SIGURNOST RAČUNALNIH SUSTAVA, 2020/2021

ZADATCI ZA PRIPREMU ZA ZAVRŠNI ISPIT
14.6.2021.

1. Je li jednostavnije skenirati TCP ili UDP pristupe? Objasnite zašto.

2. Koja je razlika između skeniranja otvorenih pristupa metodama "TCP SYN" i "TCP connect"? Kako biste otkrili da ste žrtva skeniranja tipa "TCP connect".

3. Snimanjem prometa alatom tcpdump, na poslužitelju s adresom 10.0.1.10 primjećujete veliku količinu dolaznih ICMP paketa s raznih adresa. Poslužitelj pritom nije slao nikakve ICMP pakete koji bi prouzrokovali taj promet. O kojem se napadu radi? Koje je vrijednosti napadač trebao unijeti u polja izvorišne (source) i odredišne (destination) adrese u IP zaglavlju početnog ICMP paketa kako bi izveo napad? Sve podmreže u zadatku koriste prefiks duljine 24 bita.

   ispis naredbe "`tcpdump -ni eth0`"

```
10:09:49.062946 IP 10.0.0.1 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.062970 IP 10.0.0.21 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.062972 IP 10.0.0.22 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.062994 IP 10.0.0.30 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
...
10:09:49.062999 IP 10.0.0.29 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.063001 IP 10.0.0.32 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.063013 IP 10.0.0.35 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
10:09:49.063018 IP 10.0.0.20 > 10.0.1.10: ICMP echo reply, id 0, seq 0, length 8
...
```

4. Što je IP zavaravanje (IP spoofing) i kako se može zloupotrijebiti?

5. Što je to DDoS? Navedite neki primjer i objasnite kako radi.

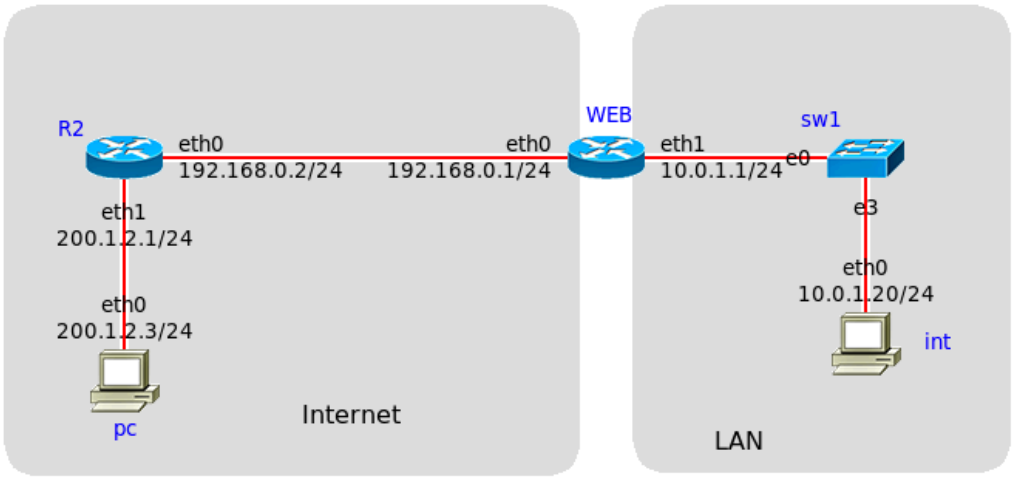
6. Objasnite pojam CA (Certificate Authority) u sklopu arhitekture PKI (Public Key Infrastructure). Koja su mu glavna zaduženja?

7. Objasnite ranjivosti protokola ARP. Opišite moguće napade.

8. Objasnite pojam „demilitarizirane zone“.

9. Koji osnovni sigurnosni zahtjevi se osiguravaju korištenjem protokola SSH? Objasnite kako.

10. Prikazana je konfiguracijska datoteka vatrozida instaliranog na računalu WEB koje se korisiti kao web poslužitelj. Računalo ima dva mrežna sučelja, eth0 koje je spojeno na Internet i eth1 koje je spojeno na lokalnu mrežu.



popis pristupa:
tcp/22 ssh
tcp/23 telnet
tcp/25 smtp
tcp/53 dns
udp/53 dns
tcp/80 http
tcp/443 https

```
#interface eth0 192.168.0.1/24 (outside)
#interface eth1 10.0.1.1/16 (inside)
#interface lo 127.0.0.1/8 (loopback)

*filter
:INPUT DROP [0:0]
:OUTPUT DROP [0:0]
:FORWARD DROP [0:0]

-A INPUT -i lo -j ACCEPT
-A INPUT -d 127.0.0.0/8 !  -i lo -j DROP

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

a. Napišite pravilo koje će svim računalima iz Interneta omogućiti pristup web poslužitelju protokolom https.
b. Napišite pravilo koje će omogućiti pristup vatrozidu protokolom SSH isključivo s računala "int" iz lokalne mreže (LAN).
c. Je li dozvoljen pristup s firewalla na mail.google.com korištenjem protokola http kroz SSL/TLS? Označite redak u konfiguraciji kojim se to dopušta/zabranjuje. Objasnite.

d. Napišite pravilo kojim ćete zabraniti ulaz spoofanim dolaznim paketima iz vanjske mreže s izvorišnom adresom jednakom adresama iz lokalne mreže (tj. iz inside mreže).
e. 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?Prikazana je konfiguracijska datoteka vatrozida instaliranog na računalu WEB koje se korisiti kao web poslužitelj. Računalo ima dva mrežna sučelja, eth0 koje je spojeno na Internet i eth1 koje je spojeno na lokalnu mrežu.

11. Koje sigurnosne zahtjeve ostvarujemo ispravnim korištenjem protokola HTTPS na webu?

12. Što je tipičan cilj napada XSS (cross-site scripting)? Objasnite kako nas u tom smislu štiti politika istog izvorišta (same origin policy)

13. Na koji napad na webu je osjetljiv sljedeći kod? Što bi trebali napraviti kako bi navedeni kod bio sigurniji?

```
if( isset( $_REQUEST[ 'Submit' ] ) ) {
    $id = $_REQUEST[ 'id' ];

    $query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' .
((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) :
(($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );
    while( $row = mysqli_fetch_assoc( $result ) ) {
        $first = $row["first_name"];
        $last  = $row["last_name"];
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
    }
    mysqli_close($GLOBALS["___mysqli_ston"]);
}
```

14. Objasnite zašto ste u 3. laboratorijskoj vježbi mogli doći do izvorne lozinke korisnika *pablo*!