SAŽETAK NAJBITNIJIH POJMOVA IZ SKRIPTE

IP spoofing – ubacivanje IP datagrama u mrežu (sigurnosna prijetnja ubacivanja lažne informacije); slanje IP datagrama s lažnom adresom pošiljatelja

Defacement – promjena izgleda (npr. web-stranice)

Malware – zajednički naziv za softver koji se infiltira ili oštećuje računalni sustav; spyware, adware, trojanci, crvi, virusi

Virusi: sami se umnažaju ali se ne pokreću sami; djeluju samo na jedno računalo
Crvi: sami se umnažaju i sami se pokreću; potpuno blokiraju ostali promet i djeluju na cjelokupnu mrežu

Mass mailing crvi – šire se u privitku ele. Poruka i poslatu će se na sve adrese koje pronađu na adresaru na infinicranom računalu; često koriste ugrađeni vlastiti poslužitelje ele.pošte

Trojanci: maskirani kao legitimni programi ili je njihov kod ubačen u neki legetitman program; ne mogu se izvršavati sami pa njihov uspjeh najviše ovisi o društvenom inžinjeringu

Spyware: špijuniranje rada korisnika i slanje tih podataka napadaču

Backdoor – omogućuje spajanje napadača na napadnuto računalo (izbjegavanjem autentfikacije)

Dialer – program koji pomoću modema uspostavlja dialup pristup internetu; računalo na kojem je pokrenut dialer spaja se na internet preko skupih telefonskih brojeva (ako je već ostvarena veza na lokalni ISP, dialer će je prekinuti i ponovno se spojiti na „svoj“ ISP); mogu i otvarati stranice, mijenjati homepage, kreirati bookmarke

Hoax – poruke neistinitog sadržaja; zavaravanje korisnika, uništavanje ugleda tvrtke

Kako radi antivirusni – fingerprinting??

1. Način: svaki virus ima određeni znakovni kod pa ga po tome može detektirati i nakon toga ili briše virus iz datoteke ili stavlja datoteku u karantenu ili briše inficiranu datoteku; 2. način: nadzor ponašanja svih programa; problem je što se sumnjivim akcijama proglašavaju i one legitimne

Tripwire – otkrivanje promijenjenih datoteka (računa se fingerprint svake datoteke (hash, checksum) i pohranjuje u bazu a pri provjeri se postupak ponavlja i uspoređuje s onim u bazi)

DoS – uskraćivanje usluge, napad na raspoloživost sustava

Vrste:

Smurf – slanje echo requesta i vraćanje velikog broja echo replya što opterećuje server koji onda ne može prepoznati stvarni promet

Buffer overflow – na mrežnu adresu se šalje više prometa nego što je neki defaultni, npr. slanje prevlikog broja ICMP paketa (ping of death)

Pinf of Death – kreira se i pošalje IP paket veći od maksimalno dozvoljene veličine pa dolazi do buffer overflow-a

SYN – napadač šalje zahtjeve za spajanje ali ne odgovara na povratne poruke koje šalje poslužitelj

Teardrop – napad na fragmentaciju; napadač IP-u dostavlja zbunjujuće podatke za sastavljanje fragmenata pa paketi ne mogu biti sastavljeni već samo prima fragente i dolazi do buffer overflowa

Firewall se bavi sprečavanjem napda a IDS detekcijom napada

IDS pokriva i napade koji dolaze iz unut mreže; otkrivanje anomalija (ponašanje sustava koje odudara od normalnog), prepoznavanje uzoraka (npr. nepropisno započinjanje FTP sesije)

HIDS – sakuplja i analzira podatke s računala na kojem su instalirani, provjerava cjelovitost datoteka i otkriva napade na aplikacijskom sloju

NIDS – analizira sve podatke koji putuju mrežom; promatraju pakete i uspoređuju ih s poznatim uzorcima; mrežna kartica je postavljena u promisk. način rada što omogućuje primanje svih paketa sa svim MAC adresama

Cookie – podaci koje web-poslužitelj prosljeđuje pregledniku kad korisnik pristupi sjedištu, a zatim ih preglednik spremi na disk; služi za identificiranje računala prilikom ponovnog slanja zahtjeva za dohvat nekog resursa na web-poslužitelju

https: znači da se komunikacija između preglednika i web-poslužitelja šifrira, tj da se između aplikacijskog protokola HTTp i transp. Protokola TCP koristi i SSL koji šifrira komunikaciju iznad transportnog sloja

MAC flooding – switch održava tablicu MAC adresa i portova; prepuni tablicu i prelazi u hub način rada; hub je bolje koristiti za sniffanje je promet koji dobije šalje na sve portove

Skeniranje UDP-a: ako je port zatvoren ugl se dobiju poruke ICMP port unreachable; spora o teška tehnika; retransmisija

Imate ovu super stranicu, meni je puno lakše iz tog neke stvari naučit, prvenstveno za usmjeni: http://www.cert.hr/dokumenti?field_doc_cat_value=All&body=same i upišete temu, otvori vam dio, a ispod je i cijeli pdf.

ZI 2014./2015.

1. netstat dana su 2 opisa, koje su razlike, koji je napad u pitanju, napadi prepoznati ih i prepoznati IP adresu napadača, mislim da je ovako a) TCP flooding jer je sve na portu 80, b) TCP skeniranje jer prolazi kroz portove 22,...,80,81,82
2. skicirati i objasniti transportni i tunelirani način rada IPsec-a
3. ransomware i 3 načina kako se može dobiti
4. u 2.labosu smo koristili john-a. kakav je to bio napad i objasnite
5. Opiši DNS spoofing napad. Koji je primjer takvog napada?
6. nacrtano je: DMZ, zaštićena mreža, lokalna mreža a imamo: bazu podataka, web server, web aplikaciju i aplikacijski server. nacrtati to
7. imaš firmu, VPN, firewall, HTTP, IDS.. nacrtaj i objasni
8. od prijatelja dobiš sms (koristiš android) da ideš na neki link. hoćeš li to napraviti?
9. Koje metode antivirusi koriste za zaštitu od malwarea? Objasni ih.
10. kako biste osigurali neporecivost i povjerljivost prilkom slanja maila?
11. što je WoT? kako se koristi u PGP-u?
12. razlika signed-data i clear-signed data MIME
13. koji su dijelovi certifikata? kako ćemo provjeriti važenje certifikata?
14. pravila kao u 1.MI, jedno od pitanja je može li se s firewall-a pristupiti na www.google.com ako se koristi https?
15. neki kod, prepoznati napad i opisati, SQL injection
16. Zašto je opasan RFID sniffing? Kako se od toga štiti?
17. Za što služi kontejnerizacija? Kako sličan princip zovemo kod računala?

1. Marko Č. hackira facebook, mijenja sadržaje i blokira pristup Zuckerbergu. Koja su načela sigurnosti time povrijeđena?

Cjelovitost, povjerljivost, raspoloživost.

2. Korisnik ima username i password u nekoj mreži. Kako on to može zlorabiti?

3. Mala tvrtka postavlja IDS, a ne može ga stalno updatetati. Kakav biste im IDS preporučili i koji su rizici vezani uz njega?

Alat koji funkcionira na principu proučavanja nepravilnosti. Princip se temelji na tome da alat u početku “nauči” što je normalna aktivnost u mreži i da na temelju toga kasnije uočava odstupanja. Glavni rizik je potencijalno veliki broj lažnih uzbuna.

4. Što je PGP i malo ga opisati (načini razmjene ključeva, princip funkcioniranja)?

PGP je mehanizam koji osigurava povjerljivost komunikacije elektroničkom poštom s kraja na kraj. Omogućava 5 osnovnih usluga: autentifikaciju, šifriranje, sažimanje (kompresiju), kompatibilnost s infrastrukturom elektroničke pošte, segmentaciju i ponovno slaganje poruke. Povjerenje u ključeve temelji se na modelu web of trust - razina povjerenja u ključ ovisi o broju potpisa na ključu od strane korisnika s kojima je od prije uspostavljeno povjerenje.

5. U požaru je uništen jedini zapis vašeg javnog ključa (PGP). Dobili ste mailove šifrirane starim javnim ključem, hoćete li ih moći pročitati? Što treba napraviti kako bi ponovno imali sigurnu komunikaciju?

Moci ce se procitat mail zato jer imamo idalje privatni kljuc. Mogli bismo traziti druge da nam posalju natrag naš javni kljuc. Ubuduće bi trebali imat backup ključeva.
*ako je privatni uništen, nećemo moći pročitati mail i morat ćemo zatražiti nove ključeve.

6. Što je wardriving i kakve su opasnosti od njega?

Wardirving je pretraživanje dostupnih Wi-Fi mreža, pri čemu se napadač kreće područjem i zapisuje razine signala i GPS koordinate okolnih mreža.
Potencijalna opasnost je otkrivanje ranjivosti dostupnih mreža.

7. Zašto su društvene mreže pogodnije za širenje malwarea?

Potencijalno maliciozni zahtjevi dolaze od mrežnih prijatelja i time djeluju uvjerljivije.
pr. *xy sent you an image.*
Morat ćeš kliknut da vidiš šta je a unutra malware!

8. Koje su (barem) dvije prijetnje najopasnije na mobitelima i koji OS je najugroženiji?

Bluetooth ranjivosti, malware, wardriving, RFID sniffing, uskraćivanje usluge, web aplikacije. Najugroženiji je Android, u Aziji Symbian.

9. Kako HTTP pruža potporu sjedničkoj komunikaciji, koji je OWASP napad vezan uz to i opisati i skicirati taj napad.
HTTP je stateless protokol. Podrsku sjednici pruza pomocu session_id tokena kojeg klijent moze poslati kroz cookie, GET ili POST. Ukoliko se ovaj token posalje (ili ukrade) do nekog treceg klijenta, treci klijent ce imati pristup originalnoj sjednici. Najcesci propust je slanje session_id tokena kroz GET parametar i onda (slucajno) dijeljenje svog URL-a sa sesssion-om nekom drugom. OWASP A2. Drugi slican napad, “session fixation” je kada nekome damo link koji u sebi sadrzi session token i pitamo ga da se ulogira na ranjivi servis. Kada se ulgoria, mi cemo s istim linkom imati pristup njegovom racunu.

10. Dan je kod koji otvara mogućnost (u ovom slučaju) injection napada. Treba to zaključiti i opisati kako se to događa u ovom slučaju.
Vjerojatno se napadaču prikaže neki prozor gdje umjesto podatke, upiše SQL naredbe koje se pohranjuju u bazu i izvode kao SQL upit te dohvaćaju natrag rezultate upita koje onda napadač preuzima.

11. Koje je sigurnosne mehanizme po defaultu predviđao SMTP?

Nikakve. Nije postojala autentifikacija za pošiljatelja, integritet ni povjerljivost. to je riješeno sa SMTPS na transportnom sloju

12. Što je buffer overflow?
Preljev spremnika se dešava kada u spremnik pokušavamo pohraniti više podataka no što je kapacitet spremnika. Preljev spremnika ima razne posljedice, između ostalog i gašenje računala. Također dolazi još i do prepisivanja memorijskih lokacija koje nisu namijenjene za smještanje podataka koji se zapisuju u polje. Budući da se ostale funkcije pozivaju sa parametrima sa određenih memorijskih lokacija, ukoliko prebrišemo prave lokacije možemo upravljati parametrima drugih funkcija.
DoS napadi u kojima se na određenu mrežnu adresu pošalje više
prometa nego što je predvideno za tu adresu. Napadac može znati da ciljani sustav ima slabosti koje može zloupotrebiti, npr. da je odredeni dio sustava nezašticen ili napadati slucajnim odabirom. Nekoliko poznatih napada te vrste temeljili su se na cinjenici da sustavi imaju osnovne odredene kapacitete (default buffer). Ti napadi provodeni su npr. slanjem prevelikog broja ICMP paketa (poznat kao ping smrti)

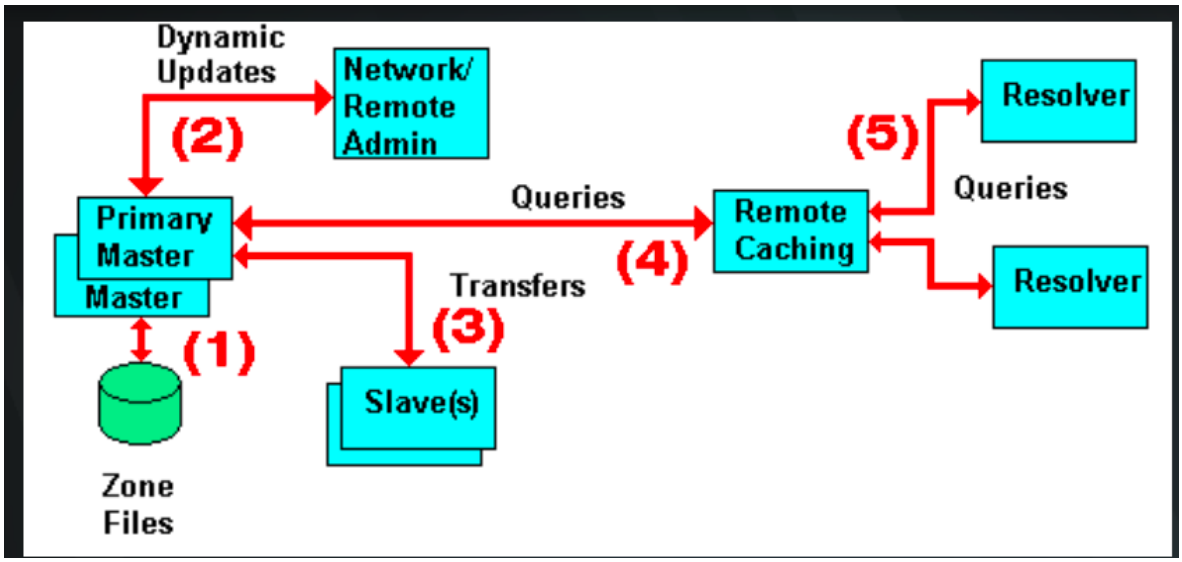
1. CIA, primjer narušavanja za svaki
povjerljivost(confidentiality) - čitamo nečije povjerljive podatke (npr. SMTP se prenosi u plaintextu)
cjelovitost,integritet(integrity) - mjenjamo sadržaj nekih informacija, možemo promijeniti i sadržaj IP paketa (opet SMTP di bi mogli mjenjat sadržaj maila)
raspoloživost(availability) - raspoloživo - DoS napad ili požaar - više nije raspoloživo

3. korisnik misli da mu je narušen integritet datoteka, koji alat biste mu preporučili i da li on u potpunosti osigurava njegovo računalo

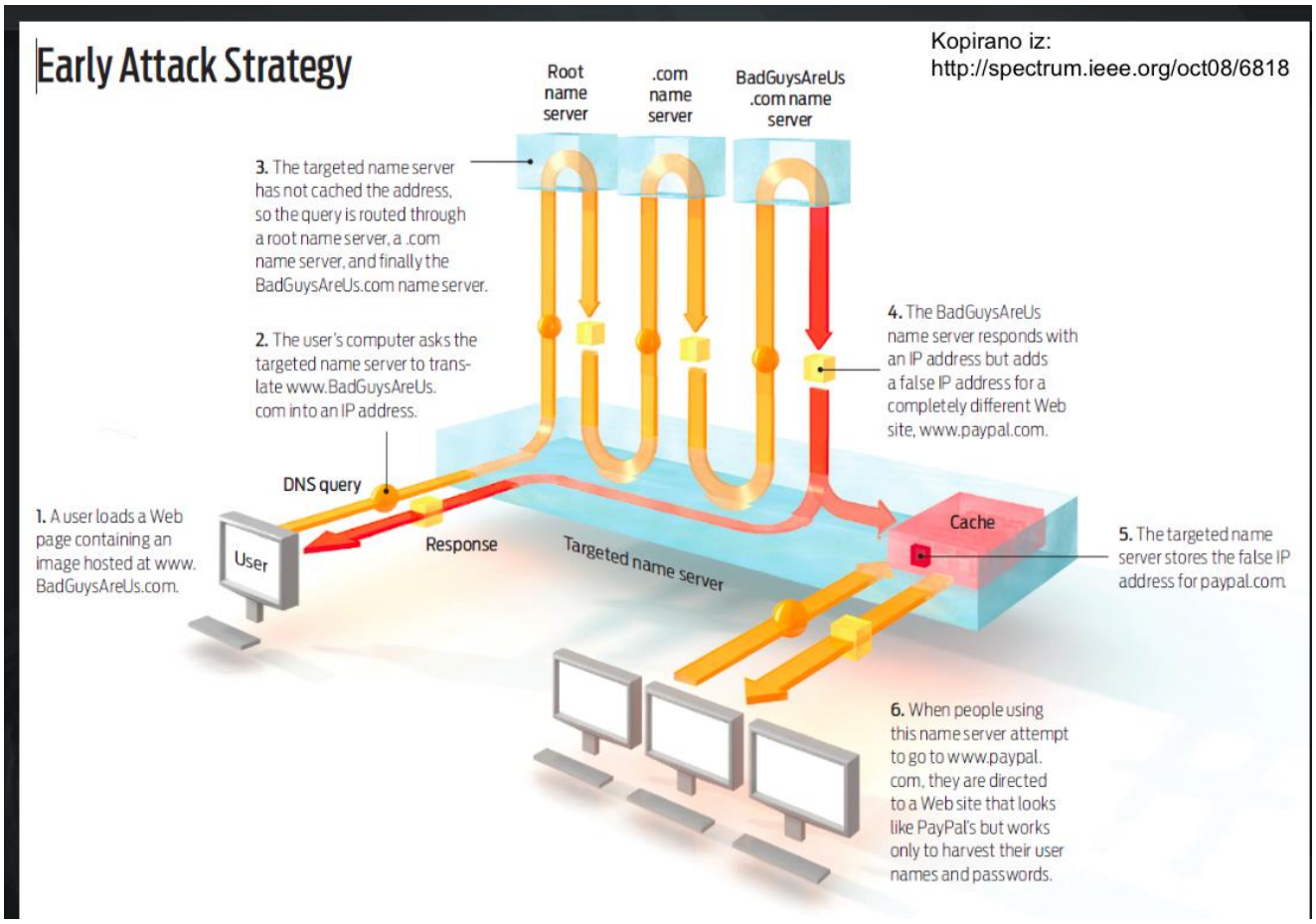
Preporučili bismo mu alat Tripwire koji generira sažetke svih datoteka u računalu i sprema ih u bazu podataka. Na taj način moguće je provjeriti poklapa li se sažetak sporne datoteke sa sažetkom u bazi podataka. Ako sažetci nisu jednaki datoteka je kompromitirana. Alat je moguće prevariti (npr. pomoću rootkita) stoga računalo nije u potpunosti osigurano.

4. nacrtati mrežu sa protokolima https, http, smtp koristeći sve mehanizme sigurnosti koje smo učili

5. DNS napadi i DNSSEC

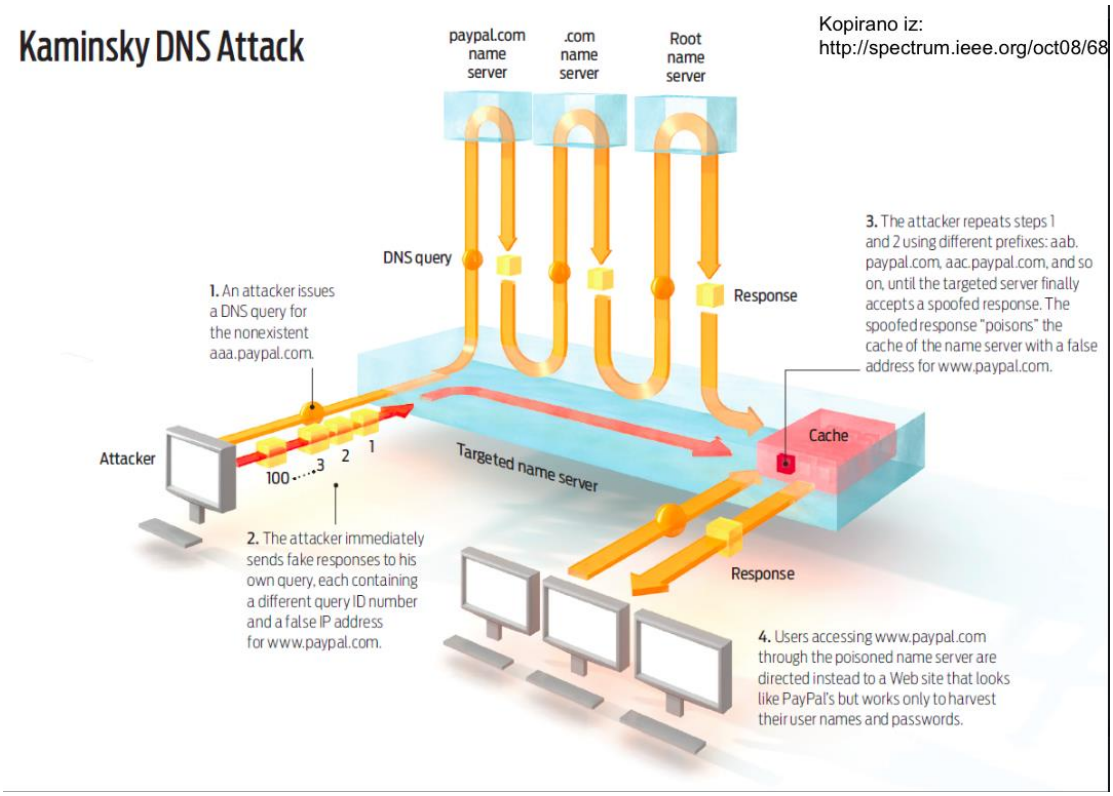


1. Pokvareni podaci
2. Neautorizirana osvježenja
3. Promijenjeni podaci o zoni, Glumljenje “mastera”
4. Zagađenje cachea (trovanje priručne memorije)
5. Glumljenje cachea



Slika prikazuje postupak zagađenja cachea meni se to ne da prevodit. Ukratko:

šalje se DNS upit (npr. za www.abc.com) i u DNS odgovoru se stavlja fejk IP adresa (npr od www.paypal.com) i sprema se u cache. Korisnik ode na paypal, sve mu izgleda kao da je na paypalu, ali ubiti mu se kradu podaci.



Imena dns servera na ovoj slici su naopako poredana. Prvo se pita Root name server. Evo jedan simpa link na youtube o Kaminsky napadu.
https://www.youtube.com/watch?v=qftKfFVHVuY

Uvođenjem DNNSEC-a postiže se autentičnost, integritet i neporecivost DNS zapisa korištenjem asimetrične kriptografije (korištenjem javnih i tajnih ključeva). Svaki DNS poslužitelj mora biti potpisan kako bi ova arhitektura mogla funkcionirati. Odgovori generirani korištenjem ovakve arhitekture su znatno veći (Do 2 kbytea). Za velike odgovore moguće je koristiti TCP kao transportni protokol umjesto UDP-a.

6. TCP i UDP napadi

- **TCP napadi**

"TCP overwrite"

Varijacija napada “teardrop”. Napad pokušava prevariti vatrozid. IP datagram se fragmentira, a TCP zaglavlje sadrži odredišni port koji vatrozid propušta. Jednom od fragmenata postavlja se pomak tako da prebriše dozvoljeni port i postavi na neki drugi port od interesa. Vatrozid treba provjeravati minimalni pomak fragmenta. - ŠTA OVO ZNAČI.

Mislim da vatrozid provjerava taj pomak fragmenata samo za prvi paket il šta već i onda ostalo propušta, a TCP overwrite se dogodi negdje kasnije pa ga vatrozid ne vidi na vrijeme.

Skeniranje TCP portova
Ista stvar kao skeniranje UDP portova, može se lakše detektirati ali ga je najlakše izvesti. Brži od UDP skeniranja. Razlikujemo:

- TCP Connect Scan
  Uspostavlja se TCP konekcija s poslužiteljem. Lako se detektira
- TCP Syn scan
  Šalje se paket sa zastavicom SYN, ako je odgovor paket sa zastavicom RST port je zatvoren, ako je SYN/ACK onda je otvoren.
- TCP FIN Scan
  Ako je port zatvoren sustav odgovara paketom sa zastavicom RST, ako nije onda ne odgovara.
- Skeniranje fragmentacijom
  Nisam našo ništa o ovom
- Idlescan - neda mi se
- OS fingerprinting
  Koriste se poznati bugovi u sustavu, posebnosti o odgovorima i parametrima kako bi se otkrila verzija operacijskog sustava - naprimjer TTL.
  Tu ih fali

- **UDP napadi**

UDP obmana - (UDPspoofing)
Mjenjamo izvorišnu adresu UDP datagrama i time se predstavljamo kao drugo računalo.

UDP otimanje - (UDPhijacking)
Napadač odgovara na klijentove zahtjeve UDP paketima koji imaju kao izvorišnu adresu adresu poslužitelja.

UDP oluje - (UDPstorms, “UDP flooding”, “UDP DoS”)
Najčešće se koriste servisi koji automatski odgovaraju na poruke, npr. chargen ili daytime. Lažira se UDP paket na način da mu se pod izvorišnu adresu stavi adresa žrtve, a pod izvorišni port port jednog automatskog servisa. Takav datagram se šalje na neko drugo računalo također na port automatskog servisa. Računala si tako automatski odgovaraju u bekonačnost.

Skeniranje UDP portova
Napadač pokušava otkriti koji se sve servisi vrte na računalu. Ako je port zatvoren, sustav može ali i ne mora odgovoriti porukom ICMP port unreachable. Ako odgovori onda je port sigurno zatvoren, ali ako ne odgovori ne možemo biti sigurni da nije zatvoren. Tehnika je spora.

7. neki kod zadan, i trebalo je napisati na koje napade je izložen i kako ih spriječiti
8. digitalni certifikat što sadrži, kako ga opozvati, što sadrži javni ključ

Opozivamo certifikat tako da odemo u CA koji je izdao certifikat, tamo prijavimo da ga želimo povući nakon čega će certifikat biti postavljen na CRL.

9. što je honeypot, da li osigurava dovoljnu zaštitu, ako ne što biste preporučili umjesto toga

-oponašanje dobro poznate rupe u zaštiti, predstavlja žrtvu napda

-ne osigurava

-

-nedostaci:

- prate napad usmjeren samo na njih
- napadači ih mogu preuzeti

- 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

10. što je hash, za šta služi i primjer korištenja

Hash je funkcija kojom se podaci hashiraju :) tj bitno promijene te je gotovo nemoguće ponovno otkriti početne podatke (one-way hash).
Služi npr. kod pohrane passworda gdje se izgenerira hash od unešenog passworda, spremi, te pri svakom idućem pokušaju autorizacije hash se ponovno generira i uspoređuje s onim prvim hashom.
Primjena: digitalni potpisi, autentifikacija, hash-tablice, checksum
Hash je funkcija kojom se stvara sažetak poruke. Ulaz je proizvoljno dug tekst, a izlaz je fiksne duljine. Koristi se kod digitalnog potpisa, autentifikacije, za provjeru

kontrolne sume. Hash je jednosmjerna funkcija što znači da iz izračunatoh hash-a nije moguće dobiti izvornu poruku.
identifikacija - prepoznavanje da postoji takav korisnik kakav se pokušava prijaviti. To je, recimo, username.
autorizacija - dokaz da se stvarno taj korisnik prijavljuje. To je password.
1. Treba napisati koje sigurnosne usluge (CIA) nude:
kakvo je ovo pitanje???
- slanje rezultata ispita preko interneta u plain textu
- hitni pozivi
- bankovna transakcija
- povjerljivi podaci

2. Primite poruku koja je šifrirana simetričnim ključem te uz nju dobijete taj isti simetrični ključ šifriran asimetričnim ključem (vašim javnim). Što morate napraviti kako biste pročitali dobivenu poruku?
Potrebno je prvo našim privatnim dešifrirati taj simetrični ključ i onda tim dešifriranim simetričnim ključem dešifrirati poruku. To je hibridni pristup.

3. Dana dva ispita s netstat i iz njih treba prepoznati dva TCP napada te otkriti napadačevu IP adresu.

4. Uočite nagli porast konekcija s protokolom UDP i ARP u petak i onda još preko vikenda to podivlja. O kojem se zloćudnom programu radi? Koji su glavni dijelovi tog zloćudnog programa? Kojim protokolom od navedenih se on vjerojatno širio?

crv koji se širi udpom

5. Napišite na kojim slojevima TCP/IP složaja se nalaze uređaji te označite koji su podložni prisluškivanju:

router - mrežni, podložan
switch - podatkovni, podložan
hub - fizički, podložan

6. IPFW naredbe, prepoznati što koja radi. Jedna je bila i s STATE ESTABLISHED, tako nešto. Prepoznati podmreže s kojih se može pingati poslužitelj. Mogu li se slati HTTP zahtjevi na poslužitelj?

Nešto ovako: -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
Hvala kolegi j0p@.

1) Propustaju se ulazni paketi koji nisu novi nego pripadaju vec postojecoj konekciji
2) Propustaju se ulazni paketi koji dolaze od zadane podmreze prema portu 22
3) Posluzitelj se moze pingati sa podmreza koje su navedene u pravilu oblika INPUT -p ICMP ACCEPT
4) Ne mogu se slati zahtjevi na posluzitelj jer ne postoji pravilo koje prihvaca pakete prema portu 80

8. U vašoj firmi se gura BYOD (*Bring your own device*) jer svi zaposlenici imaju smartphoneove. Navedite 3 moguća sigurnosna problema koji bi mogli utjecati na mrežnu strukturu. Kako bi se taj problem mogao riješiti?
-pristupa se podacima tvrtke koji ostaju na mobitelu i nakon što zaposlenik otiđe iz tvrtke i može ih netko ukrasti
-lako izvođenje phising napada na BYOD uređajima
-veća ranjivost na malware koji mogu krasti informacije kad se zaposlenik spoji na wi-fi
-laka provala u uređaj pri njegovu gubitku
Može se riješiti instalacijom antivirsunog programa ili kontejnerizacijom, gdje će uređaj imati dva profila – sigurni i obični te podatke nije moguće prebacivati iz jednog u drugi.

9. Korisnik pri prijavi na aplikaciju dobiva *Session ID*. Može li se autentifikacija osloniti u potpunosti samo na HTTP protokol? Ako da, zašto, ako ne, zašto ne? Gdje se sve može spremiti Session ID?
-ne, autentifikacija se izvodi preko SSL-a čime se dobiva sigurniji HTTPS
-SESSION ID se vidi na mreži, u pregledniku, u logovima, a može se spremiti i u URL čime se izvodi loša autentifikacija
-rj: novi SESSION ID kod svakog zahtjeva

10. Dana dva različita sažetka. Jedan je dobiven izračunom nad skinutom instalacijskom datotekom, a drugi je došao uz datoteku. Hoćete li pokrenuti tu instalacijsku datoteku. Ako da, zašto da, ako ne, zašto ne? Možete li iz sažetka rekonstruirati instalacijsku datoteku? Ako da, zašto da, ako ne, zašto ne?
-ako saželi (hash) nisu jednaki, znači da je ubačen virus, pa nećemo pokrenuti datoteku
-iz sažetka se ne može rekonstruirati instalacijska datoteke, jer je hash jednosmerna funkcija (pogledaj hash :D)

11. Dan je neki pseudo/php kod sličan ovom koji obrađuje formu, $komentar je unos korisnika:

html kod:
```
public void dodajZapis($komentar)
{
  $komentar = počisti($komentar);
```

```
  $rezultat = mysql_upit('INSERT INTO komentari (komentar) VALUES
('$komentar')');
}
public string počisti($komentar)
{
  $komentar = ukloni_sve("<script>", $komentar);
  $komentar = ukloni_sve("</script>", $komentar);
  return $komentar;
}
```

Kakav napad se može napraviti? Može li se kakav drugi način injectiona koristiti i kako?

Ovaj kod je podložan SQL Injectionu tako da možemo dumpat cijelu bazu ako si damo truda. Također, miču se jedino script tagovi tako da možemo ubacivat html kod što isto nije ok.

12. Što je *Same origin policy*? Zašto se unatoč njoj može provesti CSRF?

Od prvih inačica funkcija XHR izvedena je tako da poštuje tzv. „same origin“ pravilo. Riječ je o pravilu koje zahtjeva da se web zahtjevi mogu pokretati samo nad stranicama iz kojih su učitani. Tako je web odredište s kojeg se učita programski kod jedino odredište prema kojem mogu biti upućeni zahtjevi za sadržajem koji je dio učitanog koda. Na taj način otklanja se mogućnost CSRF napada. Ipak, valja napomenuti kako samo pravilo istog izvora i odredišta ne jamči potpunu sigurnost. Može se zaobići manipulacijama DNS-om ili skrivanjem pravog izvora zahtjeva posebnim oblikovanjem HTML-a. Primjer takvog oblikovanja može biti manipulacija „Referer“ zaglavljem koje sadrži informaciju o izvoru poruke. Razvojem Web 2.0 tehnologija sve je naglašenija potreba za komunikacijom između web odredišta bez interakcije korisnika, odnosno za odbacivanjem „same origin“ pravila. Time se otvaraju naprednije mogućnosti oblikovanja web sustava i usluga, ali se i povećava opasnost od CSRF i drugih napada.
(kopirano sa carnetove stranice)