Bezbednost na internetu: Sajber kriminal i sajber napadi, glasanje preko interneta

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Prvi autor, drugi autor, treći autor, četvrti autor
kontakt email prvog, drugog, trećeg, četvrtog autora

25. mart 2019

Sažetak

U ovom tekstu je ukratko prikazana osnovna forma seminarskog rada. Obratite pažnju da je pored ove .pdf datoteke, u prilogu i odgovarajuća .tex datoteka, kao i .bib datoteka korišćena za generisanje literature. Na prvoj strani seminarskog rada su naslov, apstrakt i sadržaj, i to sve mora da stane na prvu stranu! Kako bi Vaš seminarski zadovoljio standarde i očekivanja, koristite uputstva i materijale sa predavanja na temu pisanja seminarskih radova. Ovo je samo šablon koji se odnosi na fizički izgled seminarskog rada (šablon koji *morate* da ispoštujete!) kao i par tehničkih pomoćnih uputstava. Pročitajte tekst pažljivo jer on sadrži i važne informacije vezane za zahteve obima i karakteristika seminarskog rada.

Sadržaj

1 Uvod

Napomena: U uvodnom delu treba imati više od dva citata. Milena je na predavanju rekla da treba što više citata da se ubacuje. Postoji dva tipa citata koje je preporuceno koristiti:
1. gde se može naći detaljnije o toj temi
2. objašnjenja. Tipa odakle tvrdim da je to važno, koje istraživanje je ivršeno, pa to iznosim kao činjenicu...
Ovde [2] citiram knjigu po kojoj smo izabrali poglavlja

2 Pojam sajber kriminala

Visokotehnološki ili sajber kriminal (eng. *cyber criminal*) predstavlja moderni vid kriminala, tačnije, putem računara. Sajber kriminalci su osobe ili grupe ljudi koji koriste tehnologiju kako bi izveli zlonamerne aktivnosti putem mreže sa ciljem da ukradu osetljive podatke neke firme, lične informacije ili da profitiraju [1].
Zakoni koji se odnose na ovu vrstu kriminala se dopunjuju i razvijaju u zemljama širom sveta. Najizloženije zemlje za sajber napade su one koje su u razvoju. U takvim zemljama je zakon o ovoj oblasti slabo definisan, a u nekim ni ne postoji. Takođe, veoma je teško pronaći i uhapsiti zločinca u sajber kriminalu jer su dokazi često nepostojeći.

Treba napraviti razliku između sajber kriminalca i hakera. Sajber kriminalci sa lošim namerama vrše upad u računare, dok hakeri traže inovativne načine da koriste sistem, bili ti načini loši ili dobri.

3 Sajber kriminal i napadi

U mnogim zemljama, internet odvija ključnu ulogu u svakodnevnom životu ljudi. Olakšava virtuelnu komunikaciju među ljudima, podstiče razvoj novih poslovnih modela i kompanija, menja način na koji ljudi kupuju. U 2018. godini, transfer novca koji uključuje prodaju i kupovinu putem interneta, iznosila je oko 2800 milijardi američkih dolara. Prema statističkim studijama [3], smatra se da će u 2021. ta vrednost iznositi oko 4.88 biliona dolara. Iz ovih razloga, nije neobično da je sa porastom popularnosti interneta porasla i stopa kriminala na njemu. U ovom poglavlju otkrivamo tri vrste napada putem interneta.

3.1 Phishing

US-CERT (The United States Computer Emergency Readiness Team) definiše "phishing" kao vrstu "social engineering"-a gde se napadač pomoću elektronske pošte ili zlonamernih veb sajtova lažno predstavlja kao pouzdana organizacija ili kompanija kako bi prikupio lične podatke od pojedinca ili kompanije. Napadi "phishing"-a se često sastoje od slanja korisnicima imejlova koji izgledaju kao da su iz bankarske ili finansijske institucije ili veb servisa preko kojeg pojedinac ima račun. Cilj "phishing"-a je da prevari primaoca da da svoje podatke za prijavljivanje ili druge osetljive informacije.
Na primer, napadač može da pošalje milione imejlova sa botnet-a. Poruke obaveštavaju primaoce da je njihov nalog za elektronsku trgovinu bio

kompromitovan i upućuju ih na veb lokaciju gde bi rešili problem. Korisnici koji kliknu na link dođu do veb stranice koja je napravljena tako da podseća na originalni sajt za elektronsku trgovinu. Kada se nađu na sajtu, od njih se traži korisničko ime, lozinka i druge privatne informacije. Te informacije mogu da se iskoriste za krađu identiteta.

Ciljani (spear) "phishing" je varijanta "phishing"-a u kojoj napadač bira adrese elektonske pošte tako da cilja jednog ili određenu grupu primalaca. Na primer, napadač može ciljati starije osobe kao osobe koje se smatraju lakovjernijima ili članove grupa koji imaju pristup vrednim informacijama. "Spear phishing" može biti veoma delotvoran jer omogućava napadaču da uobliči napad tako da žrtva zbog hitnosti ili poverenja određenim osobama bude manje oprezna. Za "spear phishing" je potrebno da napadač prikupi lične podatke o žrtvi, kao što su imena prijatelja, poslodavac, rodni grad, lokacije koje posećuje, šta je nedavno kupila na mreži... Na primer, napadač može da pošalje imejl nekoliko ljudi koji izgleda kao da je od njihovog direktora, gde im je poslat poziv na sastanak putem Gmaila, a link u poruci navodi primaoce da se prijave na Gmail da prisustvuju sastanku.

Prema jednom istraživanju, bilo je najmanje 67.000 "phishing" napada širom sveta u drugoj polovini 2010. godine. Zanimljivo je povećanje "phishing" napada na kineske e-trgovine, što ukazuje na povećavanje važnosti kineske ekonomije. U 2018 godini APWG (Anti-Phishing Working Group) je otkrio 785 920 sajtova za "phishing".

3.2 SQL injekcija

SQL injekcija jeste umetanje dela ili celog SQL upita obično preko polja za unos na veb stranici. Ukoliko ovako nešto uspe može se pristupiti osetljivim podacima iz baze, mogu se modifikovati podaci, izvršiti administrativne operacije nad bazom itd. Pogledajmo primer ispod koji kreira SELECT upit koji dodaje sadržaj promenljive(txtUserId) na SELECT string. Sadržaj promenljive je sadržaj polja za unos korisničkog id-a (getRequestString).

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

Jedan od načina upotrebe SQL injekcije zasniva se na činjenici da je „1=1“ uvek istinito. Zamislimo da je korisnik u polju za unos uneo „105 OR 1=1“ . Tada bi SQL upit iz prethodnog primera izgledao ovako:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

Ovakav upit vratiće sve redove „Users“ tabele, jer je „1=1“ uvek istinito. Šta ako tabela „Users“ sadrzi imena i šifre? Haker moze pristupiti svim imenima i šiframa iz baze jednostavno dodavajuci „105 OR 1=1“ u polje za unos korisničkog imena.

„ ""="" “ je uvek istinito i ovo je još jedan način upotrebe SQL injekcije. Recimo da imamo sledeći deo koda:

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' + uName + '" AND
Pass ="' + uPass + '"'
```

Haker jednostavno može pristupiti korisničkim imenima i šiframa u bazi unoseći „ " OR ""=" " u polje za šifru ili u polje za korisničko ime. Kod na serveru ce kreirati ispravan SQL upit:

```
SELECT * FROM Users WHERE Name ="" OR ""="" AND Pass ="" OR ""="";
```

SQL upit koji se nalazi iznad vratiće sve redove iz tabele „Users“, jer je „ OR ""="" " uvek istinito.

Mnoge baze podrzavaju grupu SQL upita razdvojene „ ; “. SQL upit ispod vratiće sve redove iz tabele „Users“, i potom obrisati „Suppliers“ tabelu.

```
SELECT * FROM Users; DROP TABLE Suppliers
```

Pogledajmo sledeći primer:

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

Ukoliko bi korisnik u polje za korisnički id uneo „105; DROP TABLE Suppliers“ SQL upit koji se nalazi iznad izgledao bi ovako:

```
SELECT * FROM Users WHERE UserId = 105; DROP TABLE Suppliers;
```

Kako se zaštititi od ovakvih napada? Tako što cemo koristiti SQL parametre. SQL parametri su vredosti koje su dodate SQL upitu u vreme izvršavanja na kontrolisan način.

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = @0";
db.Execute(txtSQL,txtUserId);
```

Primer iznad je deo koda u ASP.NET-u u kome se koriste parametri. Parametri su predstavljeni znakom @. SQL mehanizam proverava parametre kako bi se uverio da su ispravni i da se tretiraju bukvalno a ne kao deo SQL-a koji se izvršava.

3.3 DoS napadi

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

DoS (Denial-of-Service) napad je radnja napravljena tako da spreči legitimitne korisnike da koriste usluge računara, tj. počinilac (izvršilac) čini mašinu ili mrežni resurs nedostupnim (gasi ih) svojim korisnicima tako što privremeno ili neograničeno ometa usluge hosta povezanog na Internet. DoS napad moze da uključi neovlašćeni pristup jednom ili više kompjuterskih sistema, ali cilj napada nije krađa informacija, nego je cilj da poremeti sposobnost servera da odgovori na korisničke zahteve tako što poplavljuje metu saobraćajem (?? popravi) ili šalje informacije koje aktiviraju razne nezgode. Ometanje normalnog rada kopjuterskih usluga moze da proizvede značajnu stetu. Firma koja se bavi nekom vrstom prodaje putem Interneta može da izgubi posao. Vojsci može da se prekine komunikacija. Vladi ili nekoj neprofitnoj organizaciji može da se desi da ne može da prenese svoju poruku javnosti.

DoS napad je primer "asimetričnog"napada, u kome jedna osoba moze dosta da naškodi velikoj organizaciji. Pošto se terorističke organizacije specijalizuju za asimetrične napade, neki strahuju da će DoS napadi postati važan deo terorističkog oružja.

3.3.1 DDoS napadi

Dodatni tip DoS napada je DDoS (Distributed Denial-of-Service) napad. Glavna razlika je u tome što meta nije napadnuta sa jedne lokacije, već sa više njih odjednom. Do DDoS napada se dolazi kada višestruki sistemi orkestriraju sinhronizovani DoS napad na jednu metu. Podela hostova koji određuju DDoS daje napadaču više prednosti:

- Napadač može iskoristiti veću količinu mašine (popravi) da izvrši ozbiljno razoran napad
- Lokacija napada se teško određuje zbog slučajne podele napadačkih sistema
- Teže je ugasiti više mašina nego jednu
- Pravu napadačku partiju (attacking party - potrazi) je veoma teško identifikovati, jer se oni prikrivaju iza mnogih (uglavnom kompromitovanih) sistema

Mnoge sigurnosne tehnologije su razvile mehanizme za odbranu od mnogih vrsta DoS napada, ali, zbog jedinstvenih karakteristika, DDoS se jos uvek smatra ozbiljnom pretnjom.

4 Sajber kriminal

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

4.1 Primeri kriminalnih napada

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

5 Sajber napadi

Sajber napad predstavlja napad od računara do računara koji povređuje poverljivost, integritet i informacije koje se nalaze na napdanutom računaru [2]. U ovom poglavlju ćemo se susresti sa nekim primerima napada na države i velike svetske gigante u poslednjih deset godina.

5.1 Primeri napada na države

1. GRUZIJA (2008)
   Gruzija je jedna od bivših Sovjetskih republika koja je stekla nezavisnost 1991. gidine. Južna Osetija, oblast na teritoriji Gruzije koja je pripadala Rusiji do 1991, nakon kratkog rata iste godine, postaje i međunarodno priznata kao autonomna pokrajna Gruzije. Nakon provokacije separatista u Južnoj Osetiji, Gruzija šalje vojsku na ovu teritoriju 7. avgusta 2008. godine. Ruske snage su 8. avgusta ušle u Južnu Osetiju i ove dve strane su se borile četiri dana. Ovaj sukob je ostao zapamćen i iz razloga što je gruzijska vlada i pre nego što je ruska vojska došla na teritoriju Južne Osetije imala problem sa velikim DDoS napadom. Njihova vlada nije bila u mogućnosti da komunicira sa ostatkom sveta. Mnogi veb sajtovi su bili srušeni na nekoliko sati. Gruzijska vlada je bila primorana da lokacije nekih svojih veb servera prebaci na SAD. Postojale su sumnje je da je

napad izvrvršila grupa kriminalaca pod nazivom "Russian Business Network", smeštenih Sent Peterburgu u Rusiji, ali je ostalo nerazlučeno da li je ova grupa imala neke veze sa ruskom vojskom.
Na isti dan godinu dana kasnije, Tviter je bio onesposobljen u celom svetu na nekoliko sati zbog masovnih DDoS napada. Maks Keli, šef za bezbednost u kompaniji Fejsbuk, rekao je da je svrha napada bila da se spreči objavljivanje teksta gruzijskog političkog blogera, pozivajući se na činjenicu da su istovremeno pali i ostali sajtovi koje je ovaj bloger koristio. Ti sajtovi su bili Fejsbuk, LiveJournal i Gugl.

2. SAD I JUŽNA KOREJA (2009)
DDos napad na američku i južnokorejsku vladu je izvršen tokom vikenda uoči 4. jula, američkog Dana nezavisnosti. Tom prilikom zabeležen je pad više od trećine veb sajtova u ovim državama. U Americi je napadnuta Bela kuća, američki trezor, Tajna služba, njujoršku berzu i kompaniju NASDAQ. U Južnoj Koreji, DDoS napad je izvršen na Plavu kuću(predsednička palata), Ministarstvo odbrane i Narodnu skupštinu.
Ova vrsta napada se smatra relativno malom jer je izvršen uz pomoć botnet-a(naći referencu za botnet) koristeći između 50 i 65 hiljada računara, što se smatra malom cifrom u poređenju na velike napade gde se koristi oko milion računara. Ipak, ova vrsta napada je ostala zapamćena i po tome što su južnokorejski sajtovi ostali nedostupni do 9. jula. Pretpostavljalo se da je napad izvršen kao vid osvete jer su Ujedinjene Nacije uvele određene sankcije Severnoj Koreji u tom periodu. I do danas se još uvek ne zna ko je tačno izveo ovaj napad jer su napadači koristili računare koji su bili u posedstvu drugih ljudi.

5.2 Primeri napada na kompanije

1. Yahoo
Yahoo je jedan od najvećih giganta na internetu. Ova kompanija je 2016. godine objavila informaciju da je bila žrtva jednog od najvećih napada u istoriji; 2013. godine je grupa hakera kompromitovala tri milijarde naloga korisnika. Pored imena, datuma rođenja, imejl adresa i šifara, zaštitna pitanja i odgvori su takođe otkriveni. Pored ovog napada, 2014. je zabeležen još jedan napad na ovu kompaniju. Tada su obelodanjena imena, imejl adrese, datumi rođenja i brojevi telefona 500 miliona korisnika. Ovoga puta su šifre ostale zaštićene.

2. eBay
Ova kompanija se bavi prodajom proizvoda putem interneta. Bila je napadnuta u maju 2014. kada su otkrivena imena, adrese, datumi rođenja i enkriptovane šifre(naći referencu za enkripciju) od 145 miliona korisnika. Kriminalci su "upali"u bazu tako što su koristili kreditacije troje zaposlenih i imali su pristup unutrašnjosti 229 dana.U tom periodu su imali vremena da pristupe bazi podataka korisnika. Informacije koje se tiču finansija kao što su brojevi kreditnih kartica su ostale zaštićene jer se ta vrsta podataka čuva u odvojenoj bazi.

3. Uber
Uber je američka kompanija koja se predstavlja kao mreža koja pruža

uslue transporta. Ona je 2016. bila napadnuta od strane samo dva hakera koji su uspeli da dođu do imena, imejl adresa i brojeva telefona 57 miliona korisnika Uber aplikacije. Takođe, otkriveni brojevi vozačkih dozvola 600000 vozača na ovoj platformi.
Hakeri su pristupili i Uberovom nalogu na GitHub platformi(referenca) gde su pronašli korisničko ime i lozinku kreditacije ka AWS nalogu(referenca). Uber je ovaj napad objavio godinu dana kasnije. Ova kompanija je platila 100000 američkih dolara hakerima da unište podatke.

6 Glasanje preko interneta

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

6.1 podnaslov

Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst. Ovde pišem tekst.

7 Zaključak

Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak. Ovde pišem zaključak.

Literatura

[1] Trend Micro. Cybercriminals, 2019. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

[2] Michael J. Quinn. *Ethics for the information age*.

[3] Statista. Retail e-commerce worldwide, 2017. https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

1. https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals
2. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
3. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
4. https://www.w3schools.com/sql/sql_injection.asp
5. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html