SRS ZI 21/22

4. Objasnite napad tipa „UDP based amplification“.

Napadač šalje UDP paket sa lažiranom izvorišnom adresom (adresom žrtve). Paket se šalje na servis/računalo koje će odgovoriti na UDP paket sa više informacija/podataka nego što je poslano. Time napadač pojačava količinu podataka kojom opterećuje žrtvu.

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

DDoS - Distributed Denial of Service

Vrsta napada u kojem više računala (obično zaraženih) generira određenu količinu prometa prema žrtvi i time preopterećuje žrtvu.

Primjer: Žrtva web poslužitelj. Svako računalo pod kontrolom napadača se spaja na web poslužitelj, šalje spore zahtjeve i time ga preopterećuje.

6. Navedite osnovne podatke koje sadrži digitalni certifikat.

Informacije o korisniku (naziv, institucija, država), javni ključ, rok trajanja certifikata, status(povučen ili aktivan), digitalni potpis institucije koja jamci za certifikat (CA).

7. Netko je na javno dostupnoj stranici http://mrepro.tel.fer.hr/ objavio digitalni certifikat FER-ove stranice https://www.fer.unizg.hr/. Predstavlja li to neki sigurnosti rizik? (zašto)

Javno objavljivanje nečijeg (tuđeg) certifikata predstavlja sigurnosni rizik. Tada se efektivno druga stranica "pretvara" (impersonating) da je Ferova stranica. Ovo može navesti žrtve da povjeruju napadačevoj stranici.

Alternativno (ako nije objavljen i privatni ključ), onda nema izravnog sigurnosnog rizika.

8. Kao mrežni administrator dobili ste zadatak na siguran način povezati mrežu udaljene poslovnice s mrežom u sjedištu tvrtke.

Koju tehnologiju ćete preporučiti? VPN (point to point)

Navedite neki protokol ili aplikaciju koja se može za to koristiti: IPSec, OpenVPN, TLS,...

9. Održavate sustav na kojem je instaliran web poslužitelj na TCP pristupu 80. Vaš šef je negdje na internetu pročitao da je nesigurno pristupati mrežnim adresama oblika „http://www.nesto.com“. Što ćete napraviti?

Prilagoditi arhitekturu da umjesto HTTP podržava HTTPS. Pribaviti digitalni certifikat. Dopustiti da server komunicira na portu 443.

10. Spajate se na FER web putem preglednika weba i uočavate „lokot“ kod imena fer.unizg.hr. Što vam to jamči?

a) Cjelovitost
b) Povjerljivost
c) Autentifikaciju klijenta
d) Autentifikaciju poslužitelja
e) Raspoloživost
f) Neporecivost
g) Sve navedeno
h) Ostalo (navedite):

11. Koje podatke osigurava DNSSec? Možemo li umjesto DNSSec koristiti „DNS over HTTPS“?

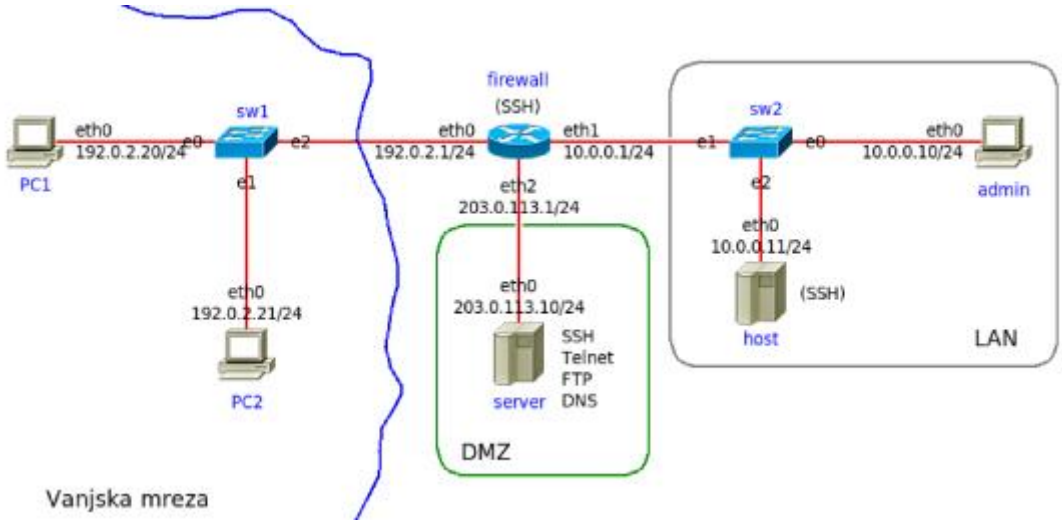
DNSSec osigurava kriptografski dokaz ispravnosti primljenih podataka. Ne možemo, DNS over HTTPS će osigurati povjerljivost podataka (tajnost).

Koriste se za totalno različite stvari!!!! HTTPS sam po sebi ne sadrži kriptografski dokaz ispravnosti. Ova dva postupka se mogu kombinirati.

12. Navedite primjene korištenja protokola SSH (ne treba navoditi konkretne naredbe) . Ukratko: …za što služi SSH?

SSH (Secure Shell) prvenstveno sluzi za ostvarivanje sigurnog udaljenog pristupa preko mreže. Primjerice, može se koristiti za pristup i izvršavanje naredbi na udaljenom web serveru.

13. Na slici 2 je prikazana topologija mreže iz 4. lab vježbe. Snimamo TCP promet na sučelju računala PC1. Relevantni dio snimljenog prometa prikazan je u nastavku.



192.0.2.20:4016	>	203.0.113.10:22	:	Flags [S], seq 0, win 8192, length 0
203.0.113.10:22	>	192.0.2.20:4016	:	Flags [S.], seq 1451154, ack 1, win 64240, len 0
192.0.2.20:4016	>	203.0.113.10:22	:	Flags [R], seq 1, win 0, length 0
192.0.2.20:5623	>	203.0.113.10:22	:	Flags [R.], seq 0, ack 0, win 8192, length 0
192.0.2.20:11194	>	203.0.113.10:53	:	Flags [S], seq 0, win 8192, length 0
203.0.113.10:53	>	192.0.2.20:11194:		Flags [S.], seq 2363391, ack 1, win 64240, len 0
192.0.2.20:11194	>	203.0.113.10:53	:	Flags [R], seq 1, win 0, length 0
192.0.2.20:5757	>	203.0.113.10:53	:	Flags [R.], seq 0, ack 0, win 8192, length 0
192.0.2.20:47915	>	203.0.113.10:23	:	Flags [S], seq 0, win 8192, length 0
192.0.2.20:55093	>	203.0.113.10:80	:	Flags [S], seq 0, win 8192, length 0
192.0.2.20:42209	>	203.0.113.10:23	:	Flags [S], seq 0, win 8192, length 0
192.0.2.20:34124	>	203.0.113.10:80	:	Flags [S], seq 0, win 8192, length 0

Ako znamo da je korisnik na računalu PC1 pozvao naredbu „nmap“. možemo zaključiti da je:

- skenirao računalo s IP adresom 203.0.133.10
- na njemu je provjeravao dostupnost „portova“: 22, 53, 23, 80
- -te je za njih otkrio slijedeća stanja („otvoren/zatvoren“): otvoreni portovi(22,53), zatvoreni portovi(23,80) Portovi 22 i 53 su otvoreni jer se uspostavi TCP veza (handshake), uocite S (syn) i S. (syn + ack) te se veza odmah zatvori da se nastavi skeniranje(R u R.). Portovi 23 i 80 su zatvoreni na firewallu jer ne dolazi nikakav odgovor (zadnje 4 linije).

14. Na slici 2 je prikazana topologija mreže iz 4. lab vježbe. Početna (nepotpuna) konfiguracija vatrozida na čvoru „firewall“ ispisana je u nastavku. Na početku su obrisana sva pravila i poliatika je postavljena na „DROP“

#! /bin/sh

IPT=/sbin/iptables

$IPT -A INPUT -m state –state ESTABLISHED, RELATED -j ACCEPT
$IPT -A OUTPUT -m state --state ESTABLISHED, RELATED -j ACCEPT

$IPT -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT

$IPT -A INPUT -m eth0 -s 127.0.0.0/8 -j DROP
$IPT -A FORWARD -m eth0 -s 127.0.0.0/8 -j DROP

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

a) Napišite pravila koje će omogućiti pristup web poslužitelju na računalu „server“ s bilo kojeg računala, korištenjem protokola https.
   -A FORWARD -p tcp -d 203.0.113.10 –dport 443 -j ACCEPT
b) Napišite pravilo koje će omogućiti konfiguriranje vatrozida na čvoru „firewall“ protokolom SSH isključivo s računala „admin“.
   -A INPUT -p TCP -i eth1 -s 10.0.0.10 -d 10.0.0.1 --dport 22 -j ACCEPT
c) Napišite pravilo kojim ćete zabraniti ulaz „spoofanim“ dolaznim paketima iz vanjske mreže s izvorišnom adresom jednakom lokalnim adresama.
   -A FORWARD -i eth0 -s 10.0.0.0/24 -j DROP
d) Napišite pravilo kojim ćete omogućiti „ping“ računala u vanjskoj mreži s računala „admin“.
   -A FORWARD -p icmp -s 10.0.0.10 -d 192.0.2.0/24 --icmp-type 8 -j ACCEPT
e) Možemo li iptables pravilima definiranim na čvoru „firewall“ ograničiti pristup čvoru „host“ s računala iz lokalne mreže (LAN)? DA/NE
   NE – Ne možemo zabraniti pristup hostu preko firewalla jer nisu spojeni preko njega već preko switcha. Ako želimo onemogućiti tada moramo onemogućiti na hostu ili na switchu.

15. Objasnite razliku između Newtwork IDS i Host-based IDS sustava.
    Mrežni IDS - uzima podatke s mreže
    Računalni IDS - uzima podatke s računala

16. Politika istog izvorišta (same origin policy) na webu:

a) Govori da se kolačićima može pristupiti jedino putem protokola HTTP te tako onemogućiti krađu kolačića iz preglednika korištenjem skripti
b) onemogućuje krađu kolačića iz preglednika zato što skripte niti jedne stranice (izvorišta) ne smiju pristupiti kolačićima
c) djelomično onemogućuje krađu kolačića iz preglednika zato što skripte samo jedne stranice (izvorišta) smiju pristupiti kolačićima
d) definira politiku preglednika vezanu uz kolačiće za praćenje (tzv. tracking cookie)

17. Na koji napad na webu je osjetljiv slijedeći kod?

„brojracuna“ je vrijednost iz zahtjeva HTTP GET

```
if ( array_key_exists ( "name", $_GET ) &&  $_GET [ 'brojracuna' ]  != NULL ) {

        echo 'Your account number is ' . $_GET[ 'brojracuna' ] ;

}
```

Kod je osjetljiv na napad XSS napad (cross site scripting)

Kako biste mogli zaštiti ovaj kod protiv tog napada?

Napadač u poveznici kao parametar brojracuna šalje JS kod. Sanitizacija koda (uklanjanje <script> i ostalih tagova, tretiranje unosa kao jedan string(bez mogućnosti izvođenja, HTTP/HTTPS only cookie, uključiti same origin policy za cookie).

18. Provalili ste u bazu podataka neke web aplikacije i tamo našli sažetak lozinke administratora i pripadajući SALT. Možete li doći do izvorne lozinke?

a) ne mogu jer je funkcija sažetka ireverzibilna

b) ne mogu jer se koristi i vrijednost SALT

c) mogu ako imam ključ za dešifriranje kojim je sažetak i napravljen

d) mogu ako koristim napad rječnikom i ako je lozinka u rječniku

e) mogu ako uspijem pogoditi odgovarajuću kombinaciju lozinke i SALTa

19. Razmotrite kod u nastaku.

$username = $_POST ['uname'];

$pass = $_POST [' password'];

$sql = "SELECT * FROM user_table WHERE username = ' ".$username. " ' AND userpwd = ' ".$pass" '; ";

//izvedi upis i pokaži sve (*) podatke korisniku

Na što je ranjiv ovaj kod? Navedite primjer! ➔ Kod je ranjiv na SQL injection. Primjerice dodati tautologiju (username AND password OR true) tj dodati [foo' OR 1 = 1 '].

Što biste trebali dodati kako bi ovaj kod bio siguran? Treba dodati sanitizaciju/verifikaciju korisničkog unosa kako bi se eliminirale potencijalne SQL injekcije.

Želite osigurati da lozinka ima dovoljan broj znakova. Gdje biste vršili tu provjeru? NA KLIJENTU – NA POSLUŽITELJU.

Provjera NA POSLUZITELJU (sve sto je na klijentu napadac/korisnik moze potencijalno zaobici).

20. Razvijate web aplikaciju i želite otežati pogađanje identifikatora sjednice. Koji od sljedećih izraza biste koristili?

a) $session_id = $_SESSION [' last_session_id']++;

b) $session_id = md5 (mt_rand() . time());

c) $session_id = md5 ($_SESSION ['last_session_id']++);

d) $session_id = time();