

1. Bilo je drag and drop povezivanje iot ranjivosti s objasnjenima

Tipa 3 recenice u stilu RANJIVOST OVAKVA se moze ublaziti s _____

12 Insecure Network Services – Ublazavanje (Skeniranje portova kako bi se utvrdilo što je sve pokrenuto (nmap), Provjera ranjivosti otvorenih servisa, Posebno paziti na UPnP portove)

14 Lack of Secure Update Mechanism – Ublazavanje (Može li se software/firmware uređaja uopće ažurirati?)

15 Use of Insecure or Outdated Components – Ublazavanje (pobrojati što se sve koristi, je li sve ažurirano)

16 Insufficient Privacy Protection – Ublazavanje (Kakve sve podatke uređaj IoT skuplja, Što se radi s tim podacima, Jesu li anonimizirani, Domena GDPR-a)

17 Insecure Data Transfer and Storage – Ublazavanje (Analiza prometa kako bi se utvrdilo je li dio ili sav promet šifriran, Ako se koristi TLS provjeriti da se koristi ispravno)

18 Lack of Device Management – Problem (zamjena/isključivanje uređaja)

19 Insecure Default Settings – Ublazavanje (Ako već proizvođač ne forsira jake lozinke, mogu li ih sam forsirati na administratorskom sučelju?)

110 Lack of Physical Hardening – Ublazavanje (Mogu li jednostavno "otvoriti" uređaj, Mogu li se spojiti na ulaze, Mogu li programski onemogućiti lokalno spajanje, pohranjeni podaci šifrirani)

2. Identican koncept identicno pitanje vezano uz mobilne

3. Bilo je zadano

Blue jacking (slanje poruka na uređaj kroz BT, reklame ovisne o lokaciji, spam)

Blue sniping (prosirenje napada vecom antenom)

Blue snarfing (neovlasten pristup BTu, preuzimanje slika, kontakata, kalendara i poruka) ili kako god se zove) i morao si izabrat koje objasnjenje pase uz koji pojam

4. Bila je nacrtana mreza i ti moras napisat iptables pravila za firewall. Takvih je bilo tipa 6 i budu u stilu "pc21 smije napraviti nespojnu konekciju sa server 1"

Onda imas lijepo svaki komadic pravila za izabrat (npr svaki je na pocetku imao oces -A ili -J ili tak nes pa izaberes A) onda drugi komadic biras FORWARD/input/output, treci komadic biras izmedu -s/-src/PRAZNO cetvrti su ponudene sve adrese itd itd. Ponudeni protokoli su bili samo najosnovniju protokoli (80 za http i 22 za ssh i jos dva random)

5. Pitanje s Mla:

Bila je nacrtana mreza neka osnovna (dva kompa pa prema switchu pa prema routeru pa prema nekakvom serveru a la internet) i velikim slovima napisano 80 (broj protokola s kojim se prica) i onda je bilo pitanje tipa ana se dopka s ovom iz iste mreze i malo je zabrinuta za sigurnost.

Koji protokol koristi? Ponudeni tipa ssh/http/https/smtp

Poruke se razmjenjuju kriptografskom zastitom

6. Odaberite neistinitu tvrdnju:

Mogu li se hakirati pc-evi u NATu (T/N) : **T**

7. Nadopuni:

Sustav koji nadzire mrežu, sustav za detekciju i prevenciju napada i jos nesto.

Sigtran koristi **[Stream]** Control **[Transmission]** Protocol.

8. Bilo je koja od ponuđenih je puni naziv za protokol TMSI (**temporary mobile subscriber identities**)

9. **MIME (T/N)** – šifrira s kraja na kraj (**N, to radi S/MIME**)

10. Povezi pojmove:

clear-signed: **sazeto i sifriran sažetak**

signed: **sazeto i sifrirana i poruka i sažetak**

envelope: **opcento sifrirano**

11. Bilo je od cega je kratica BYOD (**bring your own device**)

12. Bilo je pitanje sto znaci kontejnerizacija za mobilne. Dva odgovora su bila jako glupa (tipa stavit mob u kutiju kad dodes na posao), **virtualna particija za na pokretnom uredaju**,
dio mreze odvojen za zaposlenike kako bi se oni osigurali

13. Sjetila sam se jednog s MI: kako funkcionira TCP connect (**uspostavlja vezu u potpunosti i odmah ju prekida**) u odnosu na tcp 3way handshake (**uspostavlja vezu**)

14. Zanci bio je Branko Koji je ugradio SSL server za koji je samo on znao. Povremeno s njega citao obavijesti i loggove u kojima pišu IP adrese posjecenih ljudi na taj server (iako nitko ne zna da on postoji). Pitanje je bilo što je taj lik htio postići tim uređajem? I to je bilo kao nadopuna rečenice i savršeno je odgovarala riječ **HONEYPOT (resurs koji mora biti iskoristen na neki nacin)**

15. Bila je neka slika maila kad ti nektko iz neke random drzave ili kraljevine posalje mail da si ti njegov tranzitivni rodjak i da treba tvoje podatke kako bi prenio neku ostavstvinu? (**Phising**)