SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 16:

Etičko hakerisanje i ispitivanje mogućnosti proboja

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Etičko hakerisanje i ispitivanje mogućnosti proboja”**

Etičko hakerisanje i ispitivanje mogućnosti proboja

- Sadržaj poglavlja i predavanja:
  - 16.1 Etičko hakerisanje
  - 16.2 Ispitivanje mogućnosti proboja

Etičko hakerisanje - *ethical hacking*

Ispitivanje mogućnosti proboja – *penetration testing*

Napomena: Ovo predavanje podrazumeva predznanje i primenu materije iz svih prethodnih poglavlja tj. predavanja

Quote

"Program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence."

- Edsger Dijkstra

Potrebna predznanja

- Programiranje
- Računarske mreže i protokoli
- Operativni sistemi
- Sistemsko programiranje
- Strukture i modeli podataka, baze podataka

Uvod

- Kada se sprovedu sve preporučene mere za zaštitu računarskih sistema, mreža i informacionih sitema od napada i prodora, tj. narušavanja sigurnosti, potrebno je uraditi analizu i proveru uspešnosti zaštite.
- Razvijeni su načini testiranja koji bi trebalo da pokažu koliko je zaštita pouzdana i efikasna.
- Napadači su nepredvidivi i stalno smišljaju nove načine i metode da ostvare svoje ciljeve.
- Prednost napadača je u tome što imaju više vremena, mogu da biraju vreme, način i sredstva za napad, tj. imaju prednost faktora iznenađenja.
- Odbrana, međutim, mora biti spremna i aktivna u svako vreme i na svakom mestu. U protivnom, sistem će verovatno biti ugrožen.

Provera i ispitivanje sigurnosti

- Da bi zaštitili mrežu, klijenti često angažuju hakere koji po dogovoru napadaju i proveravaju sigurnost uz obavezu da svoja saznanja drže u tajnosti, da ih ne zloupotrebe i da ih isporuče samo organizaciji koja ih je angažovala i isključivo u svrhu unapređenja sigurnosti.

- Etičko hakerisanje - *ethical hacking*
- Ispitivanje mogućnosti proboja – *penetration testing*

16.1 Etičko hakerisanje

- Termin haker (engl. *hacker*) danas ima, u najmanju ruku, dvostruko značenje u računarskoj industriji. Originalno je definisan na sledeći način:
  - **Haker**: imenica,
    - 1. Osoba koja uživa u učenju detalja o računarskim sistemima, i proširivanju svog znanja i sposobnosti – obrnuto od većine korisnika računara, koji preferiraju da uče samo minimum onoga što im je potrebno.
    - 2. Onaj koji oduševljeno programira ili ko uživa u programiranju rađe nego da teoretizuje o programiranju.

- Ovaj laskav opis često se proširuje na reč hakerisanje (engl. *hacking*), koja služi da se opiše brzo učenje novog programa, ili pravljenje izmena u postojećem, obično komplikovanom softveru.

Crni i beli šeširi

- Izraz haker s belim šeširom (engl. *white hat hacker*) ili etički haker (engl. *ethical hacker*) u oblasti informacionih tehnologija, jeste lice koje je etički protiv zloupotrebe računarkih sistema. Ovaj termin se često koristi da se opišu oni koji pokušavaju da prodru u tuđe sisteme i mreže kako bi pomogli vlasnicima tih sistema da postanu svesni sigurnosnih propusta.
- Dok hakeri s belim šeširima pokušavaju da odbrane računarske sisteme, hakeri s crnim šeširima (engl. *black hat hackers*), tj. zlonamerni hakeri – „loši momci“ – pokušavaju da upadnu u tuđe mreže i sisteme, ukradu poverljive informacije i/ili nanesu neku štetu.
- Obe vrste hakera koriste slične metode i alate, ali s različitim ciljem.

Deset zapovesti računarske etike

- Institut za računarsku etiku (The Computer Ethics Institute) neprofitna je istraživačka organizacija koju čine Brookings Institute, IBM, The Washington Consulting Group i Washington Theological Consortium. Ova organizacija je objavila 10 zapovesti računarske etike:
  1. Ne koristi računar da povrediš drugog.
  2. Ne mešaj se nepozvan u tuđ rad na računaru.
  3. Ne njuškaj po tuđim datotekama.
  4. Ne koristi računar da bi lažno svedočio.
  5. Ne koristi računar da bi krao.
  6. Ne koristi komercijalni softver koji nisi platio.
  7. Ne koristi tuđe računarske resurse bez odobrenja ili nadoknade.
  8. Ne prisvajaj sebi zasluge za tuđu intelektualnu svojinu.
  9. Razmisli o posledicama koje će program koji pišeš ili sistem koji projektuješ imati na društvo.
  10. Koristi računar samo na način koji je u skladu s poštovanjem drugih.

  Ako prekršite neku zapovest možda nećete otići u pakao, ali se može desiti da odete u zatvor.

Šta je etičko hakerisanje?

- U nastojanju da donekle reše problem, mnoge organizacije i firme su zaključile da je nezavisni stručnjak za sigurnost koji će pokušati da upadne na njihov sistem, najbolji način da se proveri opasnost od upada u sistem.
- Ovo donekle podseća na nezavisnog revizora koji će proveriti knjigovodstvo u nekoj organizaciji i ukazati na propuste.
- U slučaju računarske sigurnosti, etički hakeri koristili iste tehnike i alate kao i potencijalni napadač, ali za razliku od napadača, ne oštećuju sistem i ne kradu informacije, već procenjuju sigurnost sistema i vlasnika izveštavaju o sigurnosnim propustima na sistemu i o načinima uklanjanja grešaka i propusta.

SATAN

- Rad D. Farmera i W.Z. Venema, "*Improving the Security of Your Site by Breaking into It*", koji je originalno bio poslat na Usenet mrežu u decembru 1993. godine. Oni su javno razmatrali, možda po prvi put, korišćenje hakerskih tehnika za procenjivanje sigurnosti nekog sistema.

- Više informacija o Usenetu naći ćete na lokaciji www.faqs.org/usenet/.

- Njihov program, koji su nazvali Security Analysis Tool for Auditing Networks, ili kratko SATAN, za kratko vreme je stekao veliku medijsku popularnost.

Šta karakteriše etičke hakere?

- Etički hakeri pre svega moraju da budu **osobe od poverenja**.
- **Imaju veliko iskustvo** u poslu s računarima i računarskim mrežama, programiranjem, instalacijom i administriranjem popularnih operativnih sistema (UNIX, Windows Server) koji se koriste na ciljnim računarima.
- **Strpljivost** je najvažnija osobina etičkih hakera zato što oni moraju sebe da stave u poziciju zlonamernih hakera, koji su inače poznati po tome da su veoma strpljivi i voljni da nadgledaju sistem danima ili nedeljama čekajući priliku da upadnu u sistem.

- **Najbolji kandidati** za etičke hakere jesu osobe koje imaju uspešno objavljene naučne radove, radnu istoriju koja ukazuje na dobro poznavanje oblasti sigurnosti, ili osobe koje su napravile popularne sigurnosne programe sa otvorenim kodom.
- Jedno od pravila kojeg se pridržavaju velike kompanije jeste **da se ne unamljuju bivši hakeri s crnim šeširom**. Iako protivnici ovog pravila iznose argument da samo „pravi haker“ poseduje veštinu neophodnu da se posao uspešno obavi, pravilo o apsolutnom poverenju klijenta eliminiše takve kandidate.

Šta etički hakeri rade?

- Etički haker, obavljajući svoj posao, traži odgovor na tri osnovna pitanja:
  - Šta može napadač da vidi na ciljnom sistemu?
  - Šta može napadač da uradi s tim informacijama?
  - Da li je neko primetio napadačev napad ili uspeh?

Razgovori i pitanja koje treba postaviti

- Kada klijent traži procenu, potrebno je da se pre samog posla obavi dosta razgovora i papirologije. Razgovori počinju sa odgovorima klijenata na par pitanja sličnih onima koja su postavljali Garfinkel i Spafford:
  - Šta pokušavate da zaštitite?
  - Od čega želite da se zaštitite?
  - Koliko ste vremena, truda i novca voljni da potrošite kako biste dobili odgovarajuću zaštitu?

Plan, ugovor, preciznost

- **Plan** za identifikovanje sistema koji će biti ispitivan, način ispitivanja, i sva moguća ograničenja ispitivanja.

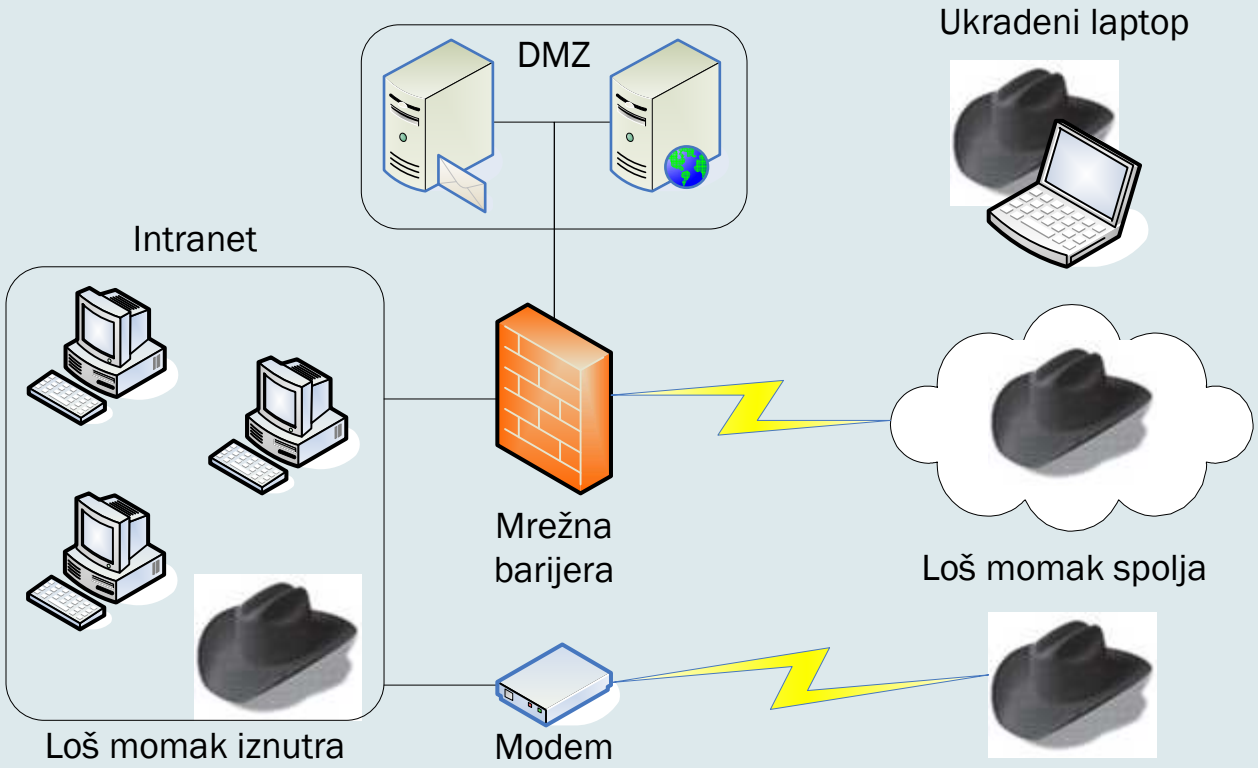
- **Ugovor** između klijenta i etičkih hakera, koji pišu obe strane zajedno. Taj ugovor, poznat pod nazivom „karta za izlazak iz zatvora“ (engl. *get out of jail free card*) štiti etičke hakere od krivičnog gonjenja, pošto je većina aktivnosti koje oni obavljaju pri proceni sigurnosti, nelegalna u mnogim zemljama.
  - Ugovor sadrži precizan opis ispitivanja - obično u obliku mrežnih adresa ili pristupnih brojeva modema sistema koji će se ispitivati.

- **Preciznost** je u ovoj fazi **izuzetno važna**, pošto mala greška može da dovede do evaluacije pogrešnog klijentovog sistema, ili - u najgorem slučaju - evaluaciju sistema neke druge firme.

Pristup „*No-holds-barred*“

- Najbolja procena se radi takozvanim „*no-holds-barred*“ pristupom (testiranje bez ograničenja)
- Najčešća ograničenja koja klijenti nameću etičkim hakerima jesu sledeća:
  - Prekid ispitivanja nakon otkrivanja prvog propusta
  - Izbor trenutka procene sigurnosti
  - Procena „u poslednjem trenutku“

Različiti načini ispitivanja



Sam čin etičkog hakerisanja

- Kao što je prikazano na slici, postoji nekoliko načina za testiranje:
  - Udaljena mreža
  - Udaljena *dial-up* mreža
  - Lokalna mreža
  - Ukraden prenosni računar
  - Društveni inženjering
  - Fizički upad

Etički haker – perspektive testova

- Etički haker može da uradi svaki od navedenih testova iz tri perspektive:
  - kao „loš momak“ spolja (engl. *outsider*)
  - „*semi-outsider*“
  - „loš momak“ iznutra (engl. *insider*), tj. regularni korisnik.

Konačan izveštaj

- Konačan izveštaj je skup saznanja do kojih je etički haker došao tokom procene sigurnosti sistema ili mreže. Detaljno su opisane pronađene ranjivosti i procedure za njihovo otklanjanje. Ukoliko su aktivnosti etičkog hakera otkrivene, opisano je reagovanje osoblja klijenta, i predlozi za poboljšanje reakcija.
- Tehnike kojima je vršeno ispitivanje nikad se ne otkrivaju, zato što osoba koja predaje izveštaj ne može da bude sigurna ko će sve da dođe u posed tog dokumenta jednom kada izađe iz ruku klijenta.
- Sama dostava izveštaja je veoma delikatna stvar. Ako su otkrivene ranjivosti, izveštaj može da bude izuzetno opasan ako padne u pogrešne ruke. Konkurencija može da iskoristi te podatke za industrijsku špijunažu, a zlonamerni haker ih može upotrebiti za upad na računar klijenta.

Šta se dešava nakon isporuke izveštaja?

- Kada je etički haker završio procenu i kada je izveštaj isporučen, klijent može da kaže „Dobro, ako popravim te greške, biću potpuno siguran, zar ne?“.
- Nažalost, nije tako. Ljudi rade na računarima i mrežama klijenta i prave greške. U prvom poglavlju smo objasnili da sigurnost nije trenutno stanje, već proces. Što više vremena prođe od ispitivanja, sigurnost klijenta opada.
- Deo izveštaja uključuje i preporuke koje klijent treba da prati kako bi i u budućnosti smanjio uticaj ovih grešaka.

Edsger Dijkstra - citat

- Veliki Edsger Dijkstra je rekao: ***"Program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence."***

- Isto važi i za ispitivanje sigurnosti: ako ispitivanjem niste pronašli probleme, to ne znači da ih i nema.
- Ispitivanje samo povećava poverenje da problema ima u prihvatljivoj meri ili da se teško pronalaze.

16.2 Ispitivanje mogućnosti proboja

- Faze od kojih je sačinjen uobičajeni hakerski napad na računarsku mrežu:
  - Izviđanje
  - Popisivanje
  - Zadobijanje pristupa
  - Proširivanje ovlašćenja
  - Potkradanje
  - Prikrivanje tragova
  - Pravljenje zadnjih vrata
  - Uskraćivanje usluga (eventualno)

- Kao što ste mogli da primetite, deo o etičkom hakerisanju više se bavi etičkim i pravnim aspektima; ovde ćemo se uglavnom baviti metodologijom i postupcima ispitivanja.

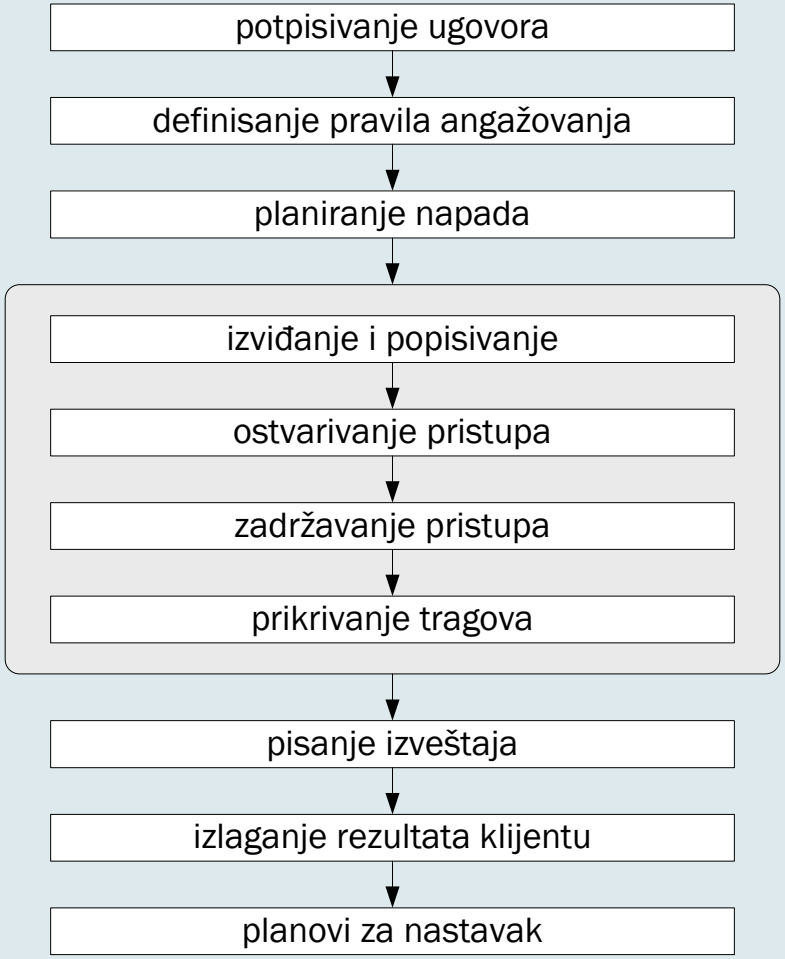
Ispitivanje mogućnosti proboja...

- Ispitivanje mogućnosti proboja (engl. *penetration testing*) - metoda ocenjivanja i provere sigurnosti računarske mreže simulacijom napada koji bi inače obavio zlonamerni haker.
- Obuhvata aktivnu analizu sistema u pogledu slabosti, tehničkih nedostataka i ranjivosti.
- Analiza se izvodi iz pozicije potencijalnog napadača – osoba koja obavlja ispitivanje sebe smešta u poziciju napadača i pokušava da prodre u mrežu i na taj način otkrije ranjivosti.
- Sve što se otkrije tokom ove analize, izlaže se vlasnicima sistema zajedno s procenom uticaja koji otkrivene ranjivosti mogu imati na sistem i predlogom tehničkih rešenja za uklanjanje ili smanjivanje uticaja otkrivenih ranjivosti.
- Testovi ove vrste treba da se sprovedu na svakom računarskom sistemu koji će biti postavljen u „neprijateljsko“ okruženje (naročito ako se računar postavlja na Internet), pre nego što se sistem tamo postavi.

Količina znanja o ciljnom sistemu

- Na osnovu količine znanja o ciljnom sistemu (ili mreži) koje je raspoloživo osobama koje vrše testiranje, testovi se mogu podeliti na ispitivanje
  - „bele kutije“ (engl. *white box*)
  - ispitivanje „crne kutije“ (engl. *black box*).
- Ispitivanje **crne kutije** podrazumeva da ispitivač nema prethodnog znanja o sistemu i infrastrukturi koja se testira. Ispitivanje **bele kutije** podrazumeva da se ispitivačima obezbeđuje kompletno znanje o infrastrukturi koja se testira, što obuhvata i mrežne dijagrame, izvorni kôd i informacije o IP adresiranju. Naravno, postoje i međuvarijacije koje se često zovu ispitivanja „**sive kutije**“ (engl. *grey box*).
- Umesto ovih termina mogu se koristiti i termini testovi s potpunim otkrivanjem (engl. *full disclosure*), delimičnim otkrivanjem (engl. *partial disclosure*) i takozvani testovi na „slepo“ (engl. *blind test*), koji odgovaraju ispitivanju bele, sive i crne kutije.

Osnovni koraci ispitivanja mogućnosti proboja



Priprema za ispitivanje

- Neophodno je da imate:
  - Tim
  - Potrebnu opremu i druge resurse
  - Vreme
- Potpisivanje ugovora
- Postavljanje (definisanje) pravila angažovanja
- Planiranje napada:
  - Okupljanje tima za ovu namenu
  - Izbor alata za ispitivanje
  - Planiranje strategije napada
    - Open-Source Security Testing Methodology Manual (OSSTMM)

Razmatranje pravnih i etičkih (moralnih) normi

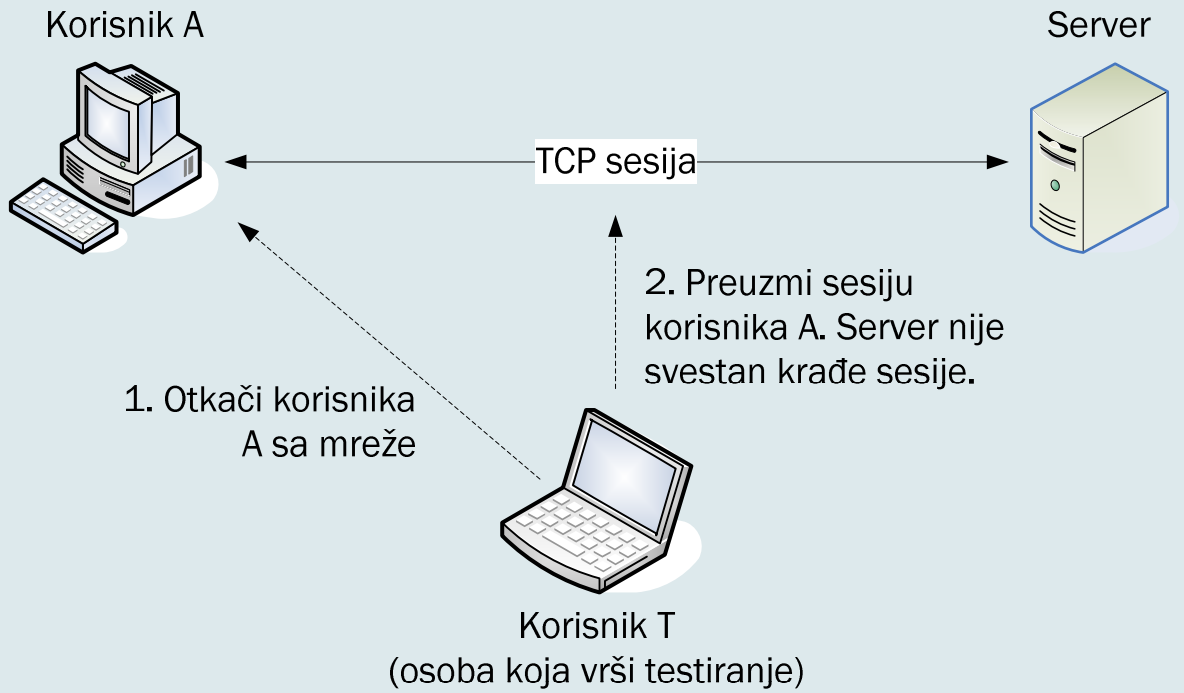
- Pomenuto u delu o etičkom hakerisanju, kao u poglavlju 14: Organizacione, fizičke i pravne metode zaštite, društveni aspekti

- Zakonska regulativa najdalje otišla u USA:
  - U.S. Code of Fair Information Practices (1973)
  - Computer Fraud and Abuse Act (CFAA, 1973)
  - U.S. Kennedy-Kasselbaum Health Insurance Portability and Accountability Act (HIPAA, 1996)
  - Graham-Leach-Bliley Act (GLBA, 2000)
  - USA PATRIOT Act (2001)
  - Federal Information Security Management Act (FISMA, 2002)
  - Sarbanes-Oxley Act (SOX, 2003)

Izvođenje ispitivanja

- Izviđanje i popisivanje
  - Pasivno izviđanje
  - Aktivno izviđanje
- Ostvarivanje pristupa
  - Krađa sesije (engl. *session hijacking*)
  - ... (nastavlja se)

Krađa sesije



Ostvarivanje pristupa – nastavak...

- Napadi na Web server
- Provaljivanje lozinki
  - Striktne mere kontrole pristupa obično su zasnovane na najmanje četiri elementa:
    - nešto što osoba zna (na primer, PIN broj ili lozinka)
    - nešto što osoba ima (na primer, sigurnosna identifikaciona kartica)
    - nešto što osoba jeste (biometrija zasnovana na fizičkim karakteristikama)
    - nešto što osoba radi (biometrija zasnovana na karakteristikama ponašanja)
- ... (nastavlja se)

Ostvarivanje pristupa – nastavak...

- Napadanje mreže
- Napadanje bežične mreže
- Probijanje UNIX, Linux i Windows servera
  - Povećanje privilegija
  - Skeneri za otkrivanje ranjivosti
  - Rootkit alati

Izvođenje napada - nastavak

- Održavanje pristupa
- Sakrivanje tragova

Pisanje izveštaja i ukazivanje na propuste

- Izveštaj
  - Izvršni rezime (engl. *executive summary*)
  - Obuhvat (opseg) projekta
  - Izvršena ispitivanja i rezultati
  - Sažetak izveštaja
  - Prilozi
- Ukazivanje na propuste i planovi za njihovo otklanjanje

Literatura

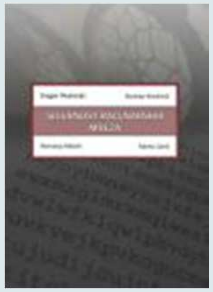
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

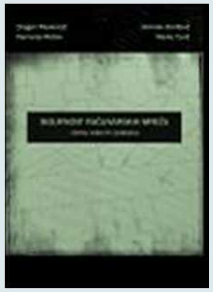
- Za predavanje 16:
  - Poglavlje 16: Etičko hakerisanje i ispitivanje mogućnosti proboja
  - Dodatak B: Besplatni i open-source alati i razni resursi koji se tiču sigurnosti

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Hacking Exposed: Network Security Secrets & Solutions**
  Prevod u izdanju Mikro knjige
  www.mikroknjiga.rs/store/prikaz.php?ref=86-7555-282-3

- **Penetration Testing and Network Defense**
  A. Whitaker, D. P. Newman
  Cisco Press, 2005.

- Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?