

Sem vložte zadání Vaší práce.



**FAKULTA
INFORMAČNÍCH
TECHNologiÍ
ČVUT V PRAZE**

Bakalářská práce

Kubernetes klastr pro lámání hesel

Tomáš Klas

Katedra informační bezpečnosti (KIB)

Vedoucí práce: Ing. Jiří Buček, Ph.D.

21. února 2020

Poděkování

Doplňte, máte-li komu a za co děkovat. V opačném případě úplně odstraňte tento příkaz.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principu při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu) licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 21. února 2020

.....

České vysoké učení technické v Praze

Fakulta informačních technologií

© 2020 Tomáš Klas. Všechna práva vyhrazena.

Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí a nad rámec oprávnění uvedených v Prohlášení na předchozí straně, je nezbytný souhlas autora.

Odkaz na tuto práci

Klas, Tomáš. *Kubernetes klastr pro lámání hesel*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

Abstrakt

Hlavní náplní práce je nakonfigurování klastru pro lámání hesel. Tento klastr je řízen pomocí technologie Kubernetes. Program využívá ke své správné funkcionalitě kontejnery. Tyto kontejnery jsou tzv. Docker kontejnery. Použité technologie jsou v práci detailně popsány a rozebrány. Dále se práce zabývá rešerží ukládání hesel v současných systémech a tím jak hesla vypadají. Na závěr na klastru bude proveden test různých metod pro lámání hesel. Tyto metody budou popsány a bude analyzováno, jak je klastr efektní a výkonný pro daný typ lámání.

Klíčová slova Kubernetes, Ansible, klastr, Docker, distribuované lámání, hesla, hashcat, nasazení.

Abstract

The main goal of the thesis is to setup a cluster managed by kubernetes for password recovery. Next step is to describe used technologies as Docker, Ansible and Hashcat. Thesis contains description of how the passwords are stored and most known attacks to crack them. Successful deployment and password cracking leads to analyzing speed of the cluster and the particular cracking method.

Keywords Kubernetes, Ansible, cluster, Docker, distributed cracking, passwords, hashcat, deployment.

Obsah

Úvod	1
1 Cíl práce	3
2 Popis použitých technologií	5
2.1 Kubernetes	5
2.2 Ansible	5
2.2.1 Komponenty	5
2.2.1.1 Control node	5
2.2.1.2 Managed node	5
2.2.1.3 Iventory	6
2.2.1.4 Modules	6
2.2.1.5 Tasks	6
2.2.1.6 Playbooks	6
2.3 Docker	6
2.3.1 Stavební kameny Dockeru	7
2.3.1.1 Jmenné prostory	7
2.3.1.2 Kontrolní skupina	7
2.3.1.3 Sjednocující souborové systémy	8
2.3.2 Kontejner vs. virtuální počítač	8
2.3.3 Komponenty	8
2.3.3.1 Docker daemon	8
2.3.3.2 Docker klient	8
2.3.3.3 Docker registr	8
2.3.3.4 Obrazy	9
2.4 Hashcat	9
2.4.1 Proč použít Hashcat?	9
3 Hesla	11
3.1 Hašovací funkce	11

3.1.1	Vlastnosti hašovací funkce	11
3.1.2	Naorzeninový paradox	12
3.2	Formáty ukládání	12
3.2.1	Windows	12
3.2.2	Linux	12
3.2.3	MacOS	12
3.3	Útoky na hesla	12
3.3.1	Hrubou silou	12
3.3.2	Pomocí masky	12
3.3.3	Se slovníkem	12
3.4	Entropie hesla	12
3.5	Ochrana před různými útoky	12
4	Realizace	13
4.1	Nasazení	13
4.2	Spuštění s různými metodami útoku	13
5	Analýza rychlosti	15
5.1	Hrubou silou	15
5.2	Pomocí masky	15
5.3	Se slovníkem	15
6	Test	17
7	Závěr	19
	Literatura	21
A	Seznam použitých zkratk	23
B	Obsah příloženého CD	25

Seznam obrázků

Seznam tabulek

2.1	Linuxové jmenné prostory	7
-----	------------------------------------	---

Úvod

Cíl práce

Popis použitých technologií

2.1 Kubernetes

2.2 Ansible

Ansible je automatizační nástroj pro konfiguraci systému, nasazení softwaru, aktualizací. Jeho nejsilnější stránka je nulové výpadky systému při aktualizaci balíčků, nebo automatické nastavovat dané zařízení.

Jeho hlavními cíly jsou jednoduchost a nenáročnost. Kód by měl být čitelný i pro lidi, kteří nejsou obeznámeni s programem. Je schopen pokrýt různě velké prostředí od malých podniků až po velice obsáhlou infrastrukturu.

Ansible se připojí na vzdálený počítač pomocí OpenSSH pomocí uživatele, který je současně přihlášen. Na spravovaném počítači není třeba žádný agent. Je možnost nakonfigurovat Ansible, aby pro připojení nepoužíval OpenSSH, ale i kerberos nebo LDAP.

2.2.1 Komponenty

2.2.1.1 Control node

Jakýkoliv počítač s nainstalovaným Ansible a pythonem, může spouštět příkazy nebo tzv. playbooks. Tento počítač se nazývá control node. Takových můžeme mít klidně více, ne však počítače, které mají nainstalovaný operační systém Windows.

2.2.1.2 Managed node

Je jakékoliv síťové zařízení. Managed nodes můžeme také nazývat jako hosts. Tyto zařízení nemusejí mít nainstalovaný Ansible, ale musejí mít nainstalovaný python. Ansible může být nakonfigurován, aby používal specifikovanou verzi pythonu, pokud není specifikována, spustí se na hostu jeho defaultní.

2.2.1.3 Inventory

Je seznam všech nastavovaných zařízení. Často se nazývá hostfile. v tomto souboru nastavujeme skupiny zařízení, jejich IP adresy a další specifikace, například jaký python má daný host použít.

2.2.1.4 Modules

Jsou to jednotlivé části kódu, které bude Ansible spouštět. Každý modul má speciální použití. Vše od správy uživatelů (user) přes nastavení systému (systemd) až k instalování balíčků (apt, yum). Můžeme spustit jeden modul v tasku, nebo více v playbooku. Pro přehlednost neuvádím všechny možné moduly, jelikož je jich přes tři tisíce.

2.2.1.5 Tasks

Jsou jednotky, které se musejí provést. Nejčasteji specifikované v deployment souboru.

2.2.1.6 Playbooks

Je seřazený seznam tasků, které se musí vykonat. Ničemu neuškodí pokud se playbook spustí znovu, protože Ansible skontroluje stav daného tasku. Playbooky jsou psané podle konvencí YAMLu.

2.3 Docker

Docker je otevřená platforma pro vývoj, dodání a spouštění aplikací. Umožňuje oddělení aplikací od infrastruktury, tedy můžeme dodávat software rychleji a bez problémů, které se váží k různorodosti prostředí, ve kterém aplikace běží. Svou fylozofií jsou velice podobné virtualním počítačům. Rozdíly mezi těmito různými pohledy na věc budou rozebrány dále v textu.

Docker zprostředkovává platformu pro zabalení aplikace i se všemi jejími závislostmi. Izoluje danou aplikaci od ostatních běžících procesů na daném počítači a zajišťuje tak její bezpečí. Docker kontejner je velice nenáročný na hardware, můžeme jich tedy na daném počítači spustit velice mnoho.

Fylosofie kontejnerů je taková, že každý kontejner je odpovědný pouze za jednu danou část aplikace. Pro příklad máme naši webovou aplikaci. Budeme tedy mít alespoň tři docker kontejnery. Jeden na kterém poběží NGINX a bude zprostředkovávat naši aplikaci uživatelům. Další bude mít naši aplikaci a ve třetím poběží databáze.

Kontejnery fungují tedy jako malé počítače, mají izolované veškeré svoje systémové zdroje (paměť, procesy, internetové rozhraní). Díky tomuto mohou být rychle a jednoduše přidány, nebo odebrány.

2.3.1 Stavební kameny Dockeru

Docker je napsaný v jazyce Go a využívá vychytávky linuxového kernelu pro svojí funkcionalitu. Díky tomuto Docker perfektně funguje na počítačích, kde běží OS založený na Linuxu. Jiné operační systémy jako je například Windows se s tímto úkolem vypořádávají složitěji. Vytváří virtuální prostředí ve kterém běží Linux a teprve v tomto prostředí mohou Docker spustit.

2.3.1.1 Jmenné prostory

Jmenné prostory zastřešují veškeré zdroje systému tak, že každý proces spuštěn v daném prostoru může používat pouze prostředky, které se váží k tomuto prostoru. Každému procesu se to jeví tak, že má svoje vlastní globální prostředky, které mohou vidět i ostatní procesy z jmenného prostoru, ale ne z jiného. Níže je možné vidět jmenné prostory, které je možné v Linuxu nalézt.

Tabulka 2.1: Linuxové jmenné prostory

Jméno	Popis
Cgroup	Cgroup root adresář
IPC	System pro komunikaci procesů, POSIX fronty
Network	Síťové rozhraní, protocols, ports, etc
Mount	Připojená zařízení
PID	ID procesů
User	Uživatelská ID a ID skupin
UTS	Hostname a NIS doménu

Při spuštění kontejneru dojde k vytvoření procesu na hostitelském systému. Procesy dostanou od systému nějaké PID a chovají se jako normální procesy. Pokud se však přihlásíme do kontejneru (command: `docker exec -it name bash`) a podíváme se na procesy běžící v daném kontejneru uvidíme, že procesy mají jiná PID a určitě mají i PID=1. Toto nám umožňuje jmenné prostory.

Každý kontejner může mít svůj vlastní souborový systém a svoje síťové rozhraní. Vše co můžeme oddělit mezi hostitelem a kontejnery je uvedeno v tabulce výše.

2.3.1.2 Kontrolní skupina

Je to vlastnost Linuxového kernelu. Jejich hlavní funkcí je limitovat zdroje. V Dockeru se používají protože dovolují sdílet prostředky mezi hostitelským systémem a dalšími kontejnery.

Často dochází k záměně pojmů mezi kontrolními skupinami a jmennými prostory. Znovu to tedy shrňme. Kontrolní skupinaz, nebo-li cgroups omezují co můžeme použít a jemenné prostoraz nebo-li namespaces omezují co jsme schopni vidět v systému.

2.3.1.3 Sjednocující souborové systémy

Sjednocující souborový systém kombinuje jmenné prostory dvou či více souborových systémů a vytváří tak jediný spojený jmenný prostor. Docker využívá vlastností takových souborových systémů pro vytváření bloků pro kontejnery. Docker efektivně pracuje s následujícími souborovými systémy:

- AUFS
- btrfs
- vfs
- DeviceMapper

Tyto souborové systémy jsou schopné v tzv. větvích kombinovat soubory a

2.3.2 Kontejner vs. virtuální počítač

2.3.3 Komponenty

2.3.3.1 Docker daemon

Docker daemon nebo-li dockerd poslouchá dotazy na docker API a spravuje objekty jakou jsou docker obrazy, kontejnery, síť a úložiště. Komunikuje ale i s dalšími daemony, aby byl schopen řídit službu Docker.

2.3.3.2 Docker klient

Je to primární cesta, jak komunikovat s Dockerem. Když použijeme příkazy, jako jsou "docker run", klient odešle příkazy daemone zmíněného výše.

2.3.3.3 Docker registr

Docker registr je úložiště pro naše Docker obrazy. Bez předchozího nastavení hledá dockerd obrazy, které chceme spustit ve veřejném Docker registru. Obrazy však mohou být dostupné i lokálně, nebo na nějaké jiné službě, např.: gitlab container registry.

Do styku s registrem přicházíme hlavně ve chvílích, kdy provádíme příkazy docker pull, docker push a docker run. Tyto příkazy vždy potřebují znát obraz, který bude spouštěn jako základní vrstva pro nový kontejner, nebo bude stáhnut na lokální počítač, či nasdílen do registru.

2.3.3.4 Obrazy

Můžeme si to představit jako šablonu, na které je spuštěn kontejner. Obraz může být složen z vícero obrazů, nebo z nich vycházet.

Pro vytvoření obrazu je třeba soubor Dockerfile. Tento soubor obsahuje jednoduché kroky, které je třeba vykonat pro vytvoření konkrétního obrazu. Např.: jaké použijeme a zveřejníme porty, jaké balíčky chceme ve vytvořeném obrazu mít atd.

Každý příkaz v Dockerfilu vytvoří na locálním počítači tzv. vrstvu, kterou při úpravě Dockerfilu mění nebo předělává pouze pokud byla změněna.

2.4 Hashcat

2.4.1 Proč použít Hashcat?

Hesla

Hesla můžeme vidět všude a ne jen v informatice. Pokud se podíváme zpět do historie např. do doby velkého Caesara a jeho šifry, ke které je třeba znát číslo, o které se posouvají znaky ve zprávě. Jak tedy můžeme vidět, hesla neslouží pouze k naší autentizaci vůči nějaké službě či serveru. Může je také použít k podepsání citlivých dokumentů jako je třeba příloha e-mailu. Následně pak nemůžeme popřít jeho poslání. Tomuto se říká elektronický podpis.

Hesla však mají nejednu nevýhodu. Útočník může s naším nebo i bez našeho vědění odhalit naše heslo a tím nám narušit naše soukromý. Hesla mohou také být v systémech, které používáme uložena nepatřičným způsobem, jako je například čistý text bez použití žádných ochranných prostředků.

Hesla též mohou ze systému uniknout. V tomto případě, pokud byla hesla uložena neptřičným způsobem nemusí se potenciální útočník nějak přemáhat, aby uživatele kompromitoval. Proto se zaměříme na to jak mohou a jak skutečně jsou uložena v nejpoužívanějších systémech.

3.1 Hašovací funkce

Jsou to takové funkce $f: X \rightarrow Y$, pro něž je snadné z jakékoli hodnoty $x \in X$ vypočítat $y = f(x)$, ale pro náhodně vybraný obraz $y \in f(X)$ nelze v relevantním čase najít její vzor $x \in X$ tak, aby $y = f(x)$.

Přitom víme, že takový vzor existuje nebo jich existuje dokonce velmi mnoho. To kolik jich existuje se odvíjí jakou hašovací funkci použijeme.

3.1.1 Vlastnosti hašovací funkce

Abychom mohli funkci považovat za hašovací, musí mít následující vlastnosti:

- jakékoliv množství vstupních dat poskytuje stejně dlouhý výstup (otisk),
- malou změnou vstupních dat dosáhneme velké změny na výstupu,

3. HESLA

- z hashe je prakticky nemožné rekonstruovat původní text zprávy,
- v praxi je vysoce nepravděpodobné, že dvěma různým zprávám odpovídá stejný hash, jinými slovy pomocí hashe lze v praxi identifikovat právě jednu zprávu (ověřit její správnost).

3.1.2 Naorzeninový paradox

3.2 Formáty ukládání

3.2.1 Windows

Windows se chovají jinak v doméně a jinak mimo ní. Pokud je počítač v doméně je preferován autentizační protokol kerberos. V současných Windows Server edicích je implementován Kerberos verze 5. Kerberos v základní nastavení operuje na portu 88 a k šifrování používá symetrickou šifru. Pokud počítač není nastaven aby se autentikoval pomocí protokolu Kerberos používají Windows šifrování NTLM.

3.2.2 Linux

Hesla v linuxových systémech se skládají ze dvou konkrétních souborů.

/etc/shadow - obsah a strukturu toho souboru můžeme vidět na následujícím obrázku.

/etc/passwd - obsah a strukturu tohoto souboru můžeme vidět na následujícím obrázku.

V /etc/shadow jsou hesla uložena pomocí hashe.

3.2.3 MacOS

3.3 Útoky na hesla

3.3.1 Hrubou silou

3.3.2 Pomocí masky

3.3.3 Se slovníkem

3.4 Entropie hesla

3.5 Ochrana před různými útoky

Realizace

4.1 Nasazení

4.2 Spuštění s různými metodami útoku

Analýza rychlosti

- 5.1 Hrubou silou**
- 5.2 Pomocí masky**
- 5.3 Se slovníkem**

KAPITOLA **6**

Test

Závěr

[1] test

Literatura

- [1] D. Merkel, “Docker: lightweight linux containers for consistent development and deployment,” *Linux journal*, vol. 2014, no. 239, p. 2, 2014.

Seznam použitých zkratek

GUI Graphical user interface

XML Extensible markup language

Obsah přiloženého CD

	readme.txt.....	stručný popis obsahu CD
	exe	adresář se spustitelnou formou implementace
	src	
	impl.....	zdrojové kódy implementace
	thesis	zdrojová forma práce ve formátu L ^A T _E X
	text	text práce
	thesis.pdf	text práce ve formátu PDF
	thesis.ps	text práce ve formátu PS