FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BEZPEČNOST ICT 1 (BPC-IC1)

Útok na jména a hesla uživatelů na SSH serveru

Autoři:

Jakub Jedlička, xjedli24

Peter Kopec, xkopec51

Maxim Ilyuschenkov, xilyus00

Brno 2020

1. Cíle laboratorní úlohy

V laboratorní úloze se naučíte vytvořit uživatele na serveru, běžící na operačním systému Ubuntu. Vyzkoušíte si pracovat z funkcí balíčku Fail2Ban. Dále se naučíte základy práce z funkcemi git a nmap. Dále si vyzkoušíte napadnutí serveru na základě enumerace přes uživatele, společně s pokusem o získaní uživatelského hesla. Kde tyto informace použijete k přístupu na server.

2. Teoretický úvod

Základ útoku vychází z nalezené zranitelnosti nalezené v roce 2018, která nese název CVE-2018-15473. Vyskytuje se na SSH serverech, které používají OpenSSH do verze 7.7. Tato zranitelnost využívá chybu v odpovědi SSH serveru na dotaz o přihlášení uživatele, kde odpovídá, že existuje nebo neexistuje, neboli nedává univerzální odpověď, z které nelze poznat, jestli uživatel existuje v databázi nebo neexistuje. Jelikož se dají zjistit uživatelská jména, tak k nim lze zjistit hesla, pokud nejsou dostatečně silná a SSH server je nesprávně nastavený.

Útok na hesla uživatelů muže probíhat jedním ze dvou způsobů. Prvním způsobem je brute force attack, neboli útok hrubou silou, který využívá všechny možné kombinace zvolených znaků společně s počtem předpovídaných znaků v hesle. Čím větší délka hesla, tím exponenciálně roste počet možností. Počet možností se spočítá podle vzorce $f(x) = \sum_{n=1}^{\infty}(k\hat{}n)$, kde k je počet znaků, které se použijí, například použití všech malých písmen abecedy bude k = 26. Dále n je rovno počtu předpovídaných znaků v hesle. Tento způsob je použitelný na krátká hesla, při délce hesla 6 znaků a použití všech malých písmen abecedy, by se muselo v nejhorším případě projít 321 272 406 kombinací hesel. Druhým způsobem je dictionary attack, neboli slovníkový útok. Slovníkový útok je založen na iteraci přes slovník, veřejně známých hesel nebo vlastních možností hesel.

Funkce Fail2Ban je používaná často pro omezení neplatných počtů pokusů o přihlášení na uživatelský účet nebo z jedné IP adresy.

3. Praktická část

3.1. Příprava pracoviště

V aplikaci Oracle VM VirtualBox naimportujte virtuální stroj ubuntu_server. Soubor > Importovat appliance, zde si zvolíte ubuntu_server.ova. V dalším kroku zvolíte Include only NAT network adapter MAC addresses a potvrdíte stiskem tlačítka import.
Dále si zde stáhnete z adresy Kali linux 64-Bit pro VirtualBox a naimportujete ho stejným způsobem jako SHH server. Následně obě dvě virtualizovaná prostředí spustíte.

3.2. Příprava SSH serveru

Přihlašovací údaje na server jsou jméno: student, heslo: student.
Přidáte si uživatele Bob, Alice, Eva a xlogin00 kde bude použit váš studentský login, těmto účtům budou nastaveny hesla následovně, pro uživatele Bob bude bandit, Alice bude 0c, Eva bude kachnicka, xlogin00 bude vaše studentské ID.

```
1 kód   sudo adduser Bob
```

V případě změny hesla lze použít příkaz passwd.

```
2 kód    sudo passwd Bob
```

Pomocí příkazu ifconfig si zjistíte IP adresu serveru a ti si někde poznamenáte.

```
3 kód    Ifconfig
```

Dále pomocí příkazu apt-get nainstalujete balíček fail2ban

```
4 kód    sudo apt-get install fail2ban
```

3.3. Konfigurace Kali linux

Přihlašovací údaje do kali jsou jméno: kali, heslo: kali.
Otevřete si terminál a vyzkoušejte ping na server, jestli máte přístup na server a následně zkuste ping na IP 8.8.8.8, abyste vyzkoušeli, jestli máte přístup k internetu.

```
5 kód    ping 8.8.8.8 –c 4
```

Argument c slouží k určení počtu pokusů.
Pomocí příkazu git clone si naklonujte repozitář z www.github.com/jedla97/ICT1, který obsahuje veškeré potřebné soubory k této laboratorní úloze. A poté se do této složky přepněte.

```
6 kód    git clone www.github.com/jedla97/ICT1
```

Ze složky /usr/share/wordlist zkopírujte soubor rockyou.txt.gz a následně pomocí příkazu gunzip rozbalte rockyou.txt.gz.

```
7 kód    cp /usr/share/wordlists/rockyou.txt.gz
8 kód    gunzip rockyou.txt.gz
```

Z důvodu kompatibility nastavíme python knihovnu paramiko na její dřívější verzi 2.0.8

```
9 kód    pip install paramiko==2.0.8
```

3.4. Zjištění parametrů serveru pomocí příkazu nmap

Pomocí příkazu nmap lze zmapovat pomocí paketů na určitou IP adrese nebo doménu jaký operační systém stanice používá, jak je nastaven firewall a spousty dalších činností. Používá se také pro mapovaní celé sítě. Pomocí příkazu nmap zjistěte podrobnosti o serveru za použití argumentů –A, který slouží pro detekci OS a jeho verze, -v, který složí pro detailnější výpis.

```
10 kód   sudo nmap –A –v [IP serveru]
```

Jak můžete vidět tak náš testovací server používá SSH verzi x, která je zranitelná na průchod přes uživatelská jména.

3.5. Získaní existujících uživatelů na serveru ze slovníku

Ve složce enum se nachází soubor pro zjištění existujících uživatelských jmen na serveru, který má možnost procházet ze slovníku uživatelských jmen nebo jednotlivé uživatelské jméno. Spusťte sss_user _enum.py se slovníkem names.txt a jeho výstup uložte do users.txt

```
11 kód  sudo python enum/ssh_user_enum.py –userList
   txtSources/names.txt     –outputFile users.txt [IP serveru]
```

Kde –userList specifikuje slovník s uživatelskými jmény, -outputFile specifikuje výstupní soubor s uživateli a jejich existencí.
Pomocí příkazu grep a cut oddělte neexistující uživatele od existujících a uložte do nového souboru validusers.txt. Následně si ho prohlédněte.

```
12 kód  grep 'is a valid user' usernames.txt | cut -d' ' -f1 >
   validUsers.txt
```

Jak lze vidět, zde lze vidět, že zde je více uživatelů než jsme vytvářeli. Tito uživatelé jsou v systému nastaveni jako výchozí při vytváření systému a taktéž se objevují v našem slovníku. Tyto uživatele odmažete a ponecháte zde pouze Alici, Boba a Evu. Co lze vidět dále, že uživatel xlogin00 nebyl nalezen, i presto že existuje. Důvod lze velmi jednoduše vysvětlit tím, že není obsažen v našem slovníku. Pro ujištění můžete použit program sss_user _enum.py s použitím argumentu –username místo –userList a bez použití uložení do souboru.

```
13 kód  sudo python enum/ssh_user_enum.py –username xlogin00 [IP
   serveru]
```

Po provedení se zobrazí „xlogin00 is valid user“

3.6. Pokus o získání uživatelských hesel

Pomocí programu passwrdcrack.py se pokuste získat hesla nalezených uživatelů. Tento program obsahuje dvě metody pokusu o prolomení hesla. První z nich je útok hrubou silou ten zvolíte argumentem –bfa, argument –nf udává z jakého zdroje chcete čerpat uživatelská jména, argument –ip udává na kterou adresu se chcete pokusit útočit. Dále zde jsou volitelné argumenty –bfas který udává od kolika znaků se bude začínat, -bfae který udává na kolika znacích se bude končit, -of zde se dá určit soubor do kterého se uloží prolomená hesla.

```
14 kód  sudo python passwrdcrack.py –bfa bfa –bfas 0 –bfae 2
   –nf validUsers.txt –ip [IP serveru] –of crackedUsers.txt
```

Po prolomení Alice zastavte program pomocí ctrl + c. Dále se pokuste prolomit uživatele Bob pomocí módu na slovníkový útok. Za použití argumentů –un kterým se specifikuje uživatelské jméno, -pf kterým se specifikuje slovník s hesly, -of zvolte stejný jako v předchozím kroku, -ip zvolte IP adresu serveru.

```
15 kód  sudo python passwrdcrack.py –un Bob –pf rockyou.txt –of
   crackedUsers.txt –ip [IP serveru]
```

U uživatele Eva se nepodaří najít, z důvodu, že pro útok hrubou silou je příliš dlouhé. Slovníkovým útokem se nepodaří nalézt, jelikož slovník neobsahuje slovo kachnicka. Zkontrolujte si pomocí příkazu grep. Z tohoto důvodu se nemá smysl pokoušet, jelikož slovník rockyou.txt obsahuje 14 344 392 hesel a program passwrdcrack jich projde za 1 min přibližně 50.
Se získanými hesly si vyzkoušejte připojit na server pomocí ssh a vytvořte soubor bylJsemTu.txt

```
16 kód  ssh uživatel@[IP serveru]
```

3.7. Zapnutí Fail2Ban na serveru a vyzkoušení obrany

V souboru jail.local nacházející se v /etc/fail2ban zde můžete měnit politiku fail2ban. Nastavte počet opakovaných pokusů na 10 a soubor uložte.

```
17 kód  vi /etc/fail2ban/jail.local
```

Zapněte obranný software fail2ban.

```
18 kód  Sudo service fail2ban start
```

A zkuste opakovat postup 3.5 Získaní existujících uživatelů na serveru ze slovníku. Prvně se souborem validUser.txt a poté ze souborem txtSource/names.txt. Po provedení můžeme vidět, i přesto že server obsahuje zranitelnost tak se tento útok nedá provést automatizovaně. To stejné platí o útoku na hesla, na něž se vztahuje také počet pokusů. To je v našem případě 10. Pokud počet pokusů překročí hranici 10 pokusů, IP adresa se na určenou dobu dostane na blocklist. Ten si zobrazíte příkazem níže.

```
19 kód  sudo fail2ban-client status sshd
```

4. Samostatný úkol

Zjistěte, jestliže uživatelé Jakub, Peter, Maxim existují na serveru. Pokud existují, pokuste se získat přístup k jejich účtům a zkopírovat obsah jejich adresářů do vaší složky. Pro kopírovaní použijte příkaz scp a vytvořte si složku do které uložíte stažené soubory.

```
20 kód  Scp uživatel@[IP serveru] :složkaNaServeru SložkaKdeUložit
```

Před začátkem samostatného úkolu vypněte fail2ban.

5. Bibliografické citace

1. ***specopssoft.com.*** **[Online] Specops Software. [Citace: 17. 04 2020.] https://specopssoft.com/blog/what-is-password-dictionary-attack/.**

2. *hacksplaining.com.* [Online] Hacksplaining. [Citace: 17. 04 2020.] https://www.hacksplaining.com/prevention/user-enumeration.

3. *en.wikipedia.org.* [Online] Wikimedia Foundation, Inc. [Cited: 17 04, 2020.] https://en.wikipedia.org/wiki/Brute-force_attack.

4. *en.wikipedia.org.* [Online] Wikimedia Foundation, Inc. [Citace: 17. 04 2020.] https://en.wikipedia.org/wiki/Dictionary_attack.

5. *cve.mitre.org.* [Online] The MITRE Corporation. [Citace: 14. 02 2020.] cve.mitre.org. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473.

6. *nvd.nist.gov.* [Online] National Institute of Standards and Technology. [Citace: 14. 02 2020.] https://nvd.nist.gov/vuln/detail/CVE-2018-15473.

7. Gardner, Justin. *github.com.* [Online] [Citace: 03. 03 2020.] https://github.com/Rhynorater/CVE-2018-15473-Exploit.

8. Jakub, Jedlička. *github.com.* [Online] [Citace: 03. 03 2020.] https://github.com/jedla97/ICT1.

9. *nmap.org.* [Online] [Citace: 09. 04 2020.] https://nmap.org/.

10. *fail2ban.org.* [Online] [Citace: 11. 04 2020.] https://www.fail2ban.org/.

11. *paramiko.org.* [Online] http://www.paramiko.org/.