

ZÁVĚREČNÁ STUDIJNÍ PRÁCE

dokumentace

Síťová bezpečnost – Wazuh a OPNsense

Vojtěch Zedek

wazuh.

Obor: 18-20-M/01 INFORMAČNÍ TECHNOLOGIE
se zaměřením na počítačové sítě a programování

Třída: IT4

Školní rok: 2023/2024

Poděkování

Rád bych poděkoval panu Ing. Petru Grussmannovi za cenné rady ohledně koncepce projektu a konfigurace sítě. Také bych chtěl poděkovat panu Mgr. Radku Mikešovi za poskytnuté studijní materiály.

Prohlašuji, že jsem závěrečnou práci vypracoval samostatně a uvedl veškeré použité informační zdroje.

Souhlasím, aby tato studijní práce byla použita k výukovým účelům na Střední průmyslové a umělecké škole v Opavě, Praskova 399/8.

V Opavě 31. 12. 2023

podpis autora práce

ABSTRAKT

Účelem projektu je simulace síťového prostředí a různých kybernetických útoků. Prostředí je simulováno v Oracle VM VirtualBoxu a konfigurovaného pomocí routovacího softwaru a firewallu OPNsense. Koncová zařízení monitoruje Wazuh, nástroj pro správu informací o událostech a zabezpečení (SIEM). Tato práce popisuje návrh sítě, její konfiguraci pomocí OPNsense, implementaci systému Wazuh do síťového prostředí a jeho konfiguraci. Výsledkem práce je analýza a možná řešení jednotlivých problémů týkajících se kybernetické bezpečnosti pomocí nástroje Wazuh.

KLÍČOVÁ SLOVA

Síťové prostředí, kybernetický útok, konfigurace, Wazuh, kybernetická bezpečnost

ABSTRACT

The purpose of this project is to simulate a network environment and various cybersecurity attacks. The network environment simulated in Oracle VM VirtualBox is configured by routing software and firewall OPNsense. Endpoints are monitored by Wazuh, an event and security information management (SIEM) tool. This paper describes the network design and configuration using OPNsense, the implementation of Wazuh into the network environment, and the analysis and possible solutions of individual cybersecurity issues using Wazuh.

KEYWORDS

Network environment, cybersecurity attack, configuration, Wazuh, cybersecurity

OBSAH

ÚVOD.....	5
1 PROBLEMATIKA KYBERBEZPEČNOSTI.....	6
1.1 KYBERNETICKÁ BEZPEČNOST.....	6
1.1.1 Kyberprostor	6
1.1.2 Kybernetický útok	7
1.1.3 Důvody kybernetických útoků	8
1.2 NEJNOVĚJŠÍ TRENDY O OBLASTI KYBERNETICKÉ BEZPEČNOSTI	9
1.2.1 Umělá inteligence a strojové učení:	9
1.2.2 Větší rozšíření cloudových bezpečnostních řešení:	9
1.3 MOŽNÁ ŘEŠENÍ.....	9
1.3.1 XMR, SIEM systémy a Wazuh	9
1.3.2 Next Generation Firewall	10
2 VYUŽITÉ TECHNOLOGIE	11
2.1 ORACLE VM VIRTUALBOX.....	11
2.2 OPNSENSE	11
2.3 WAZUH	11
2.4 DOCKER	11
2.5 KALI LINUX.....	11
3 ZPŮSOBY ŘEŠENÍ A POUŽITÉ POSTUPY.....	12
3.1 NÁVRH SÍTĚ A KONFIGURACE VE VIRTUALBOXU	12
3.1.1 Vnitřní Sít'	12
3.1.2 Síťový most.....	12
3.1.3 Konfigurace.....	12
3.2 OPNSENSE KONFIGURACE.....	14
3.2.1 Web GUI	14
3.2.2 Port forwarding a DHCP	15
3.3 WAZUH	17
3.3.1 Instalace.....	17
3.3.2 Koncepce.....	18
3.4 TESTOVÁNÍ.....	20
3.4.1 SSH brute-force attack	20
3.4.2 SQL injection	21
4 DETEKCE HROZEB	22
4.1.1 SSH	22
4.1.2 SQL	23
ZÁVĚR	24
SEZNAM POUŽITÝCH INFORMAČNÍCH ZDROJŮ	25

ÚVOD

V dnešní době, kdy digitalizace pronikla do každého aspektu našeho života, se kyberbezpečnost stává neodmyslitelnou součástí správy informačních technologií. Každý uživatel, organizace či instituce věnuje značné úsilí tomu, aby zajistil bezpečnost svých sítí a dat před nejrůznějšími hrozbami a útoky. V rámci tohoto úsilí se nabízí moderní nástroje a technologie, které pomáhají správcům sítí lépe porozumět a reagovat na kybernetická rizika.

Tato odborná práce se zaměřuje na integraci dvou nástrojů pro kyberbezpečnost – Wazuh a OPNsense. Wazuh je open-source SIEM systém, který umožňuje sledování a analýzu bezpečnostních událostí v reálném čase. Na druhé straně OPNsense představuje moderní a výkonný firewall, který nabízí pokročilé možnosti správy sítě a bezpečnosti.

Cílem tohoto projektu je prozkoumat a implementovat integraci Wazuhu a OPNsense ve virtuálním síťovém prostředí pomocí Oracle VirtualBoxu. virtuální prostředí poskytuje ideální laboratoř pro testování a simulační experimenty, což umožní studovat chování těchto nástrojů v kontrolovaném a izolovaném prostředí. Díky této integraci budeme schopni sledovat bezpečnostní události v síti v reálném čase a reagovat na potenciální hrozby.

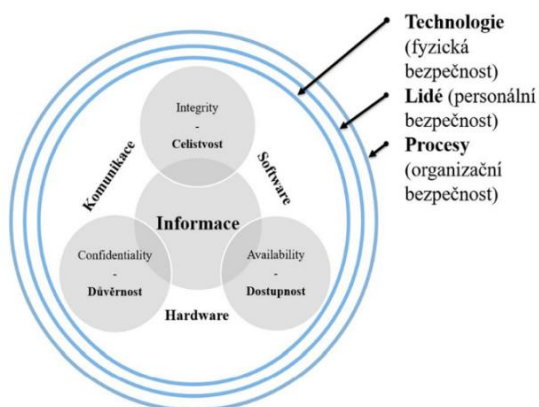
V průběhu této práce budeme zkoumat různé aspekty integrace, včetně konfigurace, monitorování a reakce na bezpečnostní incidenty.

Tato odborná práce poskytne pohled do problematiky kyberbezpečnosti a zároveň přinese praktické poznatky o využívání konkrétních nástrojů pro zlepšení bezpečnosti síťových prostředí.

1 PROBLEMATIKA KYBERBEZPEČNOSTI

1.1 Kybernetická bezpečnost

Kybernetická bezpečnost je soubor procesů, opatření a nástrojů, které jsou zaměřeny na ochranu počítačových systémů, sítí a dat před neoprávněným přístupem, použitím, zveřejněním, změnou nebo zničením. Cílem kybernetické bezpečnosti je zajistit, aby byly informace a systémy, na kterých závisí naše společnost, bezpečné a spolehlivé.



Obrázek: CIA triáda informační bezpečnosti

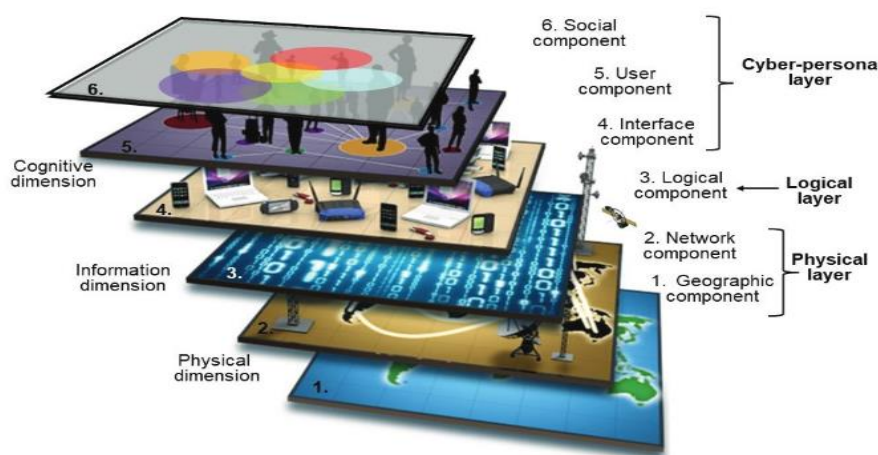
1.1.1 Kyberprostor

Kyberprostor je termín používaný k popisu virtuálního prostředí, které zahrnuje všechny informační systémy, sítě, technologie a data, která jsou propojena přes internet a další komunikační sítě. Kyberprostor se stává stále důležitějším, protože se stává klíčovou součástí moderní společnosti a ekonomiky.

Pět komponent, které tvoří kyberprostor:

1. **Geografická složka:** Tato složka se odkazuje na fyzické umístění digitálních sítí a infrastruktury, včetně datových center, serverů a dalších síťových prvků. Geografická složka je důležitá, protože určuje fyzické hranice kyberprostoru a jeho vztah k fyzickému světu.
2. **Fyzická síťová složka:** Tvoří digitální sítě, včetně routerů, přepínačů, kabelů a dalších síťových zařízení. Fyzická síťová složka je důležitá, protože poskytuje fyzickou infrastrukturu pro digitální komunikaci a výměnu dat.

3. **Logická síťová složka:** Tvoří digitální sítě, včetně protokolů, standardů a softwaru. Logická síťová složka je důležitá, protože poskytuje pravidla a mechanismy pro digitální komunikaci a výměnu dat.
4. **Kybernetická složka:** Tato složka se odkazuje na digitální identitu nebo personu, kterou uživatel vytváří a udržuje v digitálním prostředí. Kybernetická persona je důležitá, protože určuje, jak se lidé prezentují a interagují s ostatními v kyberprostoru.
5. **Osobní identita:** Tato složka se odkazuje na fyzickou identitu nebo personu, kterou uživatel přináší do digitálního prostředí, včetně osobních charakteristik a chování. Osobní identita je důležitá, protože určuje, jak se lidé interagují s ostatními v kyberprostoru na základě svých zkušeností a osobnosti.

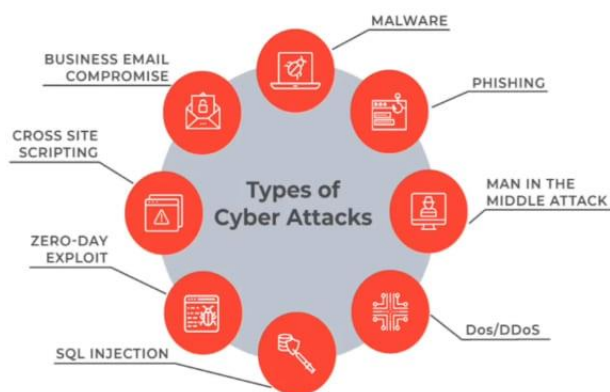


Obrázek: Dělení Kyberprostoru

1.1.2 Kybernetický útok

Kybernetický útok je jednou z hlavních součástí kybernetického zločinu. Kybernetický útok lze definovat jako jakékoliv neoprávněné činy, které zahrnují přístup, použití, zneužití nebo zničení informačních systémů, sítí nebo digitálních dat. Cílem útočníka je často získání kontroly nad systémem, získání citlivých informací nebo způsobení škody či narušení provozu infrastruktury.

Kybernetické útoky mohou mít různé formy, jako jsou DDoS útoky, malware, ransomware, sociální inženýrství nebo využití zranitelností v softwaru a hardwaru. Útočníci, kteří provádějí tyto útoky, mohou mít různé motivy, jako jsou finanční zisky, politické nebo ideologické cíle, špionáž nebo získání konkurenční výhody.



Obrázek: Typy kybernetických útoků

1.1.3 Důvody kybernetických útoků

Kritická infrastruktura nemusí mít dostatečné bezpečnostní opatření, což ji činí snadným cílem pro kybernetické zločince. To může zahrnovat zastaralý hardware nebo software, slabá hesla nebo nedostatek šifrování.

Chyba lidského faktoru: Kybernetické útoky se také mohou stát kvůli lidské chybě, jako například zaměstnanci omylem otvírají phishingové e-maily nebo nedodržují stanovené bezpečnostní protokoly.

Vnitřní hrozby: Kyberútoky mohou také být provedeny ze strany interních lidí s přístupem k citlivým informacím nebo ovládání systému. Ti mohou mít zlomyslné úmysly nebo být donuceni nebo podplaceni vnějšími aktéry.

Malware: Malware může být zaveden do systémů kritické infrastruktury různými způsoby, včetně infikovaných příloh e-mailů, USB disků nebo zákeřných odkazů. Jakmile se malware dostane do systému, může krást citlivá data nebo narušovat provoz systému.

Sociální inženýrství: Útoky sociálního inženýrství zahrnují oklamání jednotlivců k odhalení citlivých informací nebo kliknutí na zákeřné odkazy. Útočníci mohou používat různé techniky, jako napodobování důvěryhodných osob nebo použití falešných webových stránek, aby oklamali oběti a získali přístup k systémům kritické infrastruktury.

1.2 Nejnovější trendy o oblasti kybernetické bezpečnosti

1.2.1 Umělá inteligence a strojové učení:

Obrovské množství dat generovaných moderními systémy v kombinaci s rychle se vyvíjejícím prostředím hrozeb ztěžuje tradičním bezpečnostním opatřením držet krok. Algoritmy umělé inteligence a ML dokáží zpracovávat a analyzovat velké objemy dat a identifikovat vzory, anomálie a potenciální hrozby v reálném čase. To umožňuje proaktivní přístup k odhalování hrozeb, jejich prevenci a reakci na ně. Kromě toho mohou AI a ML pomoci automatizovat rutinní bezpečnostní úkoly, čímž se uvolní zdroje pro pokročilejší analýzu a zmírňování hrozeb.

1.2.2 Větší rozšíření cloudových bezpečnostních řešení:

Cloudová bezpečnostní řešení nabízejí řadu výhod, včetně škálovatelnosti, nákladové efektivity a schopnosti držet krok s rychlým technologickým pokrokem. S tím, jak stále více organizací migruje svou infrastrukturu do cloudu, roste poptávka po bezpečnostních nástrojích a službách založených na cloudu. Tato řešení často integrují funkce umělé inteligence a ML, poskytují robustní ochranu před kybernetickými útoky a zároveň umožňují organizacím přizpůsobit se neustále se měnícímu prostředí hrozeb.

1.3 Možná řešení

1.3.1 XMR, SIEM systémy a Wazuh

XDR je zkratka pro kategorii produktů Extended Detection and Response, což je přístup k zabezpečení, který rozšiřuje možnosti EDR (Endpoint Detection and Response) o integrovanou detekci a reakci nejen na koncových bodech, ale také na uživatelských profilech a lokálních datových centrech.

XDR nabízí důležitý přehled nad celým řetězcem útoku, ať už vznikl kdekoli, a přesně odhaluje, jak útok probíhal a která aktiva a uživatelé byli zasaženi, a také nabízí možnosti automatizované a řízené reakce, které řešení pro správu bezpečnostních informací a událostí (SIEM) nemohou poskytnout.

SIEM je zkratka pro systém pro správu bezpečnostních informací a událostí (Security Information and Event Management). Jedná se o analytický software, který sbírá a události z bezpečnostních a síťových zařízení, případně z aplikací. Dokáže identifikovat podezřelé události, jako jsou stažení souborů nebo příliš vysoký přenos informací.

SIEM na rozdíl od jiných bezpečnostních softwarů hrozbu neodstraňuje, ale zaznamenává data, která pomohou správcům sítě v podniknutí dalších obranných kroků. SIEM generuje bezpečnostní reporty, které zjednoduší například bezpečnostní audity.

Jelikož jsou SIEM systémy primárně analytický nástroj tak je vhodná jejich kombinace s XDR systémy nebo firewallem pro komplexnější zabezpečení sítě. Tuto kombinaci nabízí právě Wazuh.

1.3.2 Next Generation Firewall

Zatímco běžný firewall zpravidla rozeznává pouze IP adresy, NGFW může nejen kontrolovat síťový provoz, ale má přehled a kontrolu i nad konkrétními aplikacemi, jejich obsahem, a pozná i jejich uživatele.

2 VYUŽITÉ TECHNOLOGIE

2.1 Oracle VM VirtualBox

VirtualBox je profesionální vizualizační nástroj pro kompletní simulaci různých hardwarových prostředí na jednom PC. Z hostitelského zařízení je možno připojit pevné disky, CD/DVD mechaniky, USB porty apod. Umožňuje také různé typy síťové konfigurace a manipulaci se síťovými kartami, je tak vhodný pro simulaci síťového prostředí.

2.2 OPNsense

OPNsense je open-source firewall. Poskytuje také web GUI, které slouží jako routovací prostředí. Umožňuje manipulovat s provozem a průchodností sítě. S jeho použitím lze nastavit různé parametry, protokoly a funkce - např. NAT, DHCP nebo port forwarding.

2.3 Wazuh

Wazuh je open-source SIEM (tj. Security Information and Event Management) platforma. Slouží ke sběru dat a analýze událostí vztahujících se k chodu monitorovaného prostředí z různých zdrojů, včetně síťových zařízení, serverů, koncových zařízení a aplikací. Nabízí obranu a řadu řešení proti různým bezpečnostním hrozbám, které by mohly ohrozit monitorované prostředí.

2.4 Docker

Docker je open-source software, jehož cílem je poskytnout jednotné rozhraní pro izolaci aplikací do jednotlivých kontejnerů. Kontejnery jsou izolované balíčky, které obsahují aplikaci, její závislosti a konfiguraci. Neobsahují však virtualizovaný operační systém. K výhodám Dockeru patří menší velikost, větší flexibilita a tím pádem nižší nároky na provoz. Wazuh je v tomto projektu nainstalován na Ubuntu serveru pomocí Dockeru.

2.5 Kali Linux

Kali Linux je specializovaná distribuce Linuxu navržená pro účely kybernetické bezpečnosti. Tato distribuce je založena na Debianu a obsahuje širokou škálu nástrojů určených pro testování bezpečnosti a penetrace sítě. Obsahuje nástroje pro testování kybernetické bezpečnosti jak Hydra nebo Metasploit. Kali Linux lze tak použít jako útočící PC.

3 ZPŮSOBY ŘEŠENÍ A POUŽITÉ POSTUPY

3.1 Návrh sítě a konfigurace ve VirtualBoxu

Základní kámen této práce tvoří simulované síťové prostředí v Oracle VM VirtualBoxu. Budeme používat dva typy síťových karet, pojďme si o nich něco říct:

3.1.1 Vnitřní Sít'

Tento konfigurační režim nám umožňuje vytvořit lokální síť ze dvou nebo více virtuálních strojů, kde spolu mohou dva nebo více VM, které jsme nakonfigurovali, bez problémů komunikovat. V tomto konfiguračním režimu nebudou mít virtuální stroje přístup k místní domácí nebo profesionální síti ani nebudou mít přístup k internetu. V tomto provozním režimu se vytvoří virtuální síť, kde spolu mohou komunikovat pouze vybrané virtuální počítače.

3.1.2 Síťový most

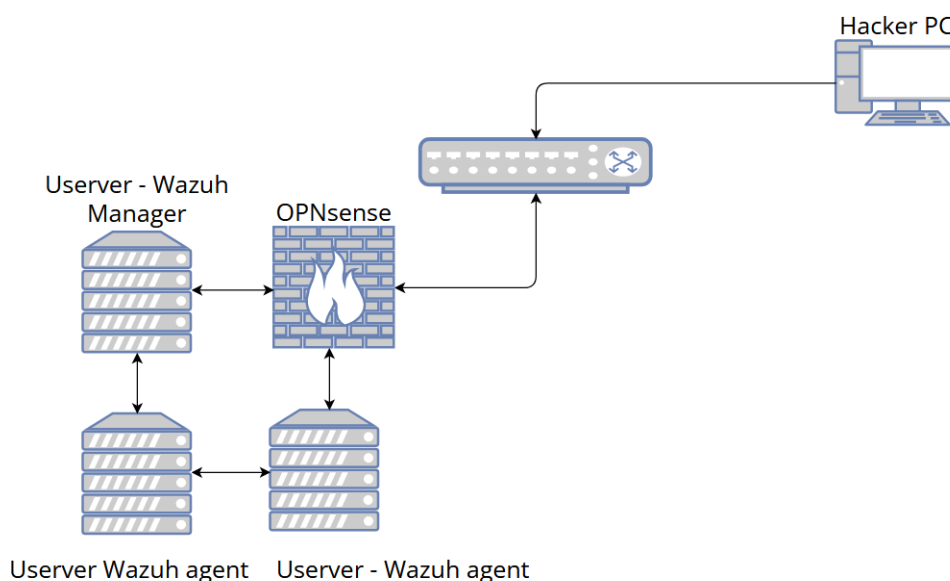
V tomto konfiguračním režimu se virtuální stroj stane dalším počítačem v domácí nebo profesionální místní síti. Pomocí fyzického síťového adaptéru skutečného počítače připojíme VM k místní síti s odpovídající MAC adresou, nebo získá IP adresu z DHCP serveru, který máme v lokální síti, a ne z DHCP VirtualBoxu. server.

V tomto provozním režimu bude virtuální stroj komunikovat se zbytkem počítačů v lokální síti a s internetem, navíc zbytek počítačů bude také moci bez problémů komunikovat s virtuálním strojem. Nyní bude VM dalším počítačem v místní síti s odpovídající MAC, privátní IP adresou atd.

Tento konfigurační režim je ideální, pokud chceme, aby virtuální stroj přešel na jiný počítač v lokální síti a chceme, aby s virtuálním strojem přímo komunikovaly i další počítače, aniž bychom museli dělat přesměrování portů nebo cokoli jiného.

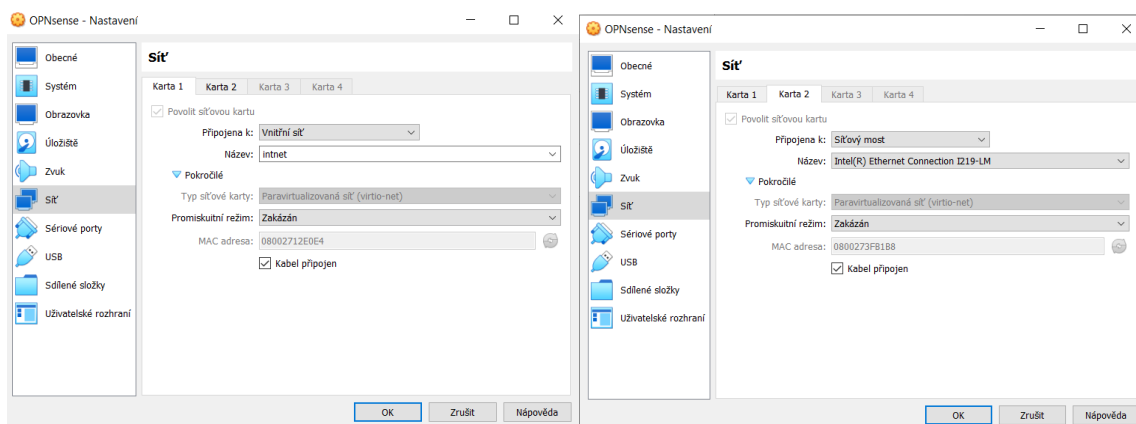
3.1.3 Konfigurace

Po konzultaci s panem Grussmanem jsem se rozhodl pro tuto síť:



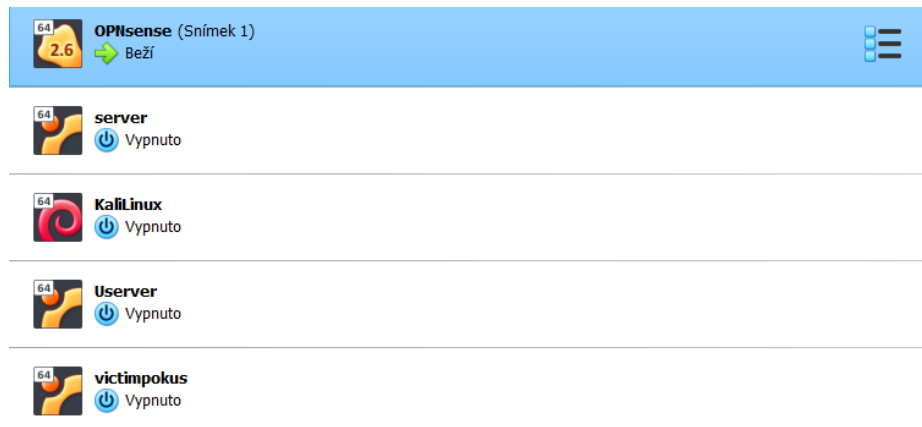
Obrázek: Návrh síťové konfigurace

OPNsense nám poslouží jako základní stavební kámen, protože jej dále lze využít pro konfiguraci sítě. Na OPNsense virtuálním stroji proto musíme nastavit 2 síťové karty, první kartu jako vnitřní síť s názvem intnet a druhou jako síťový most. Na první kartě bude LAN (local area network) vztahující se k vnitřní síti a na druhé kartě bude WAN (wide area network). Přes WAN se pomocí port forwardingu budeme dostávat na servery ve vnitřní síti nebo na webové rozhraní Wazuhu, který poběží na jednom z Ubuntu serverů. WAN také bude využívat útočící počítač, aby pronikl do naší vnitřní sítě zvenčí.



Obrázek: VirtualBox OPNsense síťová konfigurace

Na všechny Ubuntu servery si dáme vnitřní síť s názvem intnet. Název musí být pro všechna zařízení ve vnitřní síti stejný, jinak se sebou nebudou komunikovat. Na PC útočníka si nastavíme síťový most, aby mohl útočit přes WAN a port forwarding na jeden ze serverů zvenčí.



Obrázek: Síťová laboratoř ve Virtualboxu

3.2 OPNsense konfigurace

3.2.1 Web GUI

Po spuštění OPNsense ve VirtualBoxu a přihlášení do něj dostane LAN i WAN IP adresu.

```
Last login: Mon Jan 15 19:21:46 on ttyv0
-----
|      Hello, this is OPNsense 23.7      |
|                                         |
| Website:   https://opnsense.org/       |
| Handbook:  https://docs.opnsense.org/  |
| Forums:    https://forum.opnsense.org/ |
| Code:      https://github.com/opnsense |
| Twitter:   https://twitter.com/opnsense |
|                                         |
-----
*** opnsense-1.localdomain: OPNsense 23.7.10 ***

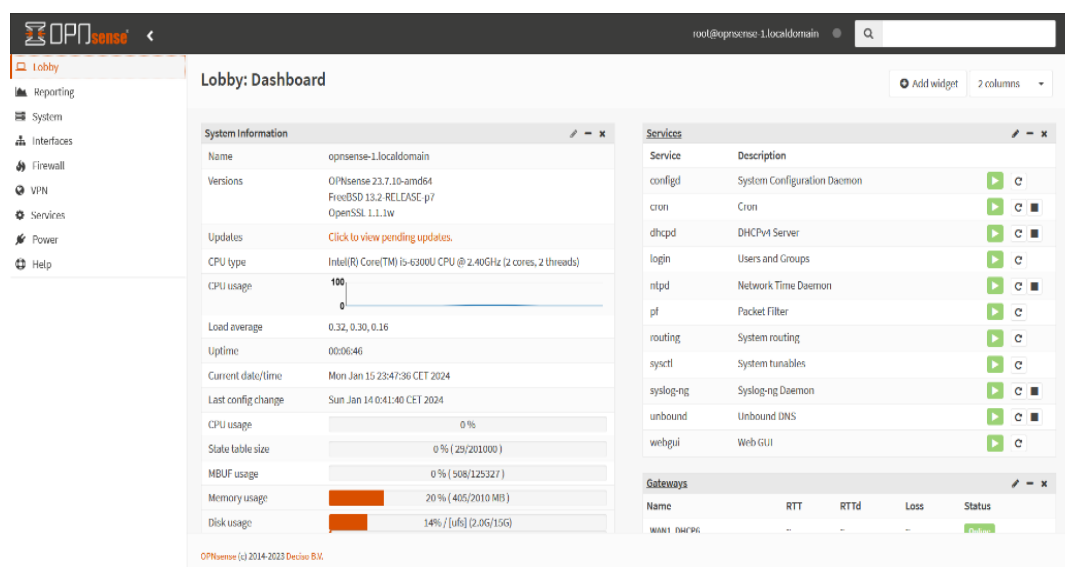
LAN11 (vtnet0)  -> v4: 192.168.11.1/24
WAN1 (vtnet1)  -> v4/DHCP4: 192.168.0.132/24

0) Logout                               7) Ping host
1) Assign interfaces                     8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 
```

Obrázek: LAN A WAN IP adresy

Na Web GUI se dostanete pomocí `http://[LAN IP]`. Ve web GUI se v `System > Settings > Administration` dá přenastavit přihlašovací adresa z LAN adresy na WAN adresu. Já se přihlašuji pomocí WAN adresy a portu 444. Po zadání přihlašovacích údajů se dostanete na titulní stránku



Obrázek: OPNsense lobby

3.2.2 Port forwarding a DHCP

Na řadu přichází ta nejdůležitější část práce s OPNsense a tou je port forwarding. Port forwarding je metoda směřování portů z jednoho síťového uzlu na druhý. Typickým použitím je umožnění vnějšímu uživateli připojit se na port na soukromé adrese v lokální síti prostřednictvím směrovače, který podporuje technologii překladu síťových adres.

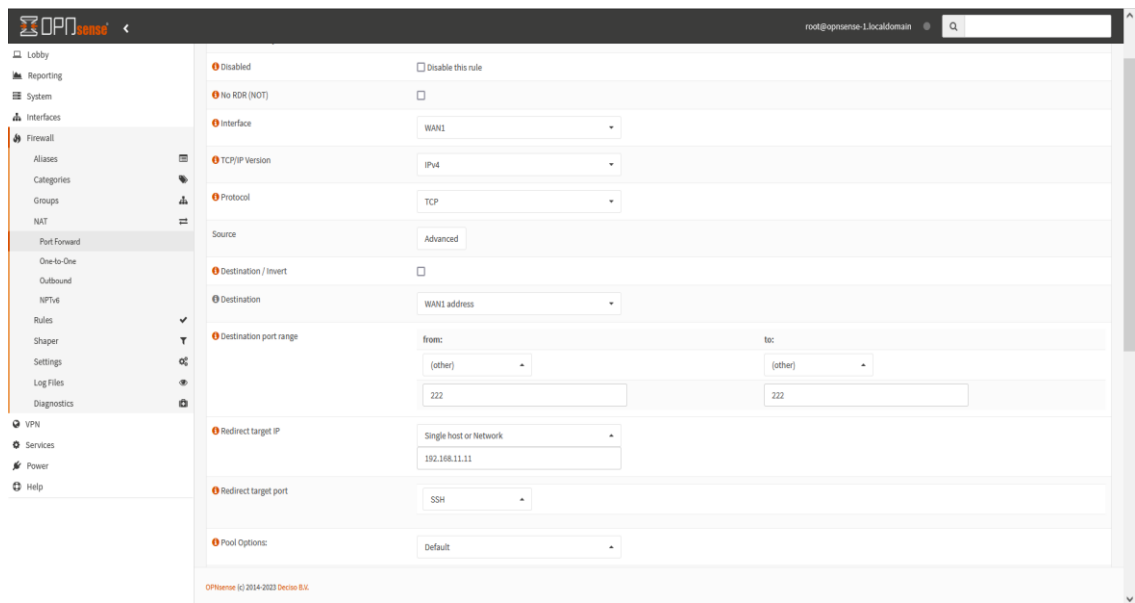
V OPNsense najde port forwarding ve `Firewall > NAT > Port forward`

Port forward použijeme k několika věcem:

- přístup z Windows terminálu na servery ve vnitřní síti pomocí SSH.
- přístup na webové rozhraní Wazuhu skrze WAN adresu a port 443, které běží na Ubuntu serveru ve vnitřní síti




































- Umožníme útočícímu PC přístup do naší sítě pro účely testování

Zajistíme přístup z našeho počítače do Ubuntu serveru ve vnitřní síti pomocí SSH. Destinace bude WAN adresa a port 222, odtud pak bude pokus o přihlášení skrze SSH přesměřován na IP adresu Ubuntu serveru a SSH port 22.



Obrázek: Vytvoření port forwarding SSH pravidla

Další port forwarding pravidla, co jsem zmiňoval mají podobnou logiku, proto příkládám celou konfiguraci

Source					Destination		NAT							
<input type="checkbox"/>	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description					<input type="checkbox"/>
<input type="checkbox"/>	 WAN1	TCP	*	*	WAN1 address	444	192.168.11.1	445 (MS DS)						
<input type="checkbox"/>	 WAN1	TCP	*	*	WAN1 address	2222	192.168.11.10	22 (SSH)						
<input type="checkbox"/>	 WAN1	TCP	*	*	WAN1 address	222	192.168.11.11	22 (SSH)						
<input type="checkbox"/>	 WAN1	TCP	*	*	WAN1 address	443 (HTTPS)	192.168.11.10	443 (HTTPS)						
<input type="checkbox"/>	 WAN1	TCP	*	*	WAN1 address	58000	192.168.11.12	22 (SSH)						
<input type="checkbox"/>	 WAN1		*	*	WAN1 address	*	192.168.11.12	*						
	Enabled rule				No redirect				Linked rule					
	Disabled rule				Disabled no redirect				Disabled linked rule					
 Alias (click to view/edit)														

Obrázek: Všechna potřebná port forward pravidla

V Services <DHCPv4<[LAN11] zaklikneme enable DHCP a zvolíme rozsah IP adresace podle našich potřeb - např. 192.168.11.10 – 192.168.11.20, tím přiřadíme adresy z toho rozsahu zařízením ve vnitřní síti. Můžeme taky přiřadit DHCP adresy staticky tím, že specifikujeme hostname, IP adresu a MAC adresu zařízení. Tím docílíme toho, že dané zařízení bude vždy dostávat tu stejnou IP adresu.

3.3 Wazuh

3.3.1 Instalace

Rozhodl jsem se Wazuh instalovat pomocí Dockeru, jedná se o single-node deployment.

```
#git clone https://github.com/wazuh/wazuh-docker.git -b v4.7.2
```

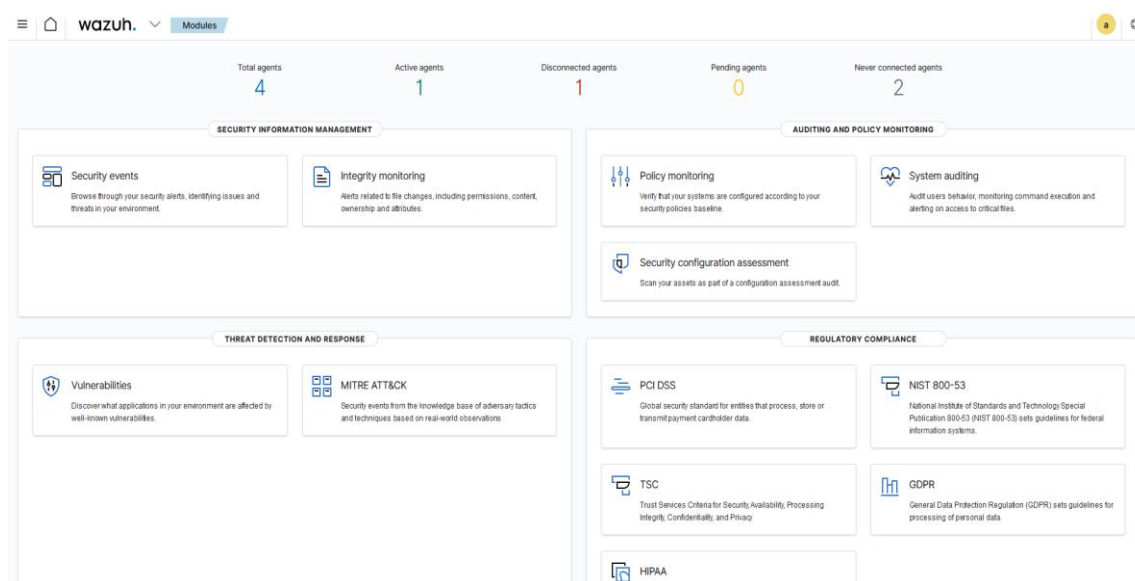
```
#docker-compose -f generate-indexer-certs.yml run --rm generator
```

```
#docker-compose up
```

```
root@rocprojektserver:~/wazuh-docker# cd single-node/
root@rocprojektserver:~/wazuh-docker/single-node# docker compose up
[+] Running 3/0
  0 Container single-node-wazuh.indexer-1    Running
  0 Container single-node-wazuh.manager-1    Running
  0 Container single-node-wazuh.dashboard-1  Running
```

Obrázek: Wazuh se úspěšně spustil

Jelikož jsme nastavili port forwarding tak na adrese <https://192.168.0.132:443> máme Wazuh dashboard. Přihlašovací údaje jsou admin a SecretPassword dokud je nenastavíme jinak.



Obrázek: Wazuh Dashboard

3.3.2 Koncepce

Zařízení, na kterém běží centrální komponenty Wazuhu se nazývá Wazuh server nebo Wazuh manager. Mezi centrální komponenty patří server, dashboard a indexer. Monitorované koncové zařízení se nazývá Wazuh agent. Agent a server mezi sebou komunikují.

V Menu > Management > Configuration > Edit configuration se nachází nejdůležitější soubor Wazuhu, konfigurace Wazuh managera. Tento soubor je zodpovědný za sběr dat, komunikaci s agenty nebo za reakce na různé bezpečnostní hrozby. Můžeme si jej upravovat podle potřeby



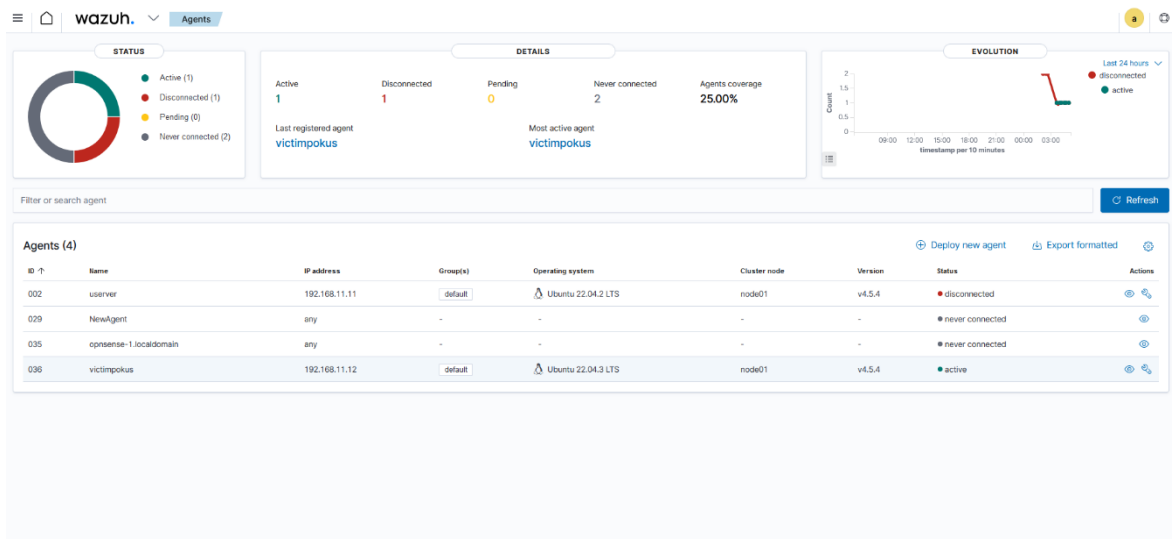
Obrázek: konfigurace Wazuh manažera

V Menu> Management> Rules můžeme spravovat a přidávat pravidla

Filter or search							Custom rules
ID ↑	Description	Groups	Regulatory compliance	Level	File	Path	
1	Generic template for all syslog rules.	syslog		0	0010-rules_config.xml	ruleset/rules	
2	Generic template for all firewall rules.	firewall		0	0010-rules_config.xml	ruleset/rules	
3	Generic template for all ids rules.	ids		0	0010-rules_config.xml	ruleset/rules	
4	Generic template for all web rules.	web-log		0	0010-rules_config.xml	ruleset/rules	
5	Generic template for all web proxy rules.	squid		0	0010-rules_config.xml	ruleset/rules	
6	Generic template for all windows rules.	windows		0	0010-rules_config.xml	ruleset/rules	
7	Generic template for all wazuh rules.	ossec		0	0010-rules_config.xml	ruleset/rules	
200	Grouping of wazuh rules.	wazuh		0	0016-wazuh_rules.xml	ruleset/rules	
201	Agent event queue rule	agent_flooding, wazuh		0	0016-wazuh_rules.xml	ruleset/rules	
202	Agent event queue is level full.	agent_flooding, wazuh	PCI_DSS GDPR	7	0016-wazuh_rules.xml	ruleset/rules	
203	Agent event queue is full. Events may be lost.	agent_flooding, wazuh	PCI_DSS GDPR	9	0016-wazuh_rules.xml	ruleset/rules	
204	Agent event queue is flooded. Check the agent configuration.	agent_flooding, wazuh	PCI_DSS GDPR	12	0016-wazuh_rules.xml	ruleset/rules	
205	Agent event queue is back to normal load.	agent_flooding, wazuh		3	0016-wazuh_rules.xml	ruleset/rules	
210	Remote upgrade alert	upgrade, wazuh		0	0016-wazuh_rules.xml	ruleset/rules	
211	Remote installation alert	upgrade, wazuh		0	0016-wazuh_rules.xml	ruleset/rules	
212	Remote upgrade started.	upgrade, wazuh		3	0016-wazuh_rules.xml	ruleset/rules	
213	Remote upgrade could not be launched. Error: error.	upgrade, upgrade_failure, wazuh		7	0016-wazuh_rules.xml	ruleset/rules	

Obrázek: manipulace s pravidly

V Menu> Agents můžeme spravovat monitorovaná zařízení



Obrázek: Administrace koncových zařízení

3.4 Testování

3.4.1 SSH brute-force attack

Pomocí PC se systémem Kali Linux a nástrojem Hydra provedeme SSH brute force attack na Ubuntu server ve vnitřní síti. Útočník se pomocí textového souboru s jmény a hesly pokusí nabourat přes SSH na náš Ubuntu server. Wazuh tuto událost zachytí a analyzuje.

Na útočícím PC si vytvoříme textový soubor s 10 jmény a druhý textový soubor s deseti hesly. Provedeme tento příkaz

```
sudo hydra-L users.txt -P passwd.txt 192.168.0.132 ssh -t 4
```

Příkaz: Útočník hádá hesla pomocí náhodných hesel v txt.souborech

```
(attacker@ kali)-[~]
$ hydrhydra -L users.txt -P passwd.txt 192.168.0.132 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-16 06:15:50
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (1:10/p:10), ~25 tries per task
[DATA] attacking ssh://192.168.0.132:22/
[STATUS] 80.00 tries/min, 80 tries in 00:01h, 20 to do in 00:01h, 4 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-16 06:17:05
```

Obrázek: SSH brute force attack

Wazuh má něco, čemu se říká active-response, je to obrana a odpověď na kybernetický útok. V případě brute force SSH může útočníka firewall zablokovat. Stačí dát kousek kódu do Menu> Management> Configuration > Edit configuration:

```
<ossec_config>
  <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>5763</rules_id>
    <timeout>180</timeout>
  </active-response>
</ossec_config>
```

kód : Útočníka zablokuje firewall

Musíte kód uložit a poté stačí manažera restartovat kliknutím na tlačítko.

3.4.2 SQL injection

SQL injection je typ útoku, který napadá databázovou vrstvu vsunutím (odtud slovo *injection*) kódu přes neošetřený vstup. S pomocí takto vsunutého kódu může útočník získat citlivé osobní informace, jako například číslo kreditní karty nebo přihlašovací údaje. Také může databázi poškodit smazáním dat, dokonce může databázi upravit ve svůj prospěch. Vyzkoušíme si, jestli Wazuh detekuje takový typ útoku.

Na našem serveru si nainstalujeme apache server

```
sudo apt update
sudo apt install apache2
```

Příkaz: Instalace apache serveru

Pote dáme na našem ubuntu server do /var/ossec/etc/ossec.conf tenhle kód:

```
<ossec_config>
  <localfile>
    <log_format>apache</log_format>
    <location>/var/log/apache2/access.log</location>
  </localfile>
</ossec_config>
```

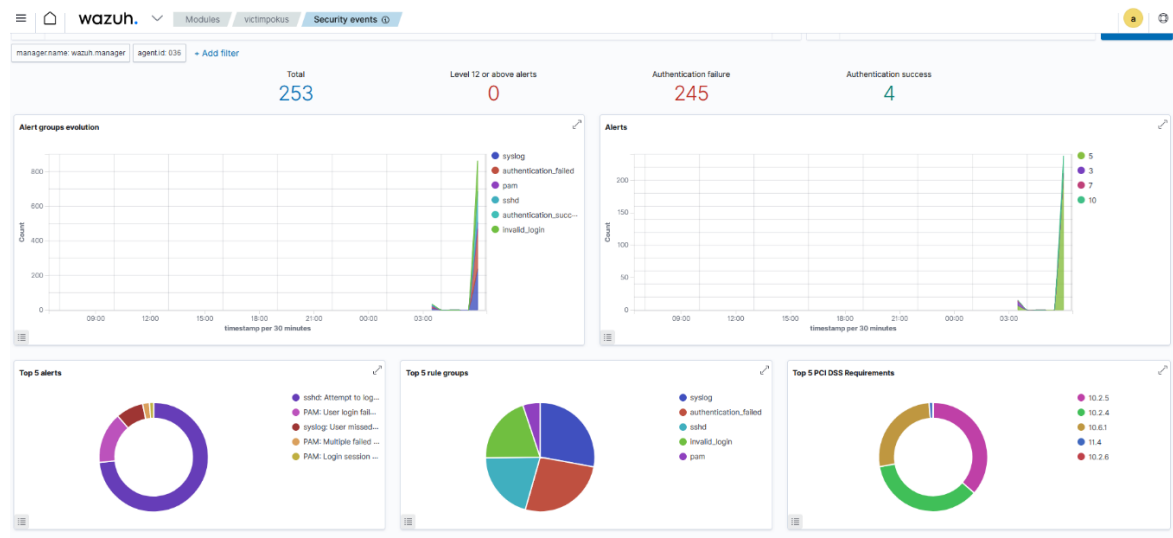
Kód: Wazuh bude monitorovat logy apache serveru

Opět provedeme útok z našeho počítače s Kali Linuxem:

```
curl -XGET "http://192.168.11.12/users/?id=SELECT*+FROM+users";
```

Kód: SQL injection attack

4 DETEKCE HROZEB



Obrázek: Monitorování agenta

4.1.1 SSH

Na prvním obrázku můžeme vidět, že Wazuh zaznamená pokus o SSH brute-force attack. Na druhém obrázku vidíme, že active-response funguje, Wazuh pomocí firewallu zablokoval útočníka

The screenshot displays the Wazuh Security events dashboard with a table of alerts. The table has columns for @timestamp, _id, agent.id, agent.ip, agent.name, data.command, data.distuser, data.origin.module, data.origin.name, data.parameters.alert.agent.id, data.parameters.alert.agent.ip, data.parameters.alert.agent.name, data.parameters.alert.data.distuser, data.parameters.alert.data.scrip, data.parameters.alert.data.scripport, data.parameters.alert.decoder.name, data.parameters.alert.decoder.parent, data.parameters.alert.full_log, and data.parameters.alert.id. The table shows a single alert entry with details about a failed password attempt for victim2 from 192.168.0.130 on port 53904.

@timestamp	_id	agent.id	agent.ip	agent.name	data.command	data.distuser	data.origin.module	data.origin.name	data.parameters.alert.agent.id	data.parameters.alert.agent.ip	data.parameters.alert.agent.name	data.parameters.alert.data.distuser	data.parameters.alert.data.scrip	data.parameters.alert.data.scripport	data.parameters.alert.decoder.name	data.parameters.alert.decoder.parent	data.parameters.alert.full_log	data.parameters.alert.id
2024-01-16T19:30:53.317Z	6f78E40BvUlpALayYkZA	036	192.168.11.12	victimpokus	add	victim2	wazuh-execd	node01	036	192.168.11.12	victimpokus	victim2	192.168.0.130	53904	sshd	sshd	Jan 16 19:30:51 ubuntu:victim sshd[7819]: Failed password for victim2 from 192.168.0.130 port 53904 ssh2	170543453.383827

Obrázek: Detekce SSH brute-force útoku.

The screenshot shows the Wazuh Security events interface. The top bar indicates the date and time as Jan 16, 2024 @ 20:17:13.639. The event is categorized as 'Credential Access' with a description 'ssh: brute force trying to get access to the system. Authentication failed.' and a severity of 10. The event ID is 5763. The main table displays the following data:

Table	JSON	Rule
@timestamp	2024-01-16T19:17:13.638Z	
_id	svf6E40BvulpALay2kar	
agent.id	036	
agent.ip	192.168.11.12	
agent.name	victimpokus	
data.dstuser	victim2	
data.scrip	192.168.0.130	
data.srport	37376	
decoder.name	sshd	
decoder.parent	sshd	
full_log	Jan 16 19:17:13 ubuntu:victim sshd[5712]: Failed password for victim2 from 192.168.0.130 port 37376 ssh2	
id	1705432633.353787	
input.type	log	
location	/var/log/auth.log	
manager.name	wazuh.manager	
predecoder.hostname	ubuntu:victim	
predecoder.program_name	sshd	
predecoder.timestamp	Jan 16 19:17:13	
previous_output	Jan 16 19:17:13 ubuntu:victim sshd[5712]: Failed password for victim2 from 192.168.0.130 port 37376 ssh2	

Obrázek: Zablokování útočníka pomocí firewallu

4.1.2SQL

Zde můžeme vidět, že Wazuh monitoruje náš apache server:

The screenshot shows the Wazuh Security events interface. The top bar indicates the date and time as Jan 16, 2024 @ 19:06:29.470. The event is categorized as 'Initial Access' with a description 'SQL injection attempt.' and a severity of 7. The event ID is 31103. The main table displays the following data:

Table	JSON	Rule
@timestamp	2024-01-16T18:08:29.470Z	
_id	afh1E40BvulpALay.Eal	
agent.id	036	
agent.ip	192.168.11.12	
agent.name	victimpokus	
data.id	404	
data.protocol	GET	
data.scrip	192.168.0.130	
data.url	/users?id=SELECT***FROM+users	
decoder.name	web-accesslog	
full_log	192.168.0.130 - - [16/Jan/2024:18:08:24 +0000] "GET /users?id=SELECT***FROM+users HTTP/1.1" 404 436 "-" "curl/7.88.1"	
id	1705429505.340713	
input.type	log	
location	/var/log/apache2/access.log	
manager.name	wazuh.manager	
rule.description	SQL injection attempt.	
rule.firetimes	1	
rule.gdpr	/V_36.7.d	
rule.groups	web_accesslog, attack, sql_injection	

Obrázek: SQL injection attack

ZÁVĚR

Cílem práce bylo simulovat síťové prostředí a provádět různé kybernetické útoky za účelem analýzy a posouzení kybernetické bezpečnosti. Práce se zaměřila na vytvoření simulovaného prostředí v Oracle VM Virtualboxu, jeho konfiguraci pomocí routovacího softwaru a firewallu OPNsense a monitorování koncových zařízení pomocí systému Wazuh.

Celkový průběh projektu byl úspěšný a přinesl cenné poznatky o konfiguraci sítě a využití systému Wazuh pro sledování kybernetické bezpečnosti. Implementace systému Wazuh do síťového prostředí byla provedena úspěšně. Výsledky testování poskytly důležité informace o potenciálních bezpečnostních hrozbách.

Možnosti systému Wazuh byly však zkoumány pouze omezeně, a stejně tak i testování různých kybernetických útoků mohlo být důkladnější. Existuje potenciál pro další rozvoj projektu a prohloubení pochopení kybernetické bezpečnosti prostřednictvím podrobnější analýzy a experimentů.

Tato práce však představuje solidní základ pro budoucí výzkum a zdůrazňuje důležitost správné konfigurace sítě a monitorování bezpečnostních událostí. Projekt nabízí perspektivu pro další rozšiřování a zdokonalování v oblasti kybernetické bezpečnosti.

Odkaz na github: <https://github.com/vojtech-zedek/finalni-projekt/tree/main>

SEZNAM POUŽITÝCH INFORMAČNÍCH ZDROJŮ

- [1] NAKIVO. VirtualBox Network Settings: Complete Guide. VIRTUALBOX. Chapter 6. Virtual Networking [online]. [cit. 2024-01-16]. Dostupné z: <https://www.nakivo.com/blog/virtualbox-network-setting-guide>
- [2] OPNSENSE. OPNsense's documentation. Online. Dostupné z: <https://docs.opnsense.org/index.html>. [cit. 2024-01-16].
- [3] PIKA, Jevgenij. Kybernetické útoky na kritickou infrastrukturu státu. Online, Bakalářská práce. Praha: AMBIS vysoká škola, a.s., 2023. Dostupné z: https://is.ambis.cz/th/voiwxBakalarska_prace_Jevgenij_Pika.pdf. [cit. 2024-01-16].
- [4] PROCOMPUTING. Co je XDR a jakou roli hraje v moderní kyberbezpečnosti? [online]. [cit. 2024-01-16]. Dostupné z: <https://procomputing.cz/co-je-xdr-a-jakou-roli-hraje-v-moderni-kyberbezpecnosti/>
- [5] WAZUH. Blocking SSH brute-force attack with active response [online]. [cit. 2024-01-16]. Dostupné z: <https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force>.

