TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Simulace penetračního testování na zařízení se systémem Debian Strech Lite

Ročníkový projekt

Studijní program: B2646 – Informační technologie
Studijní obor: 1802R007 – Informační technologie

Autor práce: **Jiří Turyna**
Vedoucí práce: Ing. Mojmír Volf

Liberec 2018

Prohlášení

Byl jsem seznámen s tím, že na můj ročníkový projekt se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mého ročníkového projektu pro vnitřní potřebu TUL.

Užiji-li ročníkový projekt nebo poskytnu-li licenci k jeho využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Ročníkový projekt jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mého ročníkového projektu a konzultantem.

Současně čestně prohlašuji, že texty tištěné verze práce a elektronické verze práce vložené do IS STAG se shodují.

9. 9. 2020 Jiří Turyna

Simulace penetračního testování na zařízení se systémem Debian Strech Lite

Abstrakt

Tato práce se zabývá simulací penetračního testování a je určena ke vzdělávacím účelům. Obsahuje manuály, dle kterých by měl případný zájemce postupovat. Tyto manuály jsou rozděleny na Blue tým a Red tým. Blue tým má za úkol nastavit Raspberry Pi a úmyslně vytvořit chyby, kterých by měl následně Red tým využít k ovládnutí celého systému. Manuály obsahují podrobné kroky společně s jejich vysvětlením, odkazy na stránky třetích stran a případnými nápovědami pro objasnění.

Poděkování

Rád bych poděkoval všem lidem, kteří se jakkoliv podíleli na zpracování této práce. Zejména bych rád poděkoval vedoucímu práce panu Volfovi za konzultace, bez kterých bych práci jenom těžko dokončil. Dík patří také lidem, kteří mi pomohli s testováním manuálů a mojí mamce Vladěně Turynové, za kontrolu gramatických a typografických chyb.

Obsah

Seznam zkratek

EU	Evropská unie
TUL	Technická univerzita v Liberci
FM	Fakulta mechatroniky
OS	Operační systém
SD	Paměťová karta
SSH	Secure shell
FTP	File Transfer Protocol
SFTP	Secure shell File Transfer Protocol
LAMP	Linux Apache Mysql Php
PHP	Hypertext Preprocessor
HTTP	Hypertext Transfer Protocol
SQL	Structured Query Language

1 Úvod

Tato práce se zabývá simulací penetračního testování. Penetrační testování, a mnoho dalších, je jednou z metod testování zabezpečení systému, zvaného jako etické hackování. Etický hacking se oproti neetickému v podstatě ničím neliší. Hlavním rozdílem je, že etický hacker je většinou najatý firmou k nalezení bezpečnostních slabin v jejich systému, které nahlásí a případně doporučí jejich opravení. Neetický hacker by neošetřenou chybu v systému mohl zneužít ke svému obohacení nebo ublížení dané firmě.

Penetrační testování se dělí na tři typy. První, Black box je typ testu nejvíce podobný realitě. Penetrační tester, stejně jako reálný hacker, nemá žádné informace o systému, který má testovat. To znamená, že před samotným útokem musí proběhnout přípravná fáze, ve které hacker sbírá informace o svém cíli. Při druhém typu testu Gray box, zná tester pouze základní informace o systému (přítomnost firewallu, schéma komunikace...). Posledním typem je White box. Tento typ penetračního testování není běžný, protože v tomto případě zná tester všechny informace o svém cíli a má také přístup ke zdrojovým kódům.

Pro průběh celé této simulace byl zvolen typ Gray box. Hlavním důvodem bylo snížení časové náročnosti o proti typu Black box. Naopak využití typu White box by nesplňovalo studijní předpoklad této práce.

2 Motivace

Hlavní motivací této práce bylo vytvoření cvičné úlohy a jejího řešení pro budoucí studium. Zároveň by si na základě této práce měli studenti uvědomit některá bezpečnostní rizika linuxových zařízení a vyzkoušet si, jak by podobný útok mohl probíhat.

Simulace se odehrává v izolované lokální síti, kde se vyskytují počitače s linuxovou distribucí a lze také připojit zařízení s operačním systémem Windows.

Stejně jako při reálném penetračním testování i v tomto ročníkovém projektu existují dva týmy. Tyto jsou označovány jako Blue tým a Red tým. Jako výsledek práce byl pro každý tým zvlášť vypracován manuál. Manuály představují sadu instrukcí a návodů, podle kterých by se měli oba týmy řídit a dokončit svůj úkol.

3 Rešerše a proces tvorby simulace

Prvním zadáním mého projektu byla rešerše metod. Celkové zadání se totiž rýsovalo během celého semestru a jelikož jsem celý projekt začal pouze se základními znalostmi linuxu byli pro mě místy obtížné i běžné věci jako instalace operačního systému na SD kartu nebo samotné přihlášení k Raspberry Pi.

Prvotní myšlenkou celého projektu byla simulace útoku z jednoho Raspberry Pi na druhé, ale vzhled k časové náročnosti, výpočetnímu výkonu Raspberry Pi a omezeným právům v učebnách jsme se s vedoucím projektu pane inženýrem Volfem rozhodli pro simulaci pomocí virtualního počítače přes službu Virtual Box.

Během semestru jsme narazili na několik problémů. Prvním z nich byl zadávání hesel tak, aby je v pozdější fázi dokázal Red tým prolomit. V ideálním případě bychom nechali Blue tým vytvořit libovolné heslo o délce alespoň 6-8 písmen. To se však stalo nereálné, když jsme zjistili, že Raspberry Pi je schopno pomocí modulu Metasploit otestovat přibližně jedno heslo za sekundu. Museli jsme tedy volbu hesel omezit.

Vznikl tedy seznam celkem dvaceti hesel, ze kterých si může Blue tým libovolně vybrat. Tyto hesla jsou speciálně připravena pro nácvik této simulace a jejich prolomení by za dodržení podmínek popsaných v tomto projektu mělo být v rozmezí od 5 do 15 minut od spuštění útoku.

Tím však vznikl další problém. Bylo potřeba vyřešit jak by měl Red tým postupovat, aby na tato hesla přišel.

První možností bylo využití regulárních výrazů při zadávání hesel v modulu Metasploit tak, aby testoval pouze hesla, která by odpovídala určitému zadání a tím se celý proces dramaticky urychlil. Tento způsob se nám však nepodařil a my jsme si uvědomili, že nejjednodušší bude vytvoření slovníku hesel s konkrétním vzorem.

Mým prvním nápadem bylo naprogramování metody, který by potřebný slovník vygenerovala, ale tato možnost by nesplňovala jak časovou náročnost 180 minut, tak hlavní myšlenku projektu a testovala by schopnosti programování místo vzdělávání v oblasti bezpečnosti.

Nakonec jsem však narazil na slovníkový generátor Crunch, který náš problém hravě vyřešil pomocí parametru "vzor".

Uvědomili jsme si, že bude potřeba celý proces provést na školních počítačích. Jenomže studenti na těchto zařízeních mají pouze omezená práva a budu schopni nainstalovat potřebné projekty jako modul Metasploit nebo slovníkový generátor Crunch. Nejjistější bylo vytvoření virtuálního počítače přes službu Virtual Box kde mají studenti však potřebná práva.

4 Blue tým

Při reálném penetračním testování vznikají dva týmy. Prvním z nich je Blue tým, který se stará o nastavení systému a jeho zabezpečení. V našem případě má Blue tým za úkol následující. Dle manuálu, mají na starost instalaci LAMP, nastavení iptables, přidání několika nových účtů, aktualizaci systému a následné předání Raspberry Pi Red týmu.

4.1 Budete potřebovat:

- Raspberry Pi a SD kartu
- Ethernet kabel a přístup k síti
- Zařízení s OS Linux nebo Windows (rozdílný postup pro připojení, ale konfigurace je stejná)

4.2 Příprava zařízení

- **Nutno dodržet postup! Pokud by došlo ke vložení SD karty po připojení k napájení je velmi pravděpodobné, že by vznikl zkrat zařízení**
- Připojte k Raspberry ethernet kabel, který vede do sítě
- Vložte SD kartu s OS
- Připojte zařízení k napájení

4.3 Připojení k Raspberry Pi - Linux

- Následující krok aplikujte pokud tuto úlohu plánujete vypracovat na vlastním linuxovém systému nebo na školních počítačích s linuxovou distribucí.

4.3.1 SSH

- SSH je zabezpečený kryptografický protokol sloužící k bezpečnému přenosu dat přes internet. Využívá se hlavně k ovládání vzdálených počítačů přes SSH port (22).
- Vygenerujte si SSH klíč
  Nápověda (příkaz):

> **SSH-keygen**

4.3.2 Zjistěte IP adresu Raspberry Pi

- Máte několik možností. Doporučuji software **Advanced Ip Scanner** nebo aplikaci **Net Analyzer** na Android zařízení
- Ověřte přes příkaz **ping**, že máte správnou IP adresu
  Odkaz k dokumentaci pro příkaz ping:

> https://linux.die.net/man/8/ping

4.3.3 Připojení k Raspberry Pi

> příkaz: **SSH Username@ip-adressa-Raspberry**

- Dle základního nastavení je Username: pi a Password: raspberry
- Pokud jste se přihlásili, můžete pokračovat do další části.
  Odkaz k dokumentaci pro příkaz SSH:

> https://man.openbsd.org/SSH.1

4.4 Připojení k Raspberry Pi - Windows

- Následující krok aplikujte pokud tuto úlohu plánujete vypracovat na systému Windows místo školních počítačů s linuxovou distribucí.

4.4.1 Stáhněte si:

- **WinSCP** - Windows klient pro FTP, WebDav a SFTP

  `https://winscp.net/eng/download.php`

- **Putty** - Open source projekt umožňující službu SSH pro systémy Windows

  `https://www.putty.org/`

4.4.2 SSH

- SSH je zabezpečený kryptografický protokol sloužící k bezpečnému přenosu dat přes internet. Využívá se hlavně k ovládání vzdálených počítačů přes SSH port (22).
- Vaším úkolem je vygenerovat si SSH klíč
  Nápověda:

  Program **Puttygen**, který jste si nainstalovali společně s WinSCP nebo příkaz:

  ssh-keygen (4.1)

4.4.3 Zjistěte IP adresu Raspberry Pi

- Máte několik možností. Doporučuji software **Advanced Ip Scanner** nebo aplikaci **Net Analyzer** na Android zařízení
- Ověřte přes příkaz **ping**, že máte správnou IP adresu
  Odkaz k dokumentaci pro příkaz ping:

  `https://linux.die.net/man/8/ping`

4.4.4 Připojení k Raspberry Pi

- Spusťte program Putty
- V kategorii **Session** vyplňte **Host Name (or IP address)** a klikněte na **Open**
- Přihlášení je dle základního nastavení Username: pi a Password: raspberry

4.5 Konfigurace Raspberry

4.5.1 Aktualizace systému

- Jednou ze základních věcí po prvním spuštění systému je jeho aktualizace. Rozhodně nechcete pracovat na neaktuálním systému, kde je několik měsíců neopravená chyba.

  Odkaz k dokumentaci pro příkaz sudo:

  `https://www.sudo.ws/man/1.8.2/sudo.man.html`

  Nápověda:

  - Systém aktualizujete následujícími příkazy:

    sudo apt-get update (4.2)

    sudo apt-get upgrade (4.3)

    sudo apt-get dist-upgrade (4.4)

4.5.2 Změna hesla pro uživatele Pi

- Dalším důležitým aspektem zabezpečeného systému jsou silná hesla. Jedním z prvních kroků, které potenciální útočník zcela jistě využije, je testování běžného přihlašování jako **pi-raspberry** nebo **root-root** (Username-Password).
- **Zvolte silné heslo (alespoň 8 znaků)**

  Nápověda (příkaz):

  sudo passwd pi

4.5.3 Přidání na Raspberry Pi dalších dvou účtů - User1 a User2

- **Hesla pro tyto účty vyberte z přiloženého textového souboru bluePasswords.txt.**
- **Instrukce pro druhý tým vychází z předpokladu, že dojde k dodržení tohoto kroku.**

  Nápověda:

  sudo adduser User1 (4.5)

  sudo adduser User2 (4.6)

4.5.4 Přidání práv uživatelům User1 a User2 k používání příkazů less, man, more

- Abychom umožnili uživatelům User1 a User2 používat příkazy "sudo less"atd., musíte upravit soubor sudoers.

  Nápověda 1 (otevření sudoers):

  sudo visudo -f /etc/sudoers

  Nápověda 2 (editace sudoers):

  - Pod sekci **User alias specification** přidáme povolení pro **user1** a **user2** k příkazům **less, man a more**

    user1, user2 ALL = (root) NOPASSWD: /usr/bin/less (4.7)

    user1, user2 ALL = (root) NOPASSWD: /usr/bin/more (4.8)

    user1, user2 ALL = (root) NOPASSWD: /usr/bin/man (4.9)

4.5.5 Instalace LAMP serveru

- Zkratka LAMP slouží pro Linux, Apache, MySQL a PHP. Jedná se o základní nastavení pro běžný linuxový server. Vaším úkolem je nainstalovat webserver Apache, systém řízení báze dat MySQL a Hypertextový Preprocesor PHP.

  Odkaz pro inspiraci:

  www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-instalace-lamp

Apache

- Apache je open source HTTP webový server. Slouží například k renderování statického (html) i dynamického obsahu (php).
- Nainstalujte na Raspberry Pi Web Server Apache a otestujte zadáním IP adresy do prohlížeče. **Nápověda:**

  sudo apt-get install apache2 -y

PHP

- Zkratka PHP slouží pro Hypertextový preprocesor. Jedná se o skriptovací jazyk, díky kterému můžeme vytvářet dynamický obsah webových stránek.
- Nainstalujte na Raspberry Pi skriptovací jazyk PHP, upravte soubor /var/html/info.php tak, aby při zadání do prohlížeče vypsal základní informace o PHP.

  Nápověda 1 (instalace):

  sudo apt-get install php libapache2-mod-php -y

  Nápověda 2 (info.php):

  - Upravte soubor info.php

    sudo nano /var/www/html/info.php (4.10)

  - Vložte následující příkaz:

    < ?php phpinfo ();? > (4.11)

- Opět vyzkoušejte v prohlížeči: ip-adresa-raspberry/info.php

MySQL

- MySQL je open source projekt zprostředkovávající databázovou službu pro OS Linux a Windows.
- Nainstalujte MySQL a otestujte příhlášením

  Nápověda (instalace)

  ```
  sudo apt install mysql-server php-mysql
  ```

  Nápověda (přihlášení)

  ```
  sudo mysql –user=root
  ```

4.5.6 Nastavení Iptables

- Iptables lze označit za linuxový firewall. Funguje jako soubor pravidel, které brání nechtěným akcím na serveru (například zakázení specifických portů).

1) Nainstalujte balíček Iptables-persistent sloužící k ukládání iptables

- **Příkaz:** sudo apt-get install iptables-persistent

2) Nastavte Iptables dle následujících požadavků

- Pravidla pro již ustálená spojení
- Povolte porty **80 (http), 22 (SSH)**
- Povolte port **3306 (mysql) pouze lokálně**
- **Drop pro ostatní porty**

  Nápověda 1 (ustálená spojení):

  ```
  sudo iptables -A OUTPUT -m state –state RELATED,ESTABLISHED -j ACCEPT
  ```
  (4.12)

  ```
  sudo iptables -A INPUT -m state –state RELATED,ESTABLISHED -j ACCEPT
  ```
  (4.13)

Nápověda 2 (SSH):

sudo iptables -A INPUT -p tcp –dport 22 -j ACCEPT (4.14)

Nápověda 3 (HTTP):

sudo iptables -A INPUT -p tcp –dport 80 -j ACCEPT (4.15)

Nápověda 4 (MYSQL local only):

sudo iptables -A INPUT -p tcp -s localhost –dport 3306 -j ACCEPT (4.16)

sudo iptables -A INPUT -p tcp –dport 3306 -j DROP (4.17)

Nápověda 5 (Ostatní porty):

sudo iptables -A INPUT -j DROP (4.18)

3) Přihlašte se jako root a uložte iptables

Přihlášení jako root: **sudo su** (4.19)

Uložení Iptables: **sudo iptables-save > /etc/iptables/rules.v4** (4.20)

4.6 Předání Raspberry Pi

- Nyní Raspberry Pi dostane Red tým, který se k Vám do systému pokusí nabourat.
- V případě, že budou úspěšní, mají za úkol vytvořit v adresáři /home/pi textový soubor se vzkazem. Vy tak můžete ověřit, že jejich práce byla úspěšná.

Gratuluji. Úspěšně jste dokončili tuto úlohu!

5 Red tým

Druhým týmem při penetračním testováním je Red tým, který v simulaci zastává roli potenciálního útočníka, snažící se o ovládnutí systému. Red tým si pomocí Virtual Boxu nainstaluje virtuální počítač s běžně dostupnou verzí linuxové distribuce Ubuntu, provede instalaci slovníkového generátoru Crunch, díky kterému vytvoří slovník hesel. Následně využije modulu Metasploit k provedení slovníkového útoku přes port SSH a přihlásí se k jednomu z účtů na Raspbery. Konečným krokem je provedení eskalace oprávnění a kompletní ovládnutí systému.

5.1 Budete potřebovat

- Nakonfigurované Raspberry Pi od Blue týmu, které je připojené k síti.
- Image Ubuntu (příloha)
- Virtual box

5.2 Instalace Ubuntu image ve Virtual Boxu

- Virtual box je multiplatformní nástroj, díky kterému můžete simulovat několik počítačů s libovolným operačním systémem zároveň. Ve Vašem případě, bude sloužit jako rozšíření linuxové distribuce Ubuntu, jelikož v učebně nemáte dostatečná práva nutná pro tuto úlohu.

5.2.1 Vytvoření virtuálního počítače s distribucí Ubuntu

- V příloze jste dostali image linuxové distribuce Ubuntu. Tu použijte k vytvoření virtuálního počítače (jde o běžně dostupnou image, ale vzhledem k její velikosti by stahování trvalo příliš dlouho).
- Postupujte dle instrukcí v instalaci a zapamatujte si heslo, které zadáte při vytváření účtu (budete ho potřebovat pro příkaz **sudo**).

5.3 Aktualizace systému

- Jednou ze základních věcí po spuštění systému je jeho aktualizace. Rozhodně nechcete pracovat na neaktuálním systému kde je několik měsíců neopravená chyba.

  Nápověda:

  - Systém aktualizujete těmito příkazy:

    sudo apt-get update (5.1)

    sudo apt-get upgrade (5.2)

    sudo apt-get dist-upgrade (5.3)

  Odkaz k dokumentaci pro příkaz sudo:

  https://www.sudo.ws/man/1.8.2/sudo.man.html

5.4 Instalace a spuštení modulu Metasploit

- Metaslpoit je projekt, který nabízí spousty modulů pro analyzování bezpečnostních slabin a je často využíván k penetračnímu testování. Ve Vašem případě bude Metasploit sloužit jako zprostředkovatel útoku na Raspberry Pi.

  Instalace Metasploit:

  https://linuxhint.com/install_metasploit_ubuntu

  Nápověda 1 (odkaz):

- Zkopírujte následující příkaz (nachází se i na doporučené stránce):

  ```
  curl https://raw.githubusercontent.com/rapid7/metasploit
  omnibus/master/config/templates/metasploit-framework-wrappers/
  msfupdate.erb > msfinstall && \
  ```

- Po instalaci vyzkoušejte jeho spuštění.

  Nápověda 2 (spuštění):

Metasploit se spouští příkazem:

msfconsole (5.4)

5.5 Samotný útok přes SSH

- Jedním z prvních útoků, který by reálný hacker vyzkoušel je tetsování základního přihlašování. Je až pozoruhodné jak často dochází při zabezpečení k lidské chybě a usnadňují tím hackerům práci.
- Proveďte útok přes port SSH a vyzkoušejte některá ze základních příhlašování jako je pi-raspberry, root-root a další (username-password).
- Zjistěte IP adresu Vašeho Raspberry Pi (např. přes příkaz Ipconfig nebo některou z aplikací sloužící k analyzování sítě. pozn.: ping nefunguje záměrně)
- Spusťte Metasploit (msfconsole)
- K provedení útoku budete používat modul SSH_login:

  Scanner SSH auxiliary modules:

  https://www.offensive-security.com/metasploit-unleashed/scanner-SSH-auxiliary-modules/

5.5.1 Nastavení modulu:

- **Modul vyberete následujícím příkazem:**

  use auxiliary/scanner/SSH/SSH_login

5.5.2 Zobrazení možností modulu

- **Možnosti modulu si zobrazíte příkazem:**

  show options

5.5.3 Nastavení modul dle následujících požadavků

- Nastavte heslo a přihlašovací jméno, které chcete otestovat (pi-raspberry, root-root, admin-admin...).
- Zadejte IP adresu Raspberry Pi
- Vyberte port útoku (22 - SSH)

set RPORT 22 - Nastaví port útoku

set RHOSTS - Specifikuje IP adresu Raspberry Pi

set Username - Vybere jméno uživatele

set PASSWORD - Zvolí heslo, si přejete otestovat

5.6 Instalace slovníkového generátoru Crunch

- Pokud se Váš předchozí pokus nezdařil, je zřejmé, že Blue tým zabezpečení nepodcenil a bude potřeba provést jiný vektor útoku. Tím je slovníkový útok.
- Dalším bodem je tedy instalace slovníkového generátoru. Ten nám bude sloužit k vytvoření textového souboru hesel, které použijete k prolomení přihlašování přes SSH port na Raspberry Pi. **Crunch:**

`www.cloudera.com/documentation/enterprise/5-4-x/topics/cdh_ig_crunch_install.html`

Instalace Crunch:

- Crunch nainstalujete zadáním následujícího příkazu do terminálu na Vašem virtuálním počítači:

sudo apt-get install crunch (5.5)

5.7 Vytvoření slovníku hesel

- Vytvořte ve Virtual boxu slovník hesel pomocí generátoru Crunch (instalovali jsme v bodě 3.4) tak, aby splňoval následující požadavky.
- **Víte, že na Raspberry Pi jsou vytvořeni 3 uživatelé: pi, User1 a User2**
- **O hesle jednoho z účtů víte tyto informace:**

  - Heslo je alphanumerického charakteru (písmena a/nebo čísla)
  - Heslo obsahuje pouze malé symboly
  - Délka hesla je přesně 6 znaků
  - Prvním znakem hesla je písmeno
  - Druhý znak je číslo **5**
  - Třetí znak je číslo **3**
  - Čtvrtý znak je písmeno **r**
  - **Poslední dva znaky hesla jsou čísla**

  Odkaz k dokumentaci pro generátor Crunch:

  `https://www.irongeek.com/i.php?page=backtrack-r1-man-pages/crunch`

  Užitečné funkce s Crunch:

  `https://null-byte.wonderhowto.com/how-to/tutorial-create-wordlists-with-crunch-0165931/`

  Nápověda 1 (rozsah):

  - Příkaz **Crunch 2 6 abcdef** vytvoří kombinaci znaků abcdef o délce od 2 do 6
  - Vy potřebujete délku přesně 6, tedy příkaz **Crunch 6 6**

Nápověda 2 (vzor):

- Vzor neboli pattern se v Crunch zadává argumentem "-t"společně se zadáním speciálních znaků.

  @ - reprezentuje malá písmena
  , - reprezentuje velká písmena
  % - reprezentuje čísla
  ∧ - reprezentuje ostatní speciální znaky

Nápověda 3 (výstup):

- Pomocí argumentu "-o"specifikujete kam se Váš slovník uloží a jak se bude jmenovat. Bez tohoto argumentu se slovník vypíše pouze na terminál.

Nápověda 4 (celý příkaz):

- Takto by měl vypadat Váš finální příkaz (slovník se uloží do Passwords.txt):

  Crunch 6 6 -t @53r%% -o Passwords.txt (5.6)

5.8 Provedení slovníkového útoku

5.8.1 Nastavení modulu

- Stejně jako u předchozího pokus nastavte IP adresu zařízení, port útoku 22 a jedno ze tří uživatelských jmen (pi, User1 nebo User2, dle vaší volby)
- Určete cestu ke slovníku hesel
- Nastavte možnosti VERBOSE a STOP_ON_SUCCESS na true

set PASS_FILE Passwords.txt
- Specifikuje cestu ke slovníku hesel

set VERBOSE true
- Bude Vám postupně vypisován výstup pro každé vyzkoušené heslo

set STOP_ON_SUCCESS true
- Pokud dojde ke shodě, celá operace se zastaví

- Ke shodě by mělo dojít do 15 minut od spuštění. V opačném případě je třeba vyzkoušet jiného uživatele.
- **Neztrácejte zbytečně čas! Blue tým má přesně zadané instrukce, dle kterých musí ke shodě s heslem dojít do 15 minut.**

5.8.2 Došlo ke shodě:

- Výborně, nyní již znáte jméno uživatele i heslo
- Přihlašte se k tomuto účtu přes SSH:

SSH ip.adresa.Vašeho.Raspberry

Odkaz k dokumentaci pro příkaz SSH:

`https://man.openbsd.org/SSH.1`

5.8.3 Ovládnutí zařízení:

Odkaz na článek o eskalaci oprávnění

`https://touhidshaikh.com/blog/?p=790`

- Přihlásili jste se k jednomu účtu na Raspberry Pi, jenomže tento účet má velmi omezená práva. Zjistěte, jaké příkazy můžete používat s příkazem **sudo**.

  Odkaz k dokumentaci pro příkaz sudo:

  `https://www.sudo.ws/man/1.8.2/sudo.man.html`

  Nápověda (příkaz):

  sudo -l

- Zjistili jste, že můžete použít příkazy **sudo man**, **sudo less** a **sudo more**. Proveďte eskalaci oprávnění a staňte se rootem.

  Nápověda (příkaz):

  ```
  sudo less /etc/hosts
  ```

- Ověřte, že se eskalace oprávnění povedla příkazem **whoami**

5.8.4 Vzkaz pro Blue tým

- Nyní před Vámi stojí poslední, a to nejtěžší úkol.
- V adresáři **/home/pi** vytvořte textový dokument s Vaším vzkazem pro Blue tým Tímto jim dáte najevo, že jste i Vy svoji úlohu úspěšně zvládli.
- Samozřejmě kreativitě se meze nekladou

Gratuluji. Úspěšně jste dokončili tuto úlohu!

6 Závěr

Tato simulace penetračního testování byla vytvořena pro vzdělávací účely Technické univerzity v Liberci s předpokladem jejího využití v některém z předmětů.

Z důvodu časové náročnosti reálného penetračního testování, byla simulace přizpůsobena podmínkám studia na Technické univerzitě v Liberci. Její časová náročnost vypracování by neměla přesáhnout hranici 180 minut. Jedná se o typ penetračního testování Gray Box (vysvětlení v kapitole 1. Úvod). Vzhledem k omezenému výpočetnímu výkonu Raspberry Pi při samotnému útoku, byla vytvořena sada hesel, které může Blue tým využití pro zabezpečení uživatelských účtů User1 a User2. Tyto hesla odpovídají časové náročnosti úlohy a prolomení každého jednoho z nich, při využití nástroje Metasploit a modulu SSH_login, by nemělo překročit hranici 15 minut. Fakt, že Red tým zná některé z částí hesla (první znak malé písmeno, poslední dva znaky čísla) není ryze didaktický předpoklad. V reálné situaci je běžné, že dojde k odchycení části hesla.

Věřím, že tato práce bude prospěšná jak studentům, kteří se s touto úlohou při svém studiu setkají, tak i případným zájemcům o penetrační testování a etický hacking.

Literatura

[1] ŠINDLER, Vojtěch. Zvýšení zabezpečení služeb sítě Liane. Liberec, 2017. Diplomová práce. Technická univerzita v Liberci. Fakulta mechatroniky, informatiky a mezioborových studií. Vedoucí práce Mojmír Volf.

[2] Kolouch, Jan CyberCrime / Jan Kolouch. 1. vydání. Praha : CZ.NIC, z.s.p.o., 2016. 522 stran : ilustrace ; 25 cm (CZ.NIC ; 14. publikace) [Právní stav byl zohledněn ke dni 1.8.2016; Přehled souvisejících právních předpisů] ISBN:978-80-88168-15-7

[3] Harris, Shon Hacking : manuál hackera / Shon Harris...[et al.]. 1. vyd.. Praha : Grada Publishing, 2008. 399 s. brož. ISBN:978-80-247-1346-5

[4] Přispěvatelé Wikipedie, Penetrační test [online], Wikipedie: Otevřená encyklopedie, c2017, Datum poslední revize 21. 03. 2017, 10:08 UTC, [citováno 19. 05. 2019] https://cs.wikipedia.org/w/index.php?title=Penetra%C4%8Dn%C3%AD_test&oldid=14814488

[5] Přispěvatelé Wikipedie, Hacker [online], Wikipedie: Otevřená encyklopedie, c2019, Datum poslední revize 21. 04. 2019, 12:00 UTC, [citováno 19. 05. 2019] https://cs.wikipedia.org/w/index.php?title=Hacker&oldid=17164237

[6] SHAIKH, Touhid. Abusing SUDO (Linux Privilege Escalation) [online]. Touhidshaikh.com, 11. 04. 2018 [cit. 19.05.2019]. Dostupné z touhidshaikh.com: https://touhidshaikh.com/blog/?p=790

[7] DOČEKAL, Michal. Správa linuxového serveru: Instalace LAMP [online]. Linuxexpres.cz, 16. 12. 2010 [cit. 19.05.2019]. Dostupné z Linuxexpres.cz: https://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-instalace-lamp