# MI – 2012/2013

1. Što je cjelovitost i kako bi ju ostvarili u mreži?

Cilj IS: zaštititi podatke od neovlaštenog brisanja, mijenjanja ili bilo kakve manipulacije bez prethodne autorizacije, načela uspostave kontrole cjelovitosti su: - dodjela samo nužnih prava pristupa

* odvajanje dužnosti
* rotacija dužnosti

1. dobio si usb za koji znaš da ima neki malware ali ne znaš jel virus, crv ili trojan. Što smiješ a što ne smiješ napravit?

Ako je crv ne smijes ni ustekati usb, jer ce odma zaraziti i dalje se prosiriti. Ako je virus ili trojan smijes ustekati, ali da bi zarazili moras pokrenuti program ili datoteku di se nalaze. Virus se onda moze dalje siriti sam, dok se trojan ne siri.

1. Koja je razlika između skeniranja portova sa TCP SYN i napada TCP SYN flood?

Skeniranje samo provjerava koja su TCP vrata otvorena, a TCP flood radi DoS. Ako je port otvoren, tcp uspije napravit connect nakon three way handshakea, a tcp syn napad pošalje gro syn requestova, server vrati istu hrpu ack-ova, ali napadač ne uspostavi niti jedan connect.

1. Koja je razlika između koncentratora i komutatora u smislu prisluškivanja prometa? Što se može izvesti da bi se prisluškivanje odvijalo jednako i na komutatoru i na koncentratoru?

Komutator ili switch radi na podatkovnom sloju, a sniffanje se odvija pomoću MAC floodinga. Hub je na fizičkom sloju i bolje ga je koristiti za sniffanje .

1. Kod  
   int main (int argc, \*\*char argv)  
   {  
   s=char[256]  
   ....  
   strcat(s, argv[1]);  
   system(s);  
   ...  
   }  
   Koji napadi bi se mogli izvesti s obzirom na kod? Kako bi spriječio te napade?

Buffer overflow. Sprijecio bi ga tako da prije inicijalizacije var s provjeravam duljinu ulaznog niza, da slucajno ne premasi duljinu od 256.

1. Ispis pravila za vatrozid (ono tipa from any to any i te šeme) i pitanja o nekim pravilima šta znače?

WebPoslužitelj ima otvorenu mogućnost slanja TCP paketa prema vanjskoj mreži. Kako vatrozid zna da je TCP paket koji dođe izvana onaj odgovor kojeg WebPoslužitelj čeka?

1. Kako bi korištenjem simetričnog i asimetričnog algoritma kriptirao poruku?

Pomoću hibridnog kriptiranja. Prvo bi poruku hashirali, te ju potpisali svojim privatnim ključem. Tada digitalni potpis zajedno s porukom zipamo, te kriptiramo zip pomocu simetricnog kljuca. Tada taj simetricni kljuc kriptiramo pomocu primateljovog javnog kljuca i sve skupa posaljemo. Primatelj prvo odkriptira svojim privatnim kljucem, dobije simetricni kljuc, tada njime odkriptira zip, odzipa dobiveno, racuna hash poruke i usporeduje ga s o onim sto ce odkriptirati svojim javnim kljucem da se provjeri autentifikacija.

1. Koja je razlika u šifriranju tokova i blokova? Ako se promijeni jedan bit u šifriranom što se dogodi kod tokova a što kod blokova?

S tokovima podataka lakše barataju ljudi, a s blokovima računala. Tok podataka: One-time pad. Blokovi podataka: AES (Advanced Encryption Standard).

1. Opiši Kaminsky napad? Može li se on spriječiti DNSSEC-om? Objasni.

Znači, kada ti pošalješ normalan zahtjev za stranicu www.google.com, to ide na DNS server, ono prolazi par servera, domena, poddomena bla bla dok ne dođe do odgovora. To inače potraje, i rezultat www.google.com neka.ip.adresa.ovdje se slaže i onaj cache. E sad kod kaminsky napada ono što ti radiš je uzmeš za željenu domenu nešto oblike nešto.google.com (dakle BILO što ŠTO si skoro siguran da ne postoji), može i 123534566574e456.google.com i tražiš od toga IP. Pošto znaš da toga nema, znaš i sigurno da ne postoji u cache tablici i da će sigurno tu trebati nešto preko DNS-a. E sad tvoja ideja je da pogodiš neki ID koji cache tablica šalje u DNS i od kojeg očekuje odgovor za tvoj DNS zahtjel i glumiš DNS tako da šalješ odgovor cacheu u obliku tvoja.lažna.adresa(123534566574e456.google.com) + pravi.ip.od.googlea (evo samo ovaj dio nisam siguran jel ovdje ide pravi ip od google, al mislim da bi trebalo). I znači ako dovoljno brzo ti uspiješ to odraditi, prije nego DNS sve izvrti (znači pogoditi pravi ID, ima ih jako malo, mislim 65535 or smth like that) i poslati odgovor, tvoj odgovor će se primiti kao legitiman i svi koji posjete google.com će ići na tvoj lažni ip. DNS odgovor koji dođe kasnije će odbaciti jer je to tak skureno napravljeno.

E sad, DNSSEC je napravljen primarno zbog problema. Dakle, DNSSEC dopušta web stranicama da ovjere (potpišu) svoje domene + ip parove kriptografijom i potpisima, ali to vrijedi samo u slučaju da je ROOT potpisan. Još veća snaga se postiže potpisivanjem i ostalih poddomena tipa .com, kao i još niže i hijerarhiji..

1. U kompjuteru se lozinke korisnika pohranjuju u bazu kao sažetak lozinke (hash). Kako bi spriječio napad riječnikom u offline modu?

Pomoću SALT-a, odnosno lozinke bi se hashirale tako da se na početak ili kraj dodaj neki radnom dodatak, pa se sve zajedno hashira. To omogućava da dvije iste lozinke daju različite hasheve.

1. Osnivamo tvrtku i imamo http, https i ssh poslužitelje. Želimo da ti poslužitelji budu raspoloživi vanjskoj mreži, ali da unutarnja mreža u isto vrijeme bude zaštićena. Skicirajte kako bi to ostvarili i objasnite.

Privatna mreza,firewall,demilitarizirana zona,firewall,javna mreza.

# ZI 2012-2013

1. Radiš u sigurnosnoj službi FER-a, dobiješ mail neki divlji [ministarstvo, povrat poreza, skini obrazac, usmjeri preglednik na tu i tu stranicu, bla bla], što trebaš napravit? (2)

Ono dobiješ mail od porezne, OBRIŠEŠ. Porezna ne šalje mailove, šalje poštom povrat poreza. Treba upozoriti i obavijestiti zajednicu o problemu, te blokirati dolazne mailove s te domene, ili trajno ukoliko je nepoznata domena, ili privremeno i obavijestiti IT ljude zaduzene za tu domenu da poprave di nevalja.

1. Honeypot? (3)

* uređaj koji predstavlja žrtvu napada
* svaka interakcija s njima je sumnjiva
* prevencija:
  + usporavaju ili zaustavljaju napad
  + zbunjuju napadača
* otkrivanje:
  + sav promet usmjeren njima po definiciji je sumnjiv
* reakcija:
  + lako se ustanovi što je bio cilj napada jer se bez posljedica sustav može analizirati
* nedostaci:
  + prate napad usmjeren samo na njih
  + napadači ih mogu preuzeti

1. Skeniranje UDP/TCP portova – razlika? (3)

Ako je port otvoren, tcp uspije napravit connect nakon three way handshakea, a UDP nije konekcijski protokol pa nema uspostave veze. On samo šalje i ne ceka na povratnu informaciju od primatelja ( znaci nema handeshake). TCP je zbog toga bolji spoofinga. (Ovdje jos fali, ne da mi se sad opisivat komplet jedno i drugo ;) )

1. Kako token daje dodatnu sigurnost?(2)

A session token is a unique identifier, usually in the form of a hash generated by a hash function that is generated and sent from a server to a client to identify the current interaction session. The client usually stores and sends the token as an HTTP cookie and/or sends it as a parameter in GET or POST queries. The reason to use session tokens is that the client only has to handle the identifier (a small piece of data which is otherwise meaningless and thus presents no security risk) - all session data is stored on the server (usually in a database, to which the client does not have direct access) linked to that identifier. There are many drawbacks of session id and it may not be enough to fulfill some developer requirements.[vague] Many developers use other logic to identify the session.

1. Jel malware na mobitelima opasniji nego na računalima i zašto? (2)

* Na telefonima je lakše doći do novca preko operatora (npr. premium SMS), uz “standardne” prevare kreditnim karticama
* pristup lokaciji korisnika
* percepcija telefona nije ista kao i percepcija laptopa ili stolnog računala
* prevare se “ne očekuju” jer korisnici nisu na njih navikli
* lakši pristup privatnim mrežama (WLAN) - napadi iznutra

1. Imaš malware i prijatelji s fejsbuka ne pričaju s tobom, šta je malware skrivio? (2)

Vjerojatno je tvojim prijateljima sam slao poruke s linkovima na zloćuden stranice i spam poruke, pa sad tvoji prijatelji kad im ti stvarno nesto posaljes ne znaju da li imaju posla s tobom stvarno, ili s malwerom.

1. Kako bi izveo DoS napad na HTTP poslužitelj? (2)

TCP SYN Flood. Samo bi zasipao žrtvu s puno TCP paketa, no ne bi odradio three way handshake do kraja, nego bi ostavio da na svakim vratima istekne timestamp za prekid konekcije jer nema odgovora

1. Izgubio si svoji privatni kljuc, dobio si mail od sebe zakljucan javnim - mozes li citati, sto uciniti da ponovno imas sigurnu komunikaciju?(3)

Ne mozemo procitati,moramo zatraziti novi par kljuceva i napravis backup kljuceva za ubuduce.

1. Radis u firmi, zelis imati javni HTTP preglednik, firewall za svoju mrezu, VPN vezu za ljude koji su kod kuce i zele se spojiti na mrezu. nacrtaj i objasni? (4)

Javna mreža - firewall - IDS - HTTP poslužitelj - firewall - lokalna mreža. Treba još još jedan ids iza http poslužitelja i staviti posebnu pristupnu točku za vpn iza koje isto staviti IDS.

1. Popis firewall pravila, objasni 3 odredena (loopback, DNS, promet koji dolazi iz lokalne mreze), sto znaci setup u tim pravilima? (4)

Setup je kod TCP protokola da može slati i primati one zahtjeve, SYN, SYN/ACK i to... Bez toga bi mi mogli poslati SYN, ali ne bismo mogli dobiti nazad SYN/ACK. E, onda setup to dinamički ostvari da možemo sve.

1. Sumnjas u napad na posluzitelj, kako detektirati izmjene na sistemskim/obicnim datotekama, koju vrstu programa koristiti, daj primjer? (2)

Treba nam IDS koji od nasih nekompromitiranih datoteka sprema hash, pa svaki put kad rabimo ili otvaramo datoteku ponovo racunamo hash i usporedimo sa zadnjom spremljenom vrijednosti hasha. Ako je ista nista nije mjenjano bez nas, ako je onda su nas sjebali. Alat Tripware se korisit tako.

1. Zašto proizvođači softwara uz sofware datoteke stavljaju i hash datoteke uz programe za skinuti (exe, zip, patch, tar) ? (2)

Zbog toga da se moze provjeriti integritet tog softwarea na korisnickoj strani. Ako su ubaceni neki virusi ili nesto ne valja, onda hash nece biti isti.

1. Dan kod (sql), web aplikacija je podlozna kojem napadu (ili napadima), daj primjer; dana tablica (username i pass(koji je hash)), mozes li dobiti pass u plaintextu? (4)

SQL injection. Primjer treba na mjesto username i na mjesto password u browseru upisati ` OR 1=1 --. Password se ne može izravno dobiti u plaintextu, no uz pomoć dictionary attacka moze se porabati otkriti ako nemaju SALT , ako imaju SALT onda je nemoguce. Ako se ima dovoljno vremena moze se probati brute force, no ugalvnom tesko je, skoro nemoguce dobiti lozinke u plain textu.