle.

Dále se naučíte používat **Metasploit: Exploitation**. To pokrývá základy skenování, hodnocení zranitelnosti a jak generovat užitečné zatížení pomocí msfvenom pro zneužití cílového systému. Každá technika je také doprovázena interaktivní laboratoří, takže můžete uplatnit své znalosti a využívat skutečné moduly a exploity.

Nakonec se dozvíte, jak **Metasploit: Meterpreter** funguje, jak používat užitečnou zátěž pro post-exploitaci a jak používat příkazy meterpreteru k procházení zneužitým systémem.

Sekce 7: Privilege Escalation



V tomto závěrečném modulu se naučíte techniky, které vám umožní eskalovat vaše oprávnění v systémech Linux i Windows. Na konci tohoto budete pohodlněji procházet systémem a porozumíte procesu eskalace privilegií.

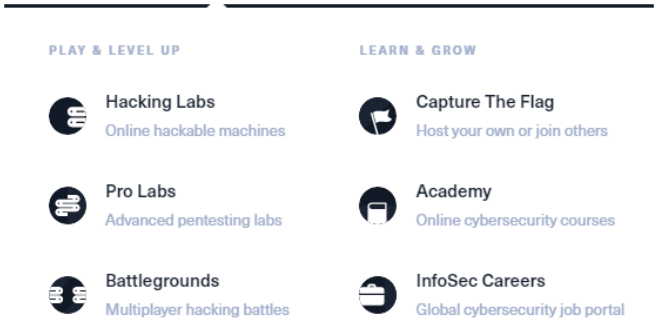
V první místnosti poslední sekce se dozvíte o **Linux Privilege Escalation**. Zde pokryjete základní výčet a běžné techniky eskalace privilegií prostřednictvím interaktivních laboratoří. Konkrétně se naučíte, jak zvýšit svá oprávnění prostřednictvím exploitů jádra, sudo, SUID, úloh cron, PATH a NFS.

Nakonec se dozvíte o **Windows Privilege Escalation**. Zejména se dozvíte, jak vytvořit výčet uživatelů v systémech a jak eskalovat oprávnění prostřednictvím zranitelného softwaru, únosu DLL (DLL hijacking) a token impersonation.

Shrnutí: TryHackMe je vyvíjeno komunitou a jednotlivé místnosti mají různou a mnohdy nesjednocenou úroveň. Poskytuje stovky místností a další výukové cesty k rozšíření znalostí uživatelů, řada místností je zdarma, ale vynechání placených částí může vést k fragmentaci znalostí. Uspořádání studia do cest má své výhody i nevýhody, výhodou je logické uspořádání, nevýhodou že na té cestě snadno uváznete i na nějakém okrajovém problému. Systém se postupně rozvíjí a chybí informace o záměrech zpracovatelů do budoucna.

1.6.4 Hack the Box

Hack The Box je online platforma, která vám umožňuje otestovat své dovednosti v oblasti penetračního testování a vyměňovat si nápady a metodiky s dalšími členy s podobnými zájmy. Obsahuje několik výzev, které jsou neustále aktualizovány. Některé z nich simulují scénáře reálného světa a některé z nich se přiklánějí spíše k výzvám ve stylu CTF – viz obr. 1.6.4.



Obr. 1.6.4: Struktura platformy Hack The Box

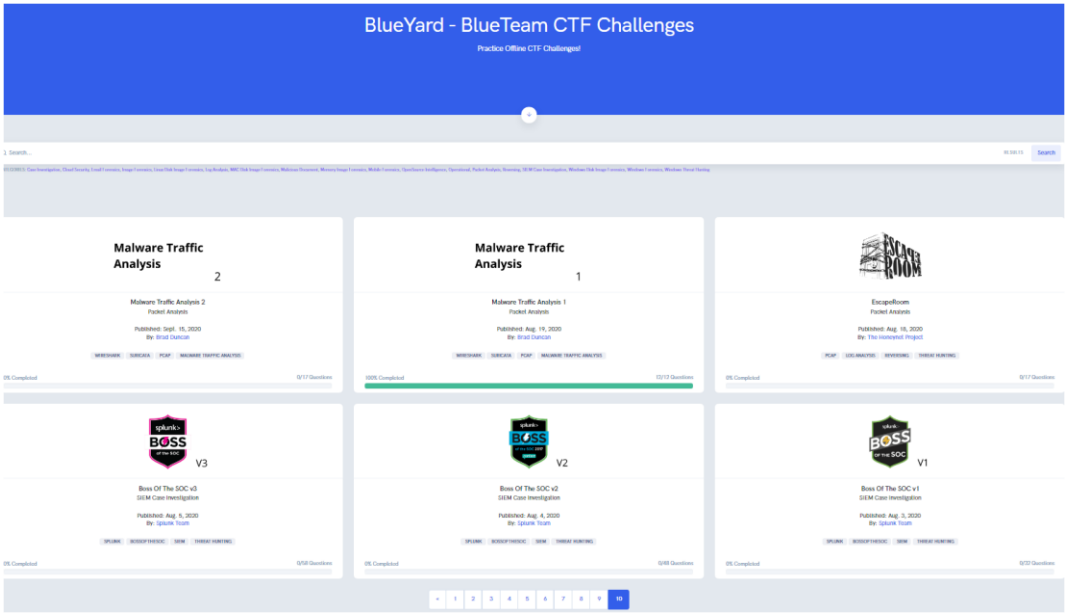
Jako jednotlivec můžete splnit jednoduchou výzvu k prokázání svých dovedností a poté si vytvořit účet, který vám umožní připojit se k privátní síti (HTB Net), kde na vás čeká několik strojů, abyste je mohli hacknout. Hackováním strojů získáváte body, které vám pomohou postoupit v žebříčku.

2 Praktická část

2.1 Malware Traffic Analysis 1 z BlueYard – BlueTeam CTF Challenges

Cyberdefenders.org je školicí platforma zaměřená na defenzivní stránku kybernetické bezpečnosti, jejímž cílem je poskytnout modrým týmům místo k procvičování, ověřování dovedností, které mají, a získávání těch, které potřebují. Platforma poskytuje tři základní služby: platformu živého hostování CTF (BlueRing), platformu profesionálního školení (BlueDemy) a oblast praktického cvičení (BlueYard).

BlueYard is je komunitní iniciativa ke shromažďování archivovaných výzev BlueTeam na jednom místě, aby se usnadnilo bezpečnostním profesionálům procvičování s kvalitními zdroji a aby tyto výzvy mohly žít navždy. Když živé CTF skončí na BlueRing, výzvy CTF se přesunou do BlueYard (obr. 2.2.1), aby byly přístupné.



Obr. 2.1.1: Úlohy praktického cvičení (BlueYard).

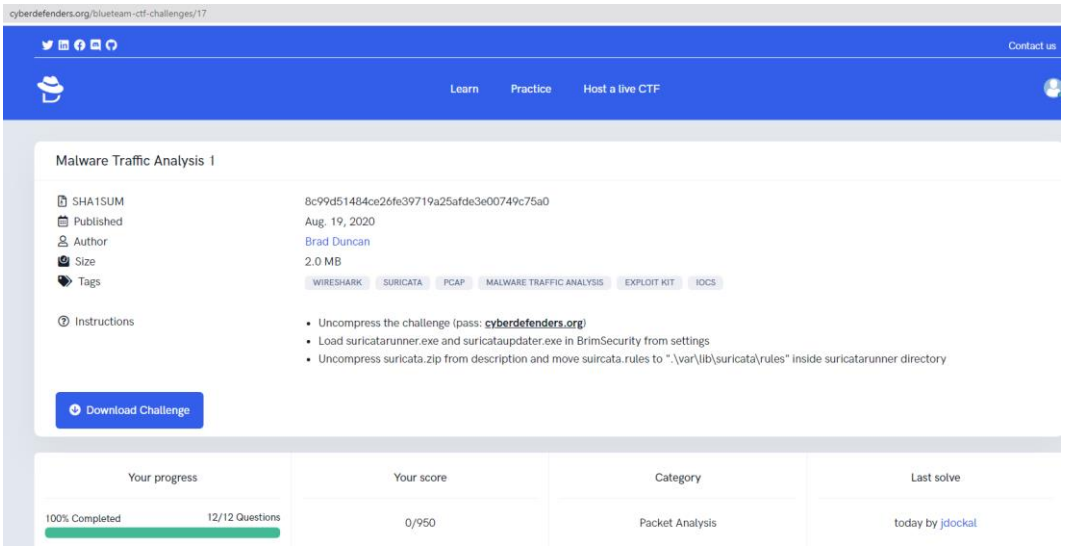
Každá výzva má svůj scénář a seznam otázek. Správné zodpovězení otázek vyžaduje projít scénářem vyšetřování, analyzovat data a extrahovat správné informace. BlueYard – viz obr. 1 je zcela zdarma ke hraní. BlueRing je zdarma pro vzdělávací instituce a neziskové organizace. Poplatky za školení BlueDemy jsou vyšší – za čtyřdenní online kurz 1800 USD.

Cílem každého cvičení je získat potřebný počet bodů viz obr. 2.1.2, za každou pomocnou otázku se snižuje jejich počet – příklad je na obr. 2.1.3. Nahlédnutí do nahrávek řešení úlohy však vede ke zmrazení získávání bodů.

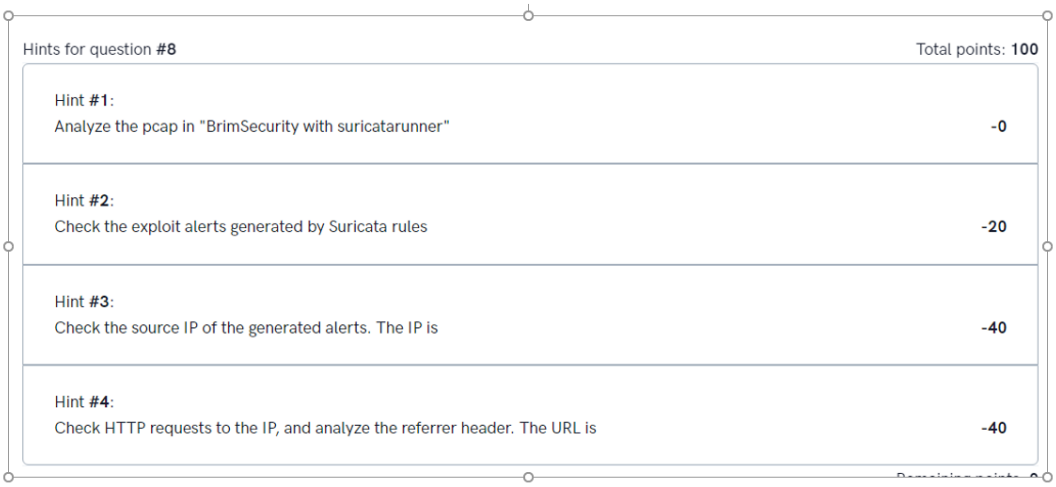
Předmětem zvoleného cvičení bude úloha Malware Traffic Analysis 1 z https://cyberdefenders.org/blueteam-ctf-challenges/17.

Cvičení poskytuje člověku znalosti v oblastech:

- Jak dochází k toku síťového provozu mezi klientem a serverem.
- Jak fungují určité protokoly a jaký je jejich účel.
- Typ a podpis několika malwarů.



Obr. 2.1.2: Čelní stránka zadání úlohy



Obr. 2.1.3: Nápověda za cenu ztráty bodů

V rámci úlohy řešitel obdrží PCAP Exploitation Kit obsahující infekci (s příspěvkem je třeba pracovat nejlépe ve virtuálním prostředí). Úkolem je provést pomocí nástrojů analýzu a odpovědět na 13 otázek:

1. URL úlohy: https://cyberdefenders.org/blueteam-ctf-challenges/17
2. Jaká je IP adresa virtuálního počítače se systémem Windows, který je infikován?
3. Jaký je název hostitele virtuálního počítače se systémem Windows, který je infikován?
4. Jaká je MAC adresa infikovaného virtuálního počítače?
5. Jaká je IP adresa napadeného webu?
6. Jaké je FQDN napadeného webu?
7. Jaká je IP adresa serveru, který doručil exploit kit a malware?
8. Jak zní úplný název domény, který dodal exploit kit a malware?
9. Jaká je adresa URL přesměrování, která ukazuje na vstupní stránku exploit kitu (EK)?
10. Kromě CVE-2013-2551 IE exploitu byl EK zaměřena na jinou aplikaci a začíná na „J“. Zadejte celý název aplikace.
11. Kolikrát byla zátěž dodána?
12. Napadený web obsahuje škodlivý skript s adresou URL. Co je to za URL?
13. Rozbalte dva soubory přenášené exploity. Napište MD5 hashe souborů těchto souborů (oddělené čárkou).

Potřebnými nástroji pro danou úlohu jsou:

- BrimSecurity
- suricatarunner
- suricata.pravidla
- NetworkMiner
- WireShark

V záložce Challenge WriteUp je sada záznamů postupu řešení, které mohou posloužit jako vhodný návod pro řešen.

V záložce Setup Guide je k dispozici nahrávka ukázky práce s BrimSecurity a Suricata (*https://www.youtube.com/watch?v=QsyEK5HjP5M&t=14s*) – viz obr. 2.1.4.

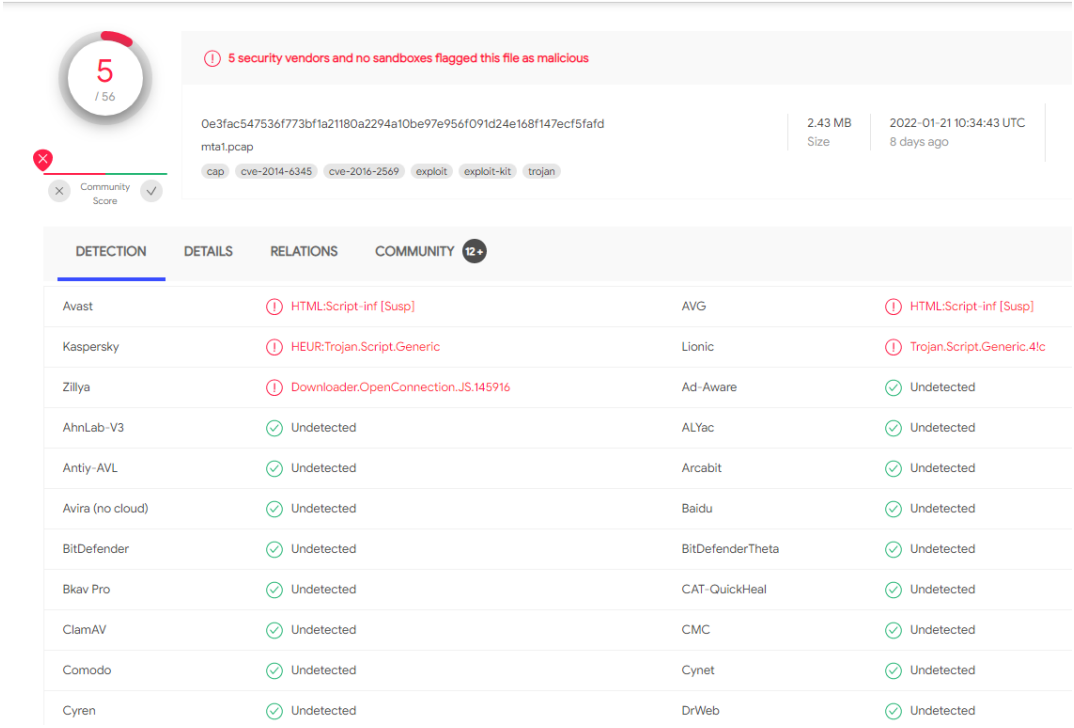
Obr. 2.1.4: Ukázka práce s BrimSecurity a Suricata

Pro praktickou práci je třeba umět z WireSharku extrahovat soubor. Součástí zadání je malware, který bude třeba otestovat pomocí softwaru Virus Total – viz obr. 2.1.5 a ověřit hodnotu hashe – obr. 2.1.6 a obr. 2.1.7.

Text Filter:

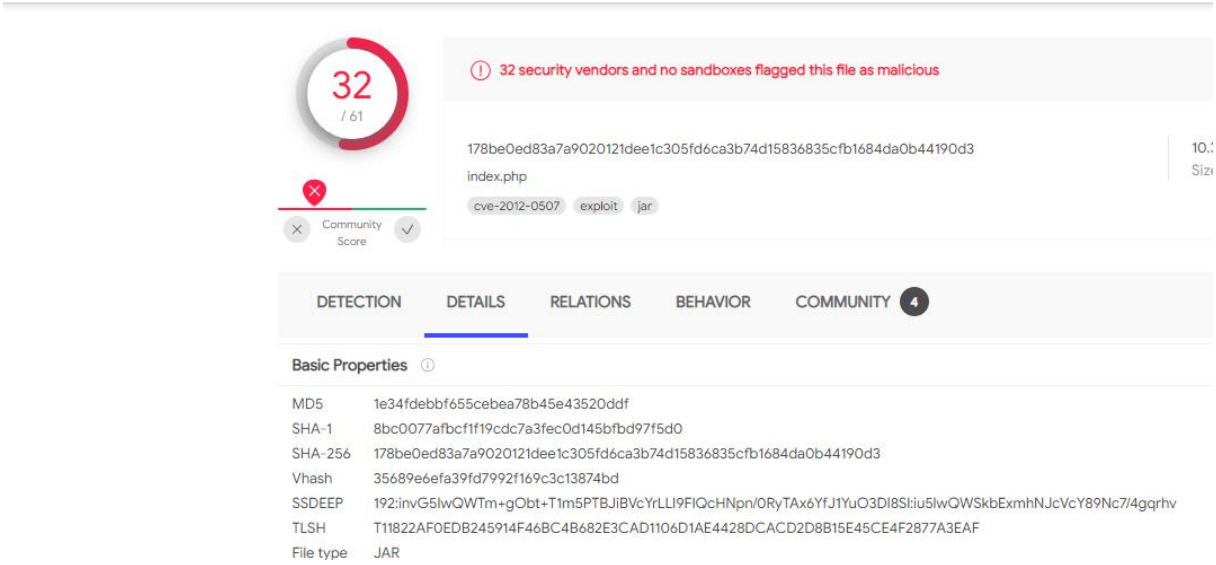
Packet	Hostname	Content Type	Size	Filename
52	www.bing.com	text/xml	948 bytes	lsp.aspx
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75&&ID=SERP,5091.1
311	www.cinihollland.nl	text/css	927 bytes	styles.css?ver=3.7.2
313	www.cinihollland.nl	text/javascript	237 bytes	functions.js
314	www.cinihollland.nl	text/css	702 bytes	page-list.css?ver=4.2
318	www.cinihollland.nl	text/html	61 kB	\
340	www.cinihollland.nl	text/css	4807 bytes	style.css
341	www.cinihollland.nl	text/javascript	7200 bytes	jquery-migrate.min.js?ver=1.2.1
401	www.cinihollland.nl	text/css	1092 bytes	reset.css
432	www.cinihollland.nl	text/javascript	8913 bytes	scripts.js?ver=3.7.2
445	www.cinihollland.nl	text/javascript	16 kB	jquery.form.min.js?ver=3.50.0-2014.02.05
495	adultbiz.in	text/html	8638 bytes	jquery.php
533	www.cinihollland.nl	text/javascript	93 kB	jquery.js?ver=1.10.2
569	www.cinihollland.nl	image/gif	1270 bytes	youtubelogo_on.gif
572	www.cinihollland.nl	image/gif	577 bytes	twitter_on.gif
573	www.cinihollland.nl	image/gif	536 bytes	facebook_on.gif
595	www.cinihollland.nl	image/gif	4660 bytes	br_logo.gif
596	www.cinihollland.nl	image/gif	2476 bytes	newsletter_on.gif
597	www.cinihollland.nl	image/gif	2316 bytes	donate_on.gif
598	www.cinihollland.nl	image/gif	65 bytes	squareorangedecor.gif
654	www.cinihollland.nl	image/jpeg	19 kB	P1260499-200x298.jpg
661	www.cinihollland.nl	image/jpeg	10 kB	IMG-20130928-WA002-150x150.jpg
976	www.cinihollland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico
1074	24corp-shop.com	text/html	890 bytes	\
1079	24corp-shop.com	text/html	890 bytes	\
1356	24corp-shop.com	image/gif	68 kB	notfound.gif
1554	stand.trustandprobaterealty.com	text/html	257 kB	?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM
1566	stand.trustandprobaterealty.com	text/html	255 kB	?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM

Obr. 2.1.5: Příklad extrakce souboru z WireSharku (**File** > Export > Objects > http)



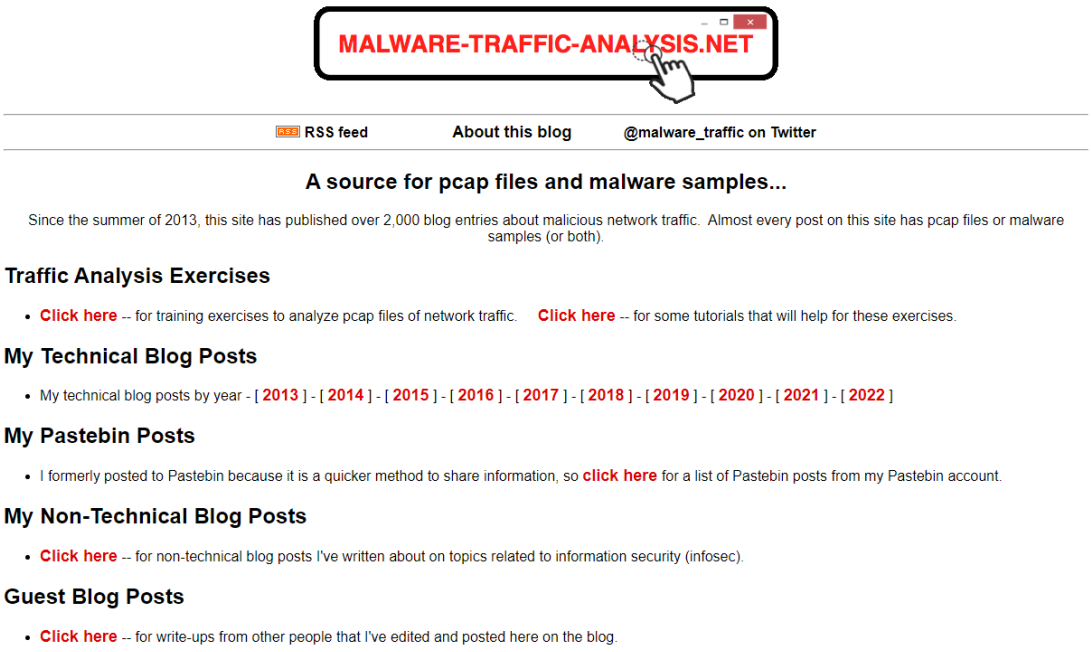
Obr. 2.1.6: Testování souborů pomocí softwaru Virus Total na přítomnost virů

178be0ed83a7a9020121dee1c305fd6ca3b74d15836835cfb1684da0b44190d3



Obr. 2.1.7: Kontrola hodnoty hashe

Autor úlohy Brad Duncan zpracoval pro BlueYard v roce 2020 šest úloh a poskytuje na svých stránkách *https://www.malware-traffic-analysis.net/* celou řadu dalších úloh pro cvičení modrých týmů – viz obr. 2.1.8.



Obr. 8 https://www.malware-traffic-analysis.net/

2.2 WPA2 PSK Cracking z https://www.attackdefense.com/

Na https://www.attackdefense.com/freelabs je sada komunitních úloh, zde byla vybrána úloha s URL https://www.attackdefense.com/challengedetails?cid=41

2.2.1 Zadání

WPA2-PSK je z hlediska zabezpečení robustnější než WPA-PSK. Je však také náchylný ke slovníkovým/bruteforce útokům stejně jako WPA-PSK. Norma bohužel neřešila problém, pokud uživatelé zvolili slabé přístupové fráze.

PCAP soubor lze nalézt v domovské složce uživatele. Obsahuje provoz z SSID zabezpečeného WPA2-PSK „SecurityTube“. Cíl cvičení je jednoduchý – zahájit crackingový útok a nalézt použitou předsdílenou přístupovou frázi.

Seznam milionu hesel: *https://github.com/duyetdev/bruteforce-database/blob/master/1000000-password-seclists.txt*

2.2.2 Řešení

Krok 1: Pomocí airodump-ng načtěte soubor PCAP.

Příkaz: airodump-ng -r WPA2-PSK.pcap

```
CH  0 ][ Elapsed: 1 min ][ 2022-02-06 20:12 ][ Finished reading input file WPA2-PSK.pcap.

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:91:D2:8E:25    0        1        4    0   1  54 . WPA2 CCMP   PSK  SecurityTube

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:21:91:D2:8E:25  60:FB:42:D5:E4:01    0    0e- 0e     0        4
```

Existuje jedno SSID s BSSID 00:21:91:D2:8E:25 a jeden klient 60:FB:42:D5:E4:01

Krok 2: Použijte aircrack-ng k zahájení útoku s daným seznamem slov.

Příkaz: aircrack-ng -w 1000000-password-seclists.txt -b 00:21:91:d2:8e:25 WPA2-PSK.pcap

```
                              Aircrack-ng 1.2 beta3

                    [00:00:02] 980 keys tested (351.33 k/s)

                           KEY FOUND! [ abcdefgh ]


      Master Key     : 5D B7 72 0E 01 FC AC 7F D1 FD 7D E6 A0 BA 8A 21
                       90 04 67 F9 39 BA 09 20 EA 02 A8 40 F5 0F D1 00

      Transient Key  : 3B 60 85 33 C0 FA 16 BE 90 B2 F5 44 89 D9 2E 10
                       63 1B 1A A7 D9 54 99 89 17 27 83 62 18 B6 9E C3
                       F9 85 39 8A A9 5A 85 CE 47 76 80 EC 93 EB 98 17
                       EE EA CE E6 72 9E F5 E6 B8 2B AD B8 F8 09 C7 B5

      EAPOL HMAC     : A1 C8 27 BC 9E 56 BD A2 3B 58 CA 8F 73 51 A7 38
student@attackdefense:~$
```

Flag: abcdefgh

Použitý zdroj: Aircrack-ng (*https://www.aircrack-ng.org/*)

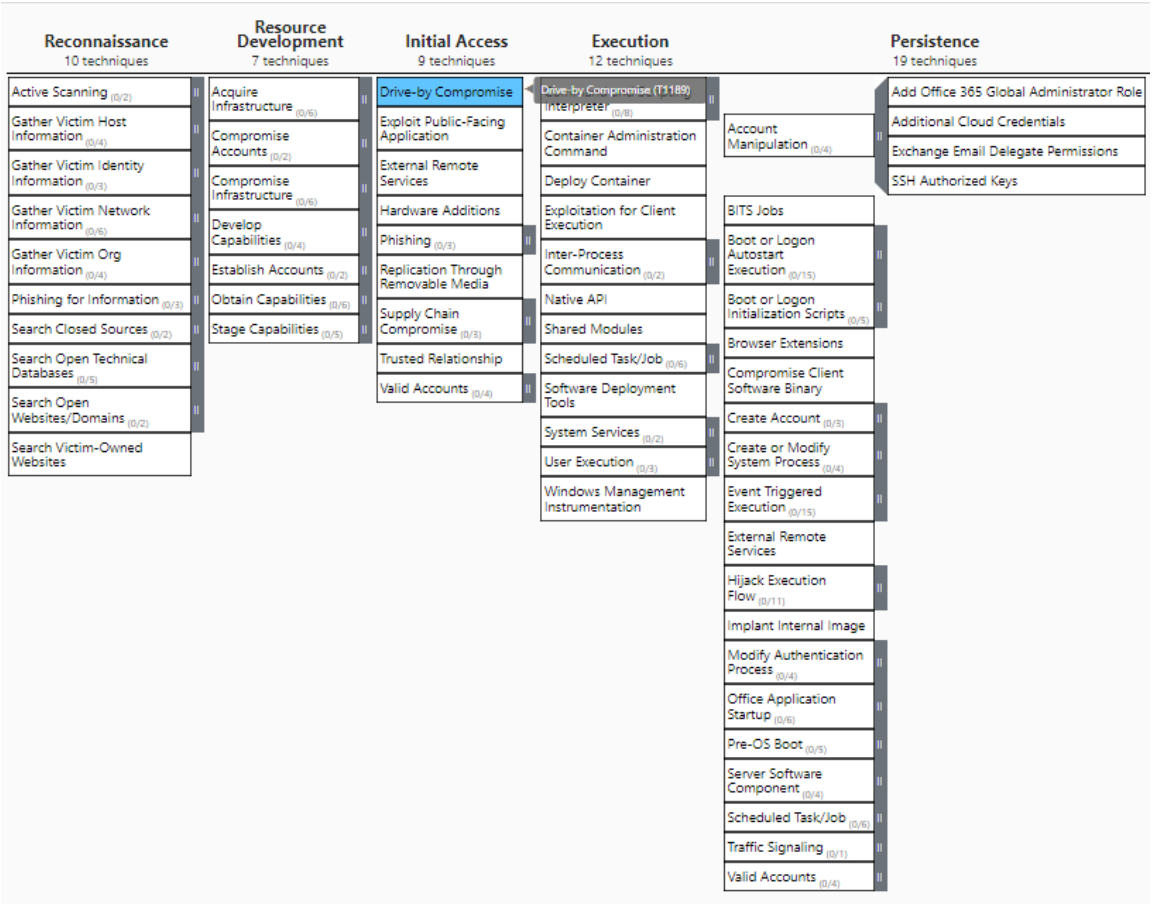
2.3 Práce s ATT&CK Navigatorem

2.3.1 Vzorový příklad použití Navigátora

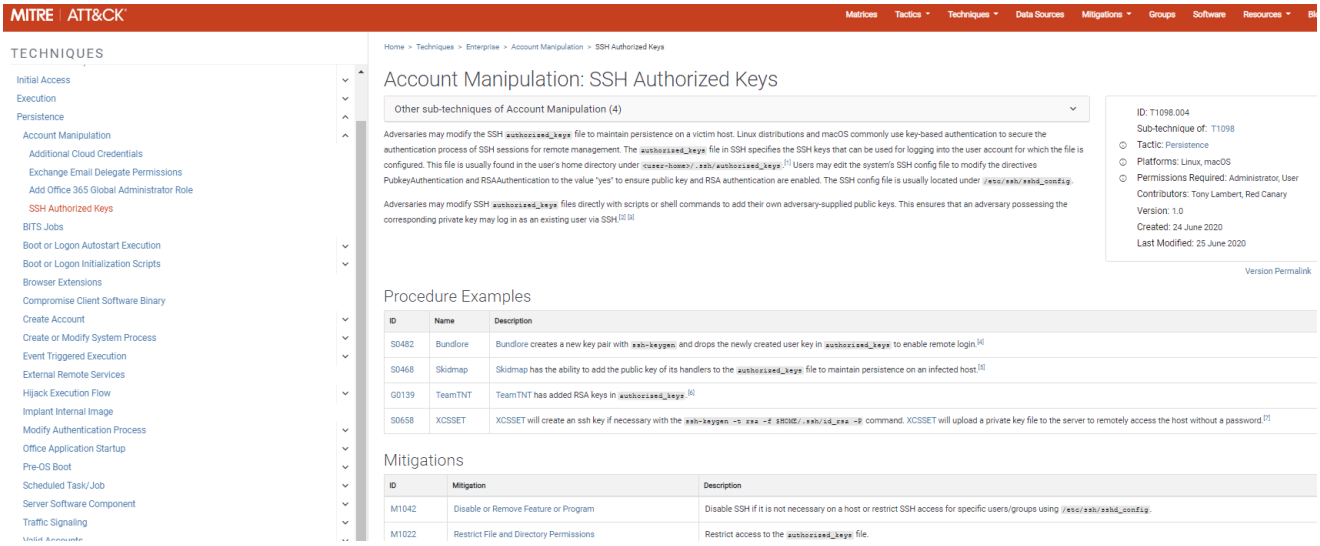
Jako analytik SOC, si všimnete řetězce kódování base64. Zkoumáním zjistíte, že to byl skript PowerShell, který byl spuštěn na jednom z koncových bodů. Máte podezření, že skript byl použit hackerem k zajištění perzistence ve vašem prostředí. Persistence (tímto termínem je označována skupina technik, které hackeři používají k udržení přístupu k systémům po restartování, změně přihlašovacích údajů a dalších přerušeních, která by jim mohly znemožnit přístup).

Víte, že musíte potvrdit své podezření, a tak začnete hledat známky manipulace s účtem. Nejprve se zaměříte na manipulaci s autorizovaným klíčem SSH, protože podle rámce MITER ATT&CK mohou protivníci pomocí skriptů měnit autorizované klíče SSH.

V Navigátoru kliknete na **Persistence**, rozklikněte úroveň II a klikněte na SSH Authorized Keys (obr. 2.3.1). Získáte popis subtechniky, příklady procedur a seznam protiopatření – viz obr. 2.3.2.



Obr. 2.3.1: *Cesta: Persistence > Account Manipulation > SSH Authorized Keys*



Obr. 2.3.2: Popis subtechniky, příklady procedur a seznam protiopatření manipulaci s autorizovaným klíčem SSH

Autorizované klíče SSH jsou veřejné klíče používané k poskytování vzdáleného přihlášení uživatelům prostřednictvím SSH, především v systémech Linux a macOS. Aby se uživatel mohl přihlásit k počítači nakonfigurovanému pro použití klíčů SSH, musel by předložit soukromou polovinu svého páru veřejného/soukromého klíče. Pokud se obě části shodují, je uživateli udělen přístup do systému. Tyto klíče jsou fakticky přihlašovací údaje, které lze použít k přihlášení do systému.

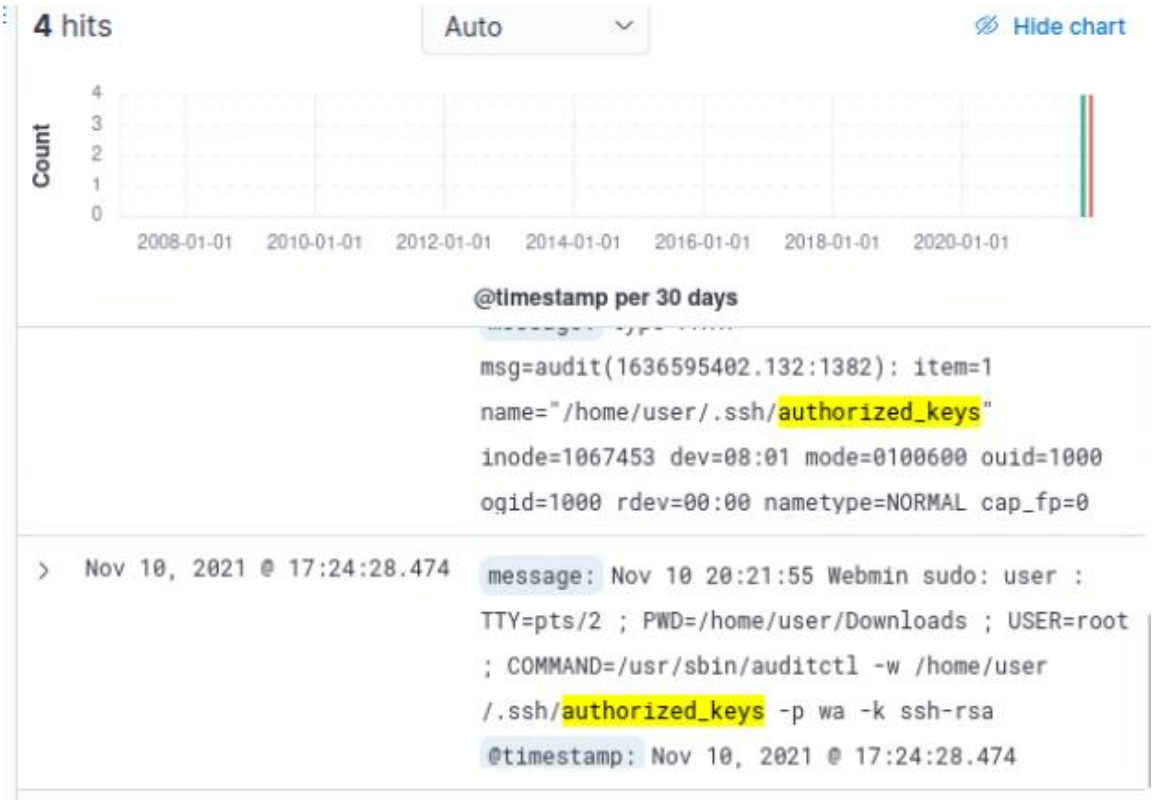
Tyto klíče jsou obvykle uloženy v domovském adresáři uživatele v následujícím umístění: **.ssh/authorized_keys**. Toto umístění však může změnit správce systému aktualizací konfiguračních souborů SSH. Konfigurační soubory SSH jsou umístěny v **/etc/ssh/sshd_config**. V zabezpečených prostředích jsou klíče obvykle uloženy v umístění vlastněném uživatelem root systému, aby se zabránilo nechtěné manipulaci s klíči. Nechtěná manipulace s klíčem SSH je přesně to chování protivníka, které budeme detekovat. Další informace o autorizovaných klíčích SSH a SSH můžete najít od tvůrců protokolu.

Jedním ze způsobů, jak zjistit manipulaci s autorizovaným klíčem SSH, je povolit monitorování integrity souborů v adresáři, kde jsou tyto klíče uloženy. Výchozí umístění je **home/<jméno uživatele>/.ssh/authorized_keys**, kde <jméno_uživatele> je nahrazeno skutečným uživatelem v systému. Správce systému může toto výchozí umístění samozřejmě změnit úpravou konfiguračních souborů SSH.

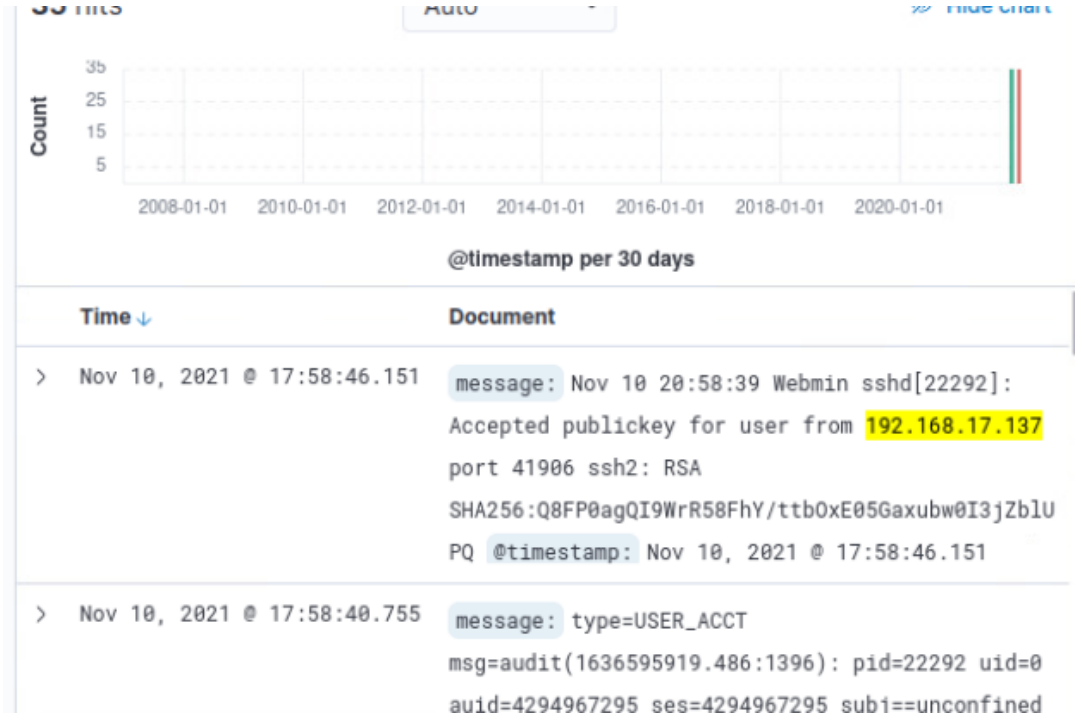
Existuje mnoho způsobů, jak nastavit monitorování integrity souborů, od centrálně spravovaných agentů EDR až po jednoduché protokolování a přeposílání. Jedním ze způsobů, jak nastavit základní monitorování integrity souborů v systému Linux, je instalace a konfigurace auditctl. Na **/etc/audit/auditd.conf** je třeba nastavit konfigurační pravidla, příkazem **auditctl – l** si je pak prolistovat.

Při větším počtu koncových zařízení je preferován SIEM, pro ukázku je příklad řešen použitím Elastic SIEMu přístupného přes webový front-end Kibana. Pomocí monitorování integrity souboru byly zjištěny změny provedené

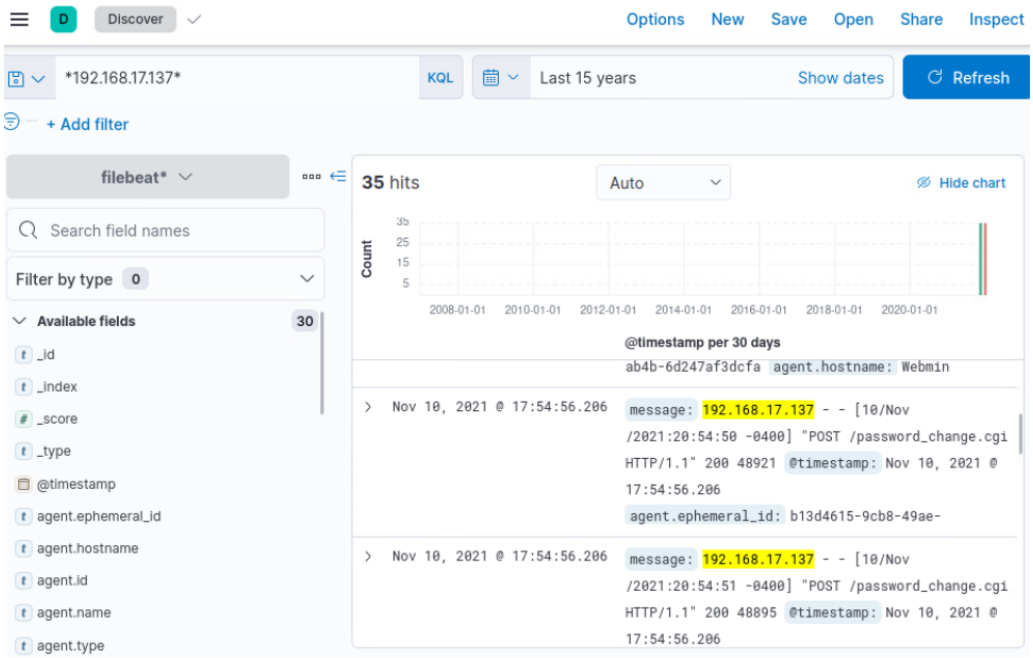
v souboru author_keys pro každého uživatele v systému – obr. 2.3.3. Poté byla nalezena IP adresa útočníka (obr. 2.3.4) a změna jeho adresy.



Obr. 2.3.3: Zjištění změny provedené v souboru author_keys pro každého uživatele v systému



Obr. 2.3.4 Nalezení IP adresy útočníka



Obr.2.3.5: Nalezení změny adresy útočníka

2.3.2 Zadání úloh práce s navigátorem včetně řešení pro učitele

Otevřete ATT&T Navigator na http://bit.ly/attacknav.

a) Zpracujte seznam technik, které používá alespoň jedna skupina ze dvou skupin hrozeb APT39 a APT32 v kategorii Discovery.

Ve skupinách hrozeb APT39 a APT32 se v kategorii Discovery používají techniky:

- File and Directory Discovery (T1083)
- Network Service Scanning (T1046)
- Network Share Discovery (T1135)
- Query Registry (T1012)
- Remote System Discovery (T1018)
- System Information Discovery (T1082)
- System Network Configuration Discovery (T1016)
- System Network Connections Discovery (T1049)
- System Owner/User Discovery (T1033)

b) Které techniky skupiny hrozeb APT38 se používají v cloudu?

Použijte filtr a naleznete:

- Drive-by Compromise (T1189)
- Brute Force (T1110)

c) Které metody prvotního přístupu používá skupina hrozeb FIN6 pro ransomware Ryuk?

- Valid Accounts (T1078),

Poznámka pro učitele: Útok by použit i vůči Benešovské nemocnici.

Shrnutí a závěr

Penetrační test je více než skenování zranitelnosti. Výsledkem práce penetračního testera je seznam zranitelností, ale ten sám o sobě neposkytuje představu o dopadu, který by tato zranitelnost mohla mít na prostředí firmy či organizace. Během penetračního testu se provádějí emulace útoků, které demonstrují potenciální obchodní dopad útoku. Penetrační testeři jdou nad rámec vytváření seznamu zranitelností kódu a konfigurace. Pentesteři musí být schopni vysvětlit, jak se škodlivý útočník dostal do prostředí, obešel kontroly, převzal nad systémem kontrolu a převzal data. Musí znát slabiny v kódu, uživatelích, procesech, systémových konfiguracích nebo fyzickém zabezpečení, aby pochopil, jak může útočník způsobit škodu. Musí znát konfigurační možnosti systému, které by zabránily opakování útoku (vytváří proof-of-concept) případně mu předcházely.

Jako pentester se musí žáci naučit mnoho dalších dovedností (např. komunikační dovednosti, dovednosti psaní zpráv z testování, manažerské dovednosti atd..) a ty spojit s technickými dovednostmi. Tim se např. lovec odměn trápit nemusí, jednoduše najde chybu a nahlásí ji. Práce pentestera je bezpečná práce, protože má stálý plat, pentester se může průběžně zapracovávat, ale pokud lovec odměn nenajde chybu za celý měsíc, je bez příjmu. Zase na druhé straně profil lovce odměn je dnes stále více žádaný, protože čím více se dnes generuje softwaru, tím více je v něm děr.

Seznam použitých zdrojů

(Cisco 2020) Cisco Module 13: Attackers and Their Tools. CyberOps Associate 1.0. Cisco 2020.

(Sophos 2021) https://news.sophos.com/en-us/2021/05/18/the-active-adversary-playbook-2021/

(Sengupta 2021) SENGUPTA, Sudip**.** *Broken Access Control snd How to Prevent it*. Sep 20 2021. Dostupné z: https://crashtest-security.com/broken-access-control-prevention/

(Anton 2021-1) ANTON (therceman). *How To Start Bug Bounty Hunting*. Crashtest Security Aug 20, 2021. Dostupné z:

https://networkingsec.com/how-to-start-bug-bounty-hunting-94b1ff3dda27

(Anto 2021-2) ANTON (therceman). *How To Start Bug Bounty Hunting*. Crashtest Security Aug 20, 2021. Dostupné z:

https://www.youtube.com/watch?v=vPG4IX9xIkU

(OWASP 2021) OWASP Top 10:2021. Dostupné z: https://owasp.org/Top10/A11_2021-Next_Steps/

(ISACA 2021) Capture-The-Flag Competitions: all you ever wanted to know! ISACA 2021. Dostupné z: https://www.enisa.europa.eu/news/enisa-news/capture