SUI ZI 2016/17

1. (3 boda) Navedena su dva ispisa naredbe netstat na napadnutom poslužitelju. U čemu je razlika? Identificirajte napade koje se izvode u oba ispisa. Ako je napadač u oba slučaja isto računalo, koja je njegova IP adresa?

ISPIS #1: netstat -ant

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	83.129.34.99:80	162.83.43.137:40136	SYN_RECV
...	...	...	...	...	...
tcp	0	0	83.129.34.99:80	162.83.43.179:40432	SYN_RECV
tcp	0	0	83.129.34.99:80	162.83.43.59:40058	SYN_RECV
tcp	0	0	83.129.34.99:80	162.83.43.69:40332	SYN_RECV

ISPIS #2: netstat -ant

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	83.129.34.99:22	83.129.34.220:40136	SYN_RECV
...	...	...	...	...	...
tcp	0	0	83.129.34.99:80	83.129.34.220:40432	SYN_RECV
tcp	0	0	83.129.34.99:81	83.129.34.220:40058	SYN_RECV
tcp	0	0	83.129.34.99:82	83.129.34.220:40322	SYN_RECV

U prvom ispisu vidimo da su nasumično odabrane adrese maske 162.83.43.1/255 nasumičnog porta visoke vrijednosti koje su slale SYN zahtjeve poslužitelju, kako poslužitelj nije dobio odgovor (veze su u poluotvorenom stanju) možemo zaključiti da su ip adrese lažirane na nepoŠtojeća računala - IP spoofing. Sve ovo nas navodi na SYN flood DoS napad.

U drugom ispisu vidimo da je poslan SYN zahtjev na sve portove našeg poslužitelja, a oni na kojima se nalazi usluga su ostali u poluotvorenom stanju. Kako nema odgovora opet pretpostavljamo IP spoofing. U ovom slučaju dokazi nas navode na TCP skeniranje.

Ne možemo prepoznati IP adresu napadača.

2. (1 bod) Napadač napada dva nepoznata računala iz iste podreže. Skeniranjem otkriva da mu jedno računalo vraća TTL vrijednost 54, a drugo 118. Što napadač može pretpostaviti o tim računalima? Objasnite.

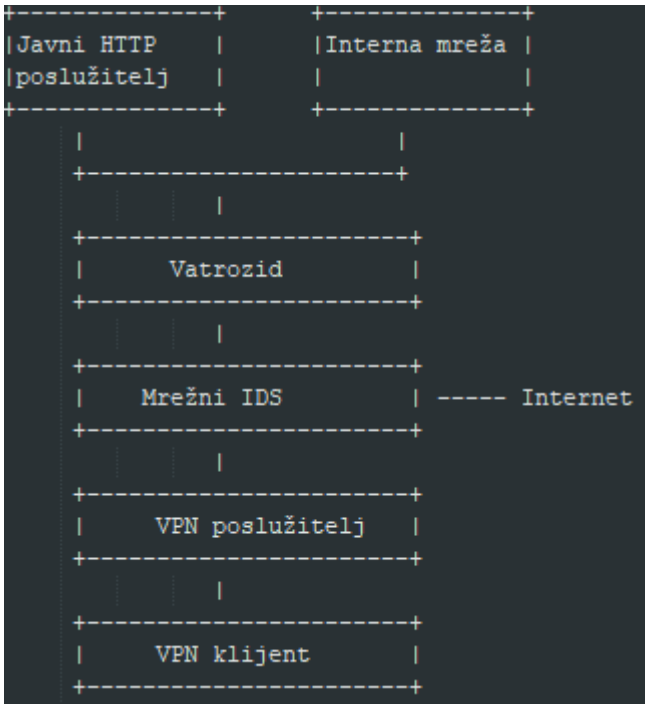
TTL je polje u zaglavlju IP paketa koje se koristi za ograničavanje životnog vijeka paketa. Svaki put kad paket prolazi kroz mrežni usmjerivač, vrijednost TTL-a se smanjuje za jedan. Ako vrijednost TTL-a postane nula, paket se odbacuje. Cilj TTL-a je spriječiti zadržavanje paketa u mreži beskonačno dugo i osigurati da se oštećeni paketi ne šire beskonačno.

Različiti operacijski sustavi mogu koristiti različite početne vrijednosti TTL-a, pa napadač može pretpostaviti o kojem se OS-u radi.

Računalo s TTL vrijednošću 54: Ova niža vrijednost TTL-a sugerira da je paket prošao kroz više usmjerivača ili da je dulje vrijeme putovao mrežom. To može ukazivati da je ovo računalo udaljenije od napadača, na primjer, da se nalazi na drugoj podmreži ili čak izvan lokalne mreže.

Računalo s TTL vrijednošću 118: Ova viša vrijednost TTL-a sugerira da je paket prošao kroz manje usmjerivača ili da je kraće vrijeme putovao mrežom. To može ukazivati da je ovo računalo bliže napadaču, na primjer, da se nalazi na iŠtoj podmreži ili u neposrednoj blizini.

3. (4 boda) Zaposleni ste u poduzeću "Mirkonis d.o.o.". Zadatak vam je postaviti sigurnosnu infrastrukturu koja uključuje vatrozid(e) i mrežni IDS. Poduzeće u sklopu svoje mreže ima javni HTTP poslužitelj. Uz to morate omogućiti VPN vezu s intranetom u poduzeću. Skicirajte i objasnite.



Vatrozid će filtrirati i kontrolirati promet koji prolazi kroz njega prema određenim pravilima i sigurnosnim politikama. Vatrozid se postavlja između vanjske mreže (Internet) i internog mrežnog segmenta kako bi se zaštitio interni poslužitelj i ostali resursi od nepoželjnog prometa i napada. Vatrozid će provjeravati dolazni i odlazni promet prema unaprijed definiranim pravilima. Pravila vatrozida trebaju omogućiti samo promet koji je nužan za javni HTTP poslužitelj, dok se blokira ili ograničava promet koji predstavlja potencijalnu prijetnju.

Mrežni IDS je sustav koji nadzire mrežni promet kako bi otkrio nepravilnosti, ranjivosti i potencijalne napade, tj. analizira promet koji prolazi kroz mrežu i upozoravati na sumnjive ili zlonamjerne aktivnosti. IDS koristi različite tehnike, kao što su detekcija potpisa, detekcija anomalija i heuristike, kako bi identificirao potencijalne prijetnje. Kada se otkrije sumnjiva aktivnost, IDS generira upozorenja koja mogu biti proslijeđena odgovornim osobama za daljnje analize i reakciju.

VPN poslužitelj je postavljen unutar interne mreže poduzeća i omogućuje sigurnu i šifriranu VPN vezu. VPN veza omogućuje udaljenim korisnicima da pristupe internim resursima, kao što su datoteke, aplikacije i poslužitelji, kao da su izravno povezani s internom mrežom poduzeća.

4. (2 boda) Objasnite postupak šifriranja dokumenta hibridnim pristupom.

Hibridni pristup šifriranju dokumenata kombinira prednosti simetričnog i asimetričnog kriptografskog sustava kako bi se osigurala sigurna komunikacija (asimetrično šifriranje omogućuje sigurnu razmjenu simetričnih ključeva, dok se simetrično šifriranje koristi za brže i efikasnije šifriranje samih dokumenata). Postupak hibridnog šifriranja dokumenata:

1. Generiranje ključeva:
    a. Početni korak je generiranje ključeva. U hibridnom pristupu koristit ćemo i simetrični i asimetrični ključ.
    b. Za simetrično šifriranje generira se jedinstveni ključ za šifriranje i dešifriranje. Taj ključ će biti korišten samo za taj određeni dokument.
    c. Za asimetrično šifriranje generira se par ključeva - javni ključ i privatni ključ. Javni ključ će biti dostupan svima, dok će privatni ključ biti poznat samo primatelju.
2. Šifriranje dokumenta:
    a. Prvo, dokument se simetrično šifrira pomoću generiranog simetričnog ključa. Simetrično šifriranje je brže i efikasnije za velike dokumente.
    b. Simetričnim ključem šifriramo sam dokument, pretvarajući ga u nečitljivu šifriranu verziju.
3. Šifriranje simetričnog ključa:
    a. Generirani simetrični ključ se zatim šifrira asimetričnim ključem primatelja (javni ključ). Samo primatelj posjeduje privatni ključ koji je potreban za dešifriranje simetričnog ključa.
    b. Asimetrično šifriranje omogućuje sigurnu distribuciju simetričnog ključa, jer je samo primatelj sposoban dešifrirati taj ključ.
4. Slanje šifriranih podataka:
    a. Šifrirani simetrični ključ i šifrirani dokument se zajedno šalju primatelju.
    b. Šifrirani simetrični ključ može biti pričvršćen na metapodatke šifriranog dokumenta ili prenesen na drugi siguran način.
5. Primanje i dešifriranje:
    a. Kada primatelj dobije šifrirane podatke, koristi svoj privatni ključ za dešifriranje simetričnog ključa.
    b. Dešifrirani simetrični ključ se zatim koristi za dešifriranje samog dokumenta.
    c. Primatelj sada može pristupiti originalnom dokumentu u čitljivom obliku.

5. (2 boda) Čemu sluzi lista opozvanih certifikata (CRL – Certificate Revocation List)? Koja je veza Certificate Authority s CRL?

Lista opozvanih certifikata (CRL - Certificate Revocation List) je popis certifikata s datumom i razlogom koje je Certificate Authority (CA) opozvao prije isteka njihovog valjanog razdoblja (npr. krađa privatnog ključa, promjena identiteta subjekta certifikata ili otkrivanje ranjivosti). Kada aplikacija ili klijent želi provjeriti certifikat, provjerava CRL kako bi vidjela je li certifikat na popisu opozvanih. Ako se certifikat nalazi na CRL-u, smatra se nevažećim i ne bi trebao biti prihvaćen.

6. (3 boda) Objasnite Kaminsky DNS napad.

Napadač šalje DNS zahtjeve za nepostojeće adrese potput aaa.paypal.com gdje onda odmah nakon šalje lažirane odgovore na vlastiti zahtjev. U tim lažiranim zahtjevima napadač mora pogoditi ID zahtjeva, a zahtjevi sadrže lažnu IP adresu za www.paypal.com. Taj proces se ponavlja sa svim mogućim prefiksima aaa, aab, aac.... sve dok napadnuti server ne prihvati lažni odgovor. Tada smo uspjeli otrovati priručnu memoriju servera sa lažnom adresom za www.paypal.com. Sada svi korisnici koji zadraže IP adresu www.paypal.com preko otrovanih DNS servera dobit će IP adresu lažne stranice.

7. (1 bod) Objasnite skraćenicu CIA u kontekstu osnovnih sigurnosnih zahtjeva.

- Povjerljivost (**C**onfidentiality):
    - Povjerljivost se odnosi na zaštitu informacija od neovlaštenog pristupa ili otkrivanja.
    - Cilj je osigurati da samo ovlašteni korisnici ili entiteti imaju pristup osjetljivim informacijama.
    - Kako bi se osigurala povjerljivost, koriste se tehnike poput kriptografije, pristupnih kontrola i sigurnosnih politika.
- Integritet (**I**ntegrity):
    - Integritet se odnosi na održavanje točnosti, cjelovitosti i neporemećenosti informacija tijekom prijenosa, pohrane ili obrade.
    - Cilj je spriječiti neovlaštene promjene, izmjene ili oštećenje podataka.
    - Integritet se osigurava korištenjem metoda poput digitalnih potpisa, heš funkcija i provjere cjelovitosti podataka.
- Raspoloživost (**A**vailability):
    - Raspoloživost se odnosi na osiguravanje pristupa informacijama i resursima kada su korisnicima potrebni.
    - Cilj je spriječiti prekide usluga, ometanja ili nedostupnost informacija.
    - Osigurava se redundancijom, ispravnim upravljanjem resursima, planiranjem oporavka od katastrofe i mrežnim zaštitnim mehanizmima.

8. (1 bod) Što se omogućuje promiskuitetnim načinom rada mrežne kartice?

Promiskuitetni način rada mrežne kartice omogućuje kartici da "uhvati" i analizira sve mrežne pakete koji prolaze kroz mrežno sučelje, čak i one koji nisu namijenjeni specifičnoj kartici čime se omogućuje pregled svog prometa koji prolazi kroz taj segmnet mreže.

9. (2 boda) Objasnite najčešći način stvaranja i distribucije malicioznih aplikacija za operacijski sustav Android.

- Lažne aplikacije u trgovinama aplikacija:
    - Napadači mogu stvoriti lažne aplikacije koje imaju privlačan naziv, ikonu i opis kako bi ih učinili privlačnima korisnicima. Ove lažne aplikacije mogu sadržavati zlonamjerne kodove koji mogu štetiti korisnikovom uređaju ili krađu osobnih podataka. Distribuiraju se putem alternativnih trgovina aplikacija ili čak putem sumnjivih web stranica.

- Zlonamjerne aplikacije u aplikacijama s treće strane:
    - Korisnici mogu preuzeti aplikacije iz izvora koji nisu službene trgovine aplikacija (poput Google Play Storea) i to može predstavljati sigurnosni rizik. Ove aplikacije mogu biti modificirane ili sadržavati skrivene zlonamjerne funkcionalnosti. Ovakve aplikacije mogu se distribuirati putem sumnjivih web stranica, torrenta ili drugih alternativnih izvora.
- Phishing napadi:
    - Napadači mogu koristiti phishing tehnike kako bi prevarili korisnike da preuzmu i instaliraju zlonamjerne aplikacije. To uključuje slanje lažnih e-mailova, SMS poruka ili reklama koje preusmjeravaju korisnike na lažne web stranice ili aplikacije koje se čine legitimnima, ali zapravo sadrže zlonamjerne kodove.
- Malverzi integrirani u legitimne aplikacije:
    - Napadači mogu hakirati legitimne aplikacije i umetnuti zlonamjerne kodove u njih. Kada korisnici preuzmu i instaliraju ovu aplikaciju, zlonamjerni kodovi mogu biti aktivirani, štetiti uređaju ili prikupljati osobne podatke.
- Drive-by preuzimanje:
    - Ova tehnika uključuje iskorištavanje sigurnosnih propusta u web preglednicima ili operacijskom sustavu kako bi se automatski preuzela i instalirala zlonamjerna aplikacija s web stranice koju korisnik posjećuje. To se može dogoditi bez znanja ili pristanka korisnika.

10. (2 boda) Skicirajte datagrame i objasnite razliku između transportnog i tuneliranog načina prijenosa podataka putem protokola IPsec.

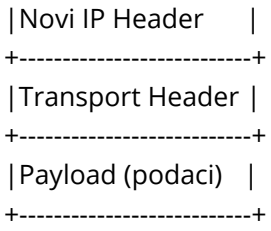
Razlika između transportnog i tuneliranog načina prijenosa podataka putem protokola IPsec je u tome što transportni način štiti samo korisničke podatke dok tunelirani način štiti cijeli IP paket, uključujući IP zaglavlje.

Transportni način koristi se kada samo sami korisnički podaci (payload) trebaju biti zaštićeni i šifrirani:

```
+--------------------------+
|IP Header                 |
+--------------------------+
|IPsec Header              |
+--------------------------+
|Transport Header          |
+--------------------------+
|Payload (podaci)          |
+--------------------------+
```

Tunelirani način koristi se kada cijeli IP paket, uključujući izvornu i odredišnu IP adresu, treba biti zaštićen i šifriran:

```
+--------------------------+
|IP Header                 |
+--------------------------+
|IPsec Header              |
+--------------------------+
```



- IP Header u transportnom načinu: Standardni zaglavlje IP paketa koje sadrži izvornu i odredišnu IP adresu.
- IP Header u tuneliranom načinu: Standardno IP zaglavlje koje sadrži izvornu i odredišnu IP adresu, ali ova adresa predstavlja izvornu i odredišnu IP adresu IPsec gatewaya (tunelnih čvorova).
- IPsec Header: Dodatno zaglavlje koje sadrži IPsec informacije, kao što su sigurnosna pravila (Security Association - SA) i indeks zaštite (Security Parameters Index - SPI).
- Novi IP Header (postoji samo u tuneliranom načinu): Dodatno IP zaglavlje koje se dodaje ispred originalnog IP zaglavlja. Ono sadrži izvornu i odredišnu IP adresu izvornog i odredišnog kraja tunela.
- Transport Header: Zaglavlje transportnog sloja, poput TCP ili UDP zaglavlja.
- Payload: Sami korisnički podaci koji se prenose (npr. aplikacijski podaci).

11. (2 boda) Što je honeypot i čemu sluzi?

Honeypot je sigurnosni mehanizam koji se koristi za privlačenje, praćenje i analizu napada na informacijski sustav. Honeypot se predstavlja kao privlačna meta za napadače, simulirajući ranjivost ili privlačnu metu koju bi napadači željeli ciljati. Glavna svrha honeypota je privući napadače i omogućiti sigurnosnim stručnjacima da prate, analiziraju i uče o napadima, napadačkim tehnikama i ranjivostima.

12. (2 boda) Koja je razlika između Host-based i Network IDS-a (Intrusion Detection System)?

Glavne razlike između HIDS-a i NIDS-a su sljedeće:

Obuhvat: HIDS se fokusira na detekciju intruzija na pojedinom hostu ili poslužitelju, dok se NIDS fokusira na detekciju intruzija na razini mreže, nadzirući promet na mrežnom segmentu.
Izvor informacija: HIDS analizira internu aktivnost sustava (logovi, datoteke, procesi itd.), dok NIDS analizira mrežni promet koji dolazi s različitih izvora.
Detekcija: HIDS se fokusira na otkrivanje nepravilnosti ili sumnjivih aktivnosti na samom hostu, dok NIDS identificira napade i sigurnosne prijetnje koje se događaju na mreži putem analize prometa.
Implementacija: HIDS se instalira na pojedinim sustavima koje treba nadzirati, dok se NIDS postavlja na mrežnom segmentu kako bi nadzirao promet koji prolazi kroz mrežu.

U praksi, često se koristi kombinacija HIDS-a i NIDS-a kako bi se osigurala cjelovita sigurnost. HIDS se koristi za detekciju napada unutar pojedinih sustava, dok NIDS pruža uvid u promet i aktivnosti koje prelaze granice pojedinih sustava.

13. (2 boda) Koji tip napada je slowloris? Kako on funkcionira?

Slowloris je tip napada na mrežne poslužitelje, posebno na HTTP poslužitelje. Funkcionira tako da iskorištava ranjivost u načinu na koji web poslužitelji obrađuju istovremene veze i resurse. Evo kako napad Slowloris funkcionira:

1. Napadač uspostavlja veliki broj nekompletnih HTTP veza prema ciljnom poslužitelju. Ove veze se otvaraju na način da napadač pošalje zahtjev za otvaranjem veze, ali ne šalje potpuni zahtjev zahtjevajući web stranicu.
2. Umjesto da zatvori veze ili ih dovrši, napadač zadržava veze otvorenima i održava minimalnu komunikaciju s poslužiteljem. Napadač periodično šalje minimalne podatke (npr. prazne TCP zaglavlje ili minimalni HTTP zaglavlje) kako bi održavao otvorenu vezu.
3. Cilj napada Slowloris je iskoristiti ograničenja poslužiteljskih resursa. Web poslužitelj ima ograničen broj istovremenih veza koje može podržavati. Stoga, kada se otvori velik broj nekompletnih veza i održava se otvoreno stanje, poslužitelj će iscrpsti svoje resurse, uključujući memorijske i procesorske resurse.
4. Kako napad napreduje i veze ostaju otvorene, poslužitelj će postupno biti preopterećen i neće biti sposoban obraditi nove ispravne zahtjeve od legitimnih korisnika. To dovodi do usporenog odziva poslužitelja i eventualno do prekida usluge za legitimne korisnike.

14. (8 bodova) Prikazana je konfiguracijska datoteka vatrozida.

```
#interface eth0 199.13.24.100/24 (outside)
#interface eth1 10.0.0.1/16 (inside)
#interface lo 127.0.0.1/8 (loopback)

filter
:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -d 127.0.0.0/8 ! -i lo -j DROP
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j DROP
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

-A OUTPUT -p tcp -m tcp --dport 80 -j DROP
-A OUTPUT -p tcp -m tcp --dport 8080 -j DROP
-A OUTPUT -d 12.18.10.20 -p udp -m udp --dport 53 -j DROP
-A OUTPUT -d 12.18.10.40 -p udp -m udp --dport 53 -j DROP
```

Popis servisa i vrata:
tcp/22 ssh
tcp/23 telnet
tcp/25 smtp
tcp/53 dns
udp/53 dns
tcp/80 http
tcp/443 https

(a) (1) Napišite pravilo koje će omogućiti pristup vatrozidu s adrese 99.98.46.10 putem protokola telnet.

-A INPUT -p tcp --dport 23 -s 99.98.46.10 -j ACCEPT

(b) (1) Napišite pravilo koje će korisnicima iz lokalne mreže (tj. iz inside mreže) omogućiti pristup DNS poslužitelju instaliranom na računalu na kojem se nalazi i vatrozid.

-A INPUT -p tcp --dport 53 -i eth1 -s 10.0.0.1/16 -j ACCEPT
-A INPUT -p udp --dport 53 -i eth1 -s 10.0.0.1/16 -j ACCEPT

(c) (2) Je li dozvoljen pristup s vatrozida na mail.google.com korištenjem protokola http kroz SSL/TLS? Pokažite liniju vatrozida kojom se to dopusta/zabranjuje. Objasnite.

Nije dozvoljen zbog pravila koje govori da se svi izlazni http zahtjevi ne propuštaju:
-A OUTPUT -p tcp -m tcp --dport 443 -j DROP.

(d) (1) Napišite pravilo kojim ćete s vatrozida omogućiti pristup poslužitelju elektroničke pošte na adresi 161.53.72.233.

-A OUTPUT -p tcp --dport 25 -d 161.53.72.223 -j ACCEPT

(e) (2) Napišite pravilo kojim ćete zabraniti ulaz spoofanim dolaznim paketima iz vanjske mreže s izvorišnom adresom jednakom adresama iz lokalne mreže (tj. iz inside mreže).

-A FORWARD -i eth0 -s 10.0.0.1/16 -j DROP

(f) (1) Kako će vatrozid odgovoriti na dolazne poruke koje su upućene s adrese 200.18.56.28 na vrata tcp/22. Objasnite zbog kojeg je pravila to tako?

Zbog pravila:
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
Prihvati dolazne poruke protokola SSH.
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
Prihvati dolazne poruke već otvorene veze.
:OUTPUT ACCEPT[0:0]
Prihvati odlazne poruke.
Provoditi će se normalna komunikacija između točaka.