SUI ZI 2016/17

1. (3 boda) Navedena su dva ispisa naredbe netstat na napadnutom posluzitelju. U cemu je razlika? Identificirajte napade koje se izvode u oba ispisa. Ako je napadac u oba slucaja isto racunalo, 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

2. (1 bod) Napadac napada dva nepoznata racunala iz iste podmreze. Skeniranjem otkriva da mu jedno racunalo vraca TTL vrijednost 54, a drugo 118. Sto napadac moze pretpostaviti o tim racunalima? Objasnite.

3. (4 boda) Zaposleni ste u poduzecu “Mirkonis d.o.o.”. Zadatak vam je postaviti sigurnosnu infrastrukturu koja ukljucuje vatrozid(e) i mrezni IDS. Poduzece u sklopu svoje mreze ima javni HTTP posluzitelj. Uz to morate omoguciti VPN vezu s intranetom u poduzecu. Skicirajte i objasnite.

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

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

6. (3 boda) Objasnite Kaminsky DNS napad.

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

8. (1 bod) Sto se omogucuje promiskuitetnim nacinom rada mrezne kartice?

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

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

11. (2 boda) Sto je *honeypot* i cemu sluzi?

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

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

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) Napisite pravilo koje ce omoguciti pristup vatrozidu s adrese 99.98.46.10 putem protokola telnet.
(b) (1) Napisite pravilo koje ce korisnicima iz lokalne mreze (tj. iz *inside* mreze) omoguciti pristup DNS posluzitelju instaliranom na racunalu na kojem se nalazi i vatrozid.
(c) (2) Je li dozvoljen pristup s firewalla na mail.google.com koristenjem protokola http kroz SSL/TLS? Pokazite liniju firewalla kojom se to dopusta/zabranjuje. Objasnite.
(d) (1) Napisite pravilo kojim cete s firewalla omoguciti pristup posluzitelju elektronicke poste na adresi 161.53.72.233.
(e) (2) Napisite pravilo kojim cete zabraniti ulaz *spoofanim* dolaznim paketima iz vanjske mreze s izvorisnom adresom jednakom adresama iz lokalne mreze (tj. iz *inside* mreze).
(f) (1) Kako ce vatrozid odgovoriti na dolazne poruke koje su upucene s adrese 200.18.56.28 na vrata tcp/22. Objasnite zbog kojeg je pravila to tako?