Centar Informacijske Sigurnosti

OSSTM metodologija

CIS-DOC-2011-04-011

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

OSSTMM (eng. *The Open Source*[1] *Security Testing Methodology Manual*) je metodološki priručnik za provođenje sigurnosnih testova i određivanje univerzalne sigurnosne metrike. Metodologija priručnika pokriva što, kada i kako testirati, besplatna je i slobodna za distribuciju pod *Open Methodology* (OML) licencom[2]. Sam priručnik je također besplatan za korištenje pod licencom *Creative Commons* 3.0. OSSTM sigurnosne revizije pokrivaju pet operacijskih kanala:

1. ljudski,
2. fizički,
3. bežični,
4. telekomunikacijski te
5. podatkovne mreže[3].

U kanalima se provjeravaju:

- podatkovne kontrole,
- razina svijesti osoblja o sigurnosti,
- razina prijevara i izloženost socijalnom inženjeringu,
- računalne i telekomunikacijske mreže,
- bežični uređaji,
- mobilni uređaji,
- fizičke sigurnosne kontrole pristupa,
- sigurnosni procesi te
- fizičke lokacije kao što su zgrade, vojne baze i sl.

Priručnik se bavi pitanjem operacijske sigurnosti (OpSec), odnosno pruža načine mjerenja kvalitete osiguranja poslovnih sustava. Iako se ovakav priručnik može činiti suvišnim jer većina ozbiljnih tvrtki već ima odjele koji se bave operacijskom sigurnošću, treba uočiti da većina sigurnosnih zahtjeva ne traži više od primjene najbolje prakse na poslovne procese i konfiguracije IT sustava. OSSTM traži da se prilikom testiranja ne pretpostavlja da će sigurnosna rješenja, proizvodi ili procesi u stvarnim slučajevima reagirati kao što bi trebali. Jednostavnije rečeno, ova metodologija će pokazati da li se ispitivani sustav ponaša stvarno onako kako vlasnik želi.

[1] *Open Source* neki smatraju filozofijom, a neki pragmatičnom metodologijom. Ideja je ta da su programska rješenja ovog tipa besplatno dostupna svima za preuzimanje, korištenje i razvijanje. Operacijski sustav Linux je primjer *open source* proizvoda naspram komercijalnog operacijskog sustava MS Windows.

[2] OML (eng. *Open Methodology Licence*) licenca je namijenjena zaštiti metodologija kao kompleksnih setova metoda, procesa i procedura koji će se primjenjivati u nekoj disciplini. Ključni zahtjevi licence su da metodologija ima vrijednost kao intelektualno vlasništvo kroz čiju se primjenu može proizvesti mjerljiva vrijednost, da je metodologija javno dostupna te da je uložen odgovarajući trud da metodologija bude transparentna svima.

[3] Podatkovna mreža (eng. *Data Network*) je mreža koja omogućava prijenos podataka među korisnicima. Česti slučaj je VPN (eng. *Virtual Private Network*), mreža na koju se korisnici mogu spojiti i s udaljene lokacije kako bi preuzeli sadržaj.

2. Nastanak OSSTM-a

Legenda kaže da je Pete Herzog dobio ideju o OSSTM-u putujući vlakom dok je pokušavao smisliti način kako testirati sigurnost u skladu sa znanstvenom metodom. Kad je sišao s vlaka, rekao je svojoj ženi: „Mislim da sam otkrio nešto veliko.“ Prva inačica priručnika objavljena je u siječnju 2001. godine i imala je 12 stranica (za usporedbu, OSSTM 3 ima 213 stranica).

OSSTM se fokusira na tehničke detalje područja koja trebaju biti testirana: što učiniti prije, tijekom i poslije sigurnosnog testiranja te kako kvantificirati rezultate. Priručniku se redovito dodaju novi testovi u skladu s međunarodnim najboljim praksama, zakonima, regulativama i etičkim pitanjima.

„U umjetnosti je krajnji rezultat predmet ljepote dok je u znanosti to način na koji se došlo do rezultata. Kada je sam test umjetnost onda su rezultati nedokazivi što potkopava vrijednost testa. Jedan način na koji se može osigurati da test ima vrijednost je osigurati da je on ispravno proveden. Da bi se to postiglo, potrebno je imati formalnu metodologiju. OSSTM teži da bude upravo to.“ - Pete Herzog, OSSTM 3

Kako bi osigurao da OSSTM ne poklekne komercijalnom utjecaju, Pete Herzog je osnovao ISECOM (eng. *The Institute for Security and Open Methodologies*) zajedno s Martom Barceló, uglednom fotografkinjom i računalnom znanstvenicom.

2.1. ISECOM

ISECOM (eng. *The Institute for Security and Open Methodologies*) je otvorena, neprofitna kolaborativna zajednica nastala u siječnju 2001. godine stvaranjem OSSTM-a. Posvećena je podizanju praktične svijesti o sigurnosti, istraživanju, certificiranju i poslovnom integritetu. ISECOM nudi certificiranje, obuku, usluge podrške nepristranih projekata, financijsku podršku projekata i infrastrukture neovisnih o dobavljaču (eng. *vendor-neutral*) kako bi pokazala da su im programi obuke, standardi i najbolje prakse uistinu neutralni od državnog i komercijalnog utjecaja.

Legenda se nastavlja, i kaže kako je brat Petea Herzoga kupio prvu domenu *ideahamster.org* na poklon Peteu dok ne uspije zaraditi za vlastitu domenu. Ime „*ideahamster*“ aludira na naviku hrčaka (eng. *hamster*) da skupljaju stvari – u ovom slučaju ideje (eng. *idea*). Upravo to im je bila i želja, skupljati izume orijentirane oko sigurnosti za *open source* zajednicu i nuditi informacije i alate pod otvorenim licencama.

Svojim istraživanjem žele omogućiti praktične metode i mjerenja sigurnosti te integriteta za svaku lokaciju, od sobe upravnih direktora do srednjoškolske učionice. ISECOM stoga usko surađuje sa školama, sveučilištima, tvrtkama i državnim agencijama kako bi osigurali da je svo istraživanje stručno recenzirano i vrhunske kvalitete.

2.2. Drugi projekti ISECOM-a[4]

Kako se svijet upoznavao s OSSTM-om, potraga za „česticom sigurnosti“ je počela rađati nove projekte. Neki od većih pothvata ISECOM-a opisani su u nastavku.

2.2.1. SCARE

Projekt SCARE [6] (eng. *Source Code Analysis Risk Evaluation*) ima za cilj stvoriti mjeru sigurnosti i kompleksnosti kojom bi se analizirao bilo kakav izvorni kôd, čime bi se dobio realističan i činjeničan prikaz vjerojatnosti da će taj kôd proizvesti problematičnu binarnu datoteku[5]. Krajnji rezultat predstavlja količinu kôda s nezaštićenim operacijama.

[4] Pojmovi iz OSSTMM-a korišteni u opisima navedenih projekata su objašnjeni u kasnijim poglavljima.

[5] Binarna datoteka (eng. *binary file*) je datoteka koja sadrži podatke u binarnom formatu (jedinice i nule) u svrhe pohranjivanja na računalu i procesiranja.

2.2.2. HSM

Projekt HSM [7] (eng. *Home Security Methodology and Vacation Guide*) koristi metode i metrike iz OSSTM priručnika kako bi se zaštitila i pojačala sigurnost doma. Krajnji rezultat je sigurniji i osiguraniji dom bez ograničenja na slobode ukućana.

2.2.3. HHS

HHS [8] (eng. *Hacker Highschool*) je oblik programa za povećanje svijesti o sigurnosti među tinejdžerima. Koristi OSSTM testiranja i istraživanja o analizi za prenošenje znanja i vještina kroz praktične lekcije i pristup testnoj mreži. Kroz lekcije se potiče dosjetljivost i kritičko razmišljanje.

2.2.4. BPP

BPP [9] (eng. *The Bad People Project*) je program podizanja svijesti o sigurnosti kod djece i roditelja. Korist OSSTM-ovu metriku Povjerenja kako bi kreirala bolja sigurnosna pravila za djecu kroz igru, priče i igranje uloga. Pravila su lakša za pamćenje, neopterećena kontradikcijama i kulturološki nepristrana. Roditelji mogu posjetiti galeriju i vidjeti dječje crteže koji pokazuju kako djeca zamišljaju „zločeste“ osobe te dodati crteže svoje djece. Ti crteži se koriste kako bi se lakše doprijelo do djece i usavršilo pravila kojima ih se uči.

2.2.5. SOMA

Projekt SOMA [10] (eng. *Security Operations Maturity Architecture*) ima za cilj omogućiti OSSTM operacijske procese na strateškoj razini. Koriste se ravi i metrika Povjerenja u određivanju zrelosti osiguranja provjeravajući način na koji zapravo funkcioniraju zaštitna strategija i taktika, a ne kako bi trebali funkcionirati prema pretpostavljenim pravilima.

2.2.6. BIT

Projekt BIT [11] (eng. *Business Integrity Testing*) proširuje OSSTM operacijsko testiranje i analizu na poslovne procese i transakcije. Time se pruža strateški pogled na sigurnost poslovnog ponašanja zaposlenika i na razvoj novih poslovnih planova.

2.2.7. Smarter Safer Better

Ovaj projekt pruža sigurnosne alate i vještine koje ljudi trebaju svaki dan za borbu protiv prevara, laži i obmana na Internetu. Alati su bazirani na ISECOM-ovom istraživanju usmjerenom na izbjegavanje uvjerljivih trikova i tehnika manipulacije. Projekt je jedinstven u načinu na koji iskorištava grupe podrške gdje se raspravlja o problemima koje su ljudi susreli te sudjeluje na njihovoj analizi [12].

2.2.8. Mastering Trust

Ovaj projekt se bavi kreiranjem materijala za seminare i radnih knjiga o načinu korištenja OSSTM-ove metrike Povjerenja u svakodnevnom životu za donošenje boljih odluka. Projekt se usmjerava na pitanje zašto je ljudski instinkt pogrešan i kako ga „popraviti“ [12].

3. OSSTM priručnik

„Ovaj priručnik pruža testne slučajeve koji kao rezultat daju ovjerene činjenice. Te činjenice prestavljaju podatke na temelju kojih se mogu donositi akcijske odluke te mogu značajno unaprijediti operacijsku sigurnost. Korištenjem OSSTM-a više se ne morate oslanjati na općenite najbolje prakse, rekla-kazala dokaze ili praznovjerja. Imati ćete ovjerene informacije specifične za vaše potrebe na temelju kojih možete donositi odluke po pitanju sigurnosti." - Pete Herzog, OSSTM 3.

Osnovna svrha priručnika je pomoću znanstvene metodologije preciznije okarakterizirati operacijsku sigurnost kroz ispitivanja i korelaciju rezultata na dosljedan i pouzdan način (objašnjeno u poglavlju 3.1). OSSTM priručnik se može prilagoditi gotovo svakom tipu revizije, uključujući penetracijska testiranja, etično hakiranje, procjene sigurnosti, procjene ranjivosti, simulacije crvenih i plavih timova[6] i slično.

Sekundarna svrha priručnika je pružiti smjernice koje, ako se ispravno slijede, omogućuju ispitivaču da obavi certificiranu OSSTM reviziju. Smjernice postoje kako bi osigurale sljedeće činjenice:

1. Testiranje je obavljeno temeljito.
2. Testiranje je uključilo sve potrebne kanale.
3. Testiranje je obavljeno u skladu sa zakonima.
4. Rezultati su kvantitativno mjerljivi.
5. Rezultati su dosljedni i ponovljivi.
6. Rezultati sadrže samo činjenice koje su prouzašle iz samih testova.

Neizravna korist priručnika je da se može koristiti za usporedbu kod svih sigurnosnih testova neovisno o veličini organizacije, tehnologiji ili zaštiti.

3.1. Operacijska sigurnost (OpSec)

Operacijska sigurnost je kombinacija odvajanja imovine koja se štiti od prijetnji te kontrola tih prijetnji. Da bi prijetnja bila efektivna, mora doći u izravnu ili neizravnu interakciju s imovinom. Odvojiti prijetnju od imovine znači sasvim izbjeći moguću interakciju. Stoga je moguće biti 100% osiguran, pod uvjetom da su prijetnja i imovina potpuno razdvojeni. U suprotnom, sigurnost je omogućena kontrolama stavljenima na imovinu ili stupnjem do kojeg je smanjen utjecaj prijetnje.

Na primjer, da bi osoba bila 100% sigurna da je neće udariti munja, mora se skloniti negdje gdje munja ne može prodrijeti – npr. duboko u planini. Prijetnje koje ne mogu biti sasvim odvojene od imovine koja se štiti moraju biti ublažene tako da njihova interakcija čini jako malo ili nimalo štete. U navedenom primjeru skrivanja od munje, ovo bi predstavljalo slučaj u kojem osoba ostaje u kući koja ima gromobran i ne prilazi prozorima i drugim otvorima. U kontekstu operacijske sigurnosti, **Osiguranje** predstavlja odvajanje imovine od prijetnje, a **Sigurnost** kontroliranje utjecaja prijetnje.

Da bi se bolje shvatilo kako OpSec može funkcionirati u operacijskoj okolini, mora se rastaviti na elemente. Ti elementi dopuštaju kvantitativno određivanje **Površine Napada** (eng. *Attack Surface*) koja zapravo predstavlja nedostatak potrebnih odvajanja i funkcionalnih kontrola koje postoje za taj **Vektor**, odnosno smjer interakcije. Ovakav pristup navodi na novi način gledanja na osiguranje i sigurnost te je potpuno sposoban dovesti do **Savršenog Osiguranja**, odnosno do ravnoteže (Tablica 1).

[6] *Red-teaming* i *blue-teaming* su pojmovi preuzeti iz vojne terminologije. Jedna ekipa (npr. crveni) simulira napadače dok druga (plavi) ima za zadatak obranu. Za razliku od ostalih revizija i testiranja, u ovom slučaju se nikome ne govori da je posrijedi testiranje kako bi se dobila što realnija slika stanja sustava.

Pojam	Objašnjenje
Površina napada (eng. *Attack Surface*)	Nedostatak razdvajanja i funkcionalnih kontrola koje postoje za dotični vektor.
Vektor napada (eng. *Attack Vector*)	Podskup vektora stvoren kako bi se sigurnosnom testiranju kompleksnog skupa pristupilo na organizirani način. Algoritam je baziran na paradigmi „podijeli pa vladaj“. Drugim riječima, rekurzivno se razbija problem na 2 ili 3 podproblema istog ili sličnog tipa dok oni ne postanu dovoljno jednostavni da ih se direktno riješi.
Kontrole (eng. *Controls*)	Kontrole za smanjenje udara i gubitaka. Osiguranje da su fizička i podatkovna imovina te kanali komunikacije zaštićeni od raznih tipova neispravnih (po pravilima kanala) interakcija. Npr. osiguranje od požara ne može spriječiti štetu na imovini, ali će isplatiti naknadu. Kontrole su podijeljene na 10 tipova razvrstanih u 2 klase, A – kontrole interakcije i B – proceduralne kontrole.
Ograničenja (eng. *Limitations*)	Trenutno stanje zamijećenih i poznatih granica kanala komunikacije, operacija i kontrola, potvrđeno revizijom (eng. *audit*). Tipovi ograničenja se klasificiraju po tome kako međudjeluju sa sigurnošću i osiguranjem na operacijskoj razini. Prilikom klasifikacije ne koriste se subjektivne pretpostavke. Npr. stara hrđava brava kojom se osiguravaju vrata trgovine ima nametnuto sigurnosno ograničenje koje pruža tek djelić snage potrebne da se odgodi ili izdrži napad. Određivanje da je brava stara i slaba kroz vizualnu potvrdu se naziva identificiranim ograničenjem. Određivanje da je brava stara i slaba korištenjem 100 kg sile, gdje je potrebno izdržati 1000 kg da bi obrana bila uspješna, je potvrđeno ograničenje. Ono se zatim klasificira u kategoriju s obzirom na posljedicu operacijske akcije – što je u slučaju mogućnosti provale u trgovinu Pristup (eng. *Access*).
Operacije (eng. *Operations*)	Operacije su nužan nedostatak osiguranja koji mora postojati da bi komunikacija bila interaktivna, korisna, javna, otvorena ili dostupna. Npr. ograničavanje trgovine na jedna vrata za ulaz i izlaz je metoda osiguranja unutar operacija trgovine.
Savršeno Osiguranje (eng. *Perfect Security*)	Potpuna ravnoteža Osiguranja i Kontrola s jedne te Operacija i Ograničenja s druge strane.
Poroznost (eng. *Porosity*)	Predstavlja sve točke i operacije interakcije. Kategorije Poroznosti su Vidljivost (eng. *Visibility*), Pristup (eng. *Access*) i Povjerenje (eng. *Trust*).
Sigurnost (eng. *Safety*)	Oblik zaštite u kojem su prijetnja ili efekti prijetnje pod kontrolom. Da bi se imovina mogla smatrati sigurnom, kontrole moraju biti funkcionalne kako bi osigurale da su prijetnja ili utjecaji prijetnje minimizirani na razinu prihvatljivu za vlasnika ili upravitelja imovine. U priručniku je sigurnost predstavljena kroz kontrole kao sredstva ublažavanja napada.
Osiguranje (eng. *Security*)	Oblik zaštite gdje se imovina odvaja od prijetnje. To podrazumijeva, između ostalog, eliminaciju ili imovine ili prijetnje. Da bi se smatrala osiguranom, imovina se uklanja od prijetnje ili se prijetnja uklanja od imovine.
Rav	Rav je mjera površine napada, količina nekontroliranih interakcija s metom, izračunata preko ravnoteže Poroznosti, Ograničenja i Kontrola. U ovoj skali, 100 rava (ili 100% rava) predstavlja savršenu ravnotežu. Manje od toga znači da je premalo kontrola te je površina za napad veća. Više od toga znači prevelik broj kontrola što može predstavljati problem jer više kontrola znači povećanu kompleksnost i više problema s održavanjem.
Meta (eng. *Target*)	Područje koje se napada. Sačinjena od imovine i zaštita na imovini.
Vektor (eng. *Vector*)	Smjer interakcije prijetnje i imovine.

Tablica 1. *Popis pojmova korištenih u priručniku*

3.1.1. Osiguranje

Kao što je već spomenuto, osiguranje je funkcija razdvajanja imovine i prijetnje. Odvojenost ili postoji ili ne postoji. Postoje 3 proaktivna načina za postizanje razdvojenosti. To su:

1. uklanjanje imovine kako bi se stvorila fizička ili logička pregrada od prijetnji,
2. pretvaranje prijetnje u bezopasno stanje ili
3. uništavanje prijetnje.

Prilikom analize sigurnosti, može se primjetiti gdje postoji, a gdje ne postoji mogućnost interakcije. Od tih interakcija sam neke, sve ili možda nijedna nije potrebna za uspješno izvršavanje operacija. Npr. od svih ulaznih vrata u poslovnu zgradu, neka su za klijente, a neka za zaposlenike. No svaka vrata su točke interakcije koje povećavaju broj i željenih i neželjenih operacija kao što je krađa. Činjenica da ispitivač možda ne zna svrhu svih točaka interakcija ovo čini **Poroznost** u osiguranju. Poroznost predstavlja smanjenu mogućnost odvajanja prijetnji i pristupnih točaka. Dijeli se u 3 kategorije (Tablica 2): Vidljivost (eng. *Visibility*), Pristup (eng. *Access*) ili Povjerenje (eng. *Trust*). Kategorija poroznosti određuje funkciju u operacijama, čime se mogu odrediti koje kontrole su potrebne u poboljšavanju zaštite.

Dakle, ako postoji odvojenost od prijetnji kao što je čovjek skriven od munje u planini, onda je osiguranje 100% uspješno. Za svaku rupu u planini, svaku mogućnost da munja ozlijedi čovjeka, poroznost se povećava kao Pristup. Svaka točka interakcije smanjuje postotak uspješnosti osiguranja. Stoga, povećanje poroznosti smanjuje osiguranje, a svaka „pora“ je Pristup, Vidljivost ili Povjerenje.

Kategorija	Definicija
Vidljivost (eng. *Visibility*)	Policija navodi „priliku“ kao jedan od 3 elementa koji potiču krađu, zajedno s „dobiti“ i „smanjenim rizikom“. Vidljivost je način izračunavanja prilike. To je sva moguća imovina mete. Nepoznata imovina je samo u opasnosti od toga da bude otkrivena naspram mogućnosti da bude naciljanja.
Pristup (eng. *Access*)	S obzirom da je osiguranje odvajanje imovine i prijetnje, tada izravna interakcija s imovinom znači pristup imovini. Pristup se računa preko broja različitih točaka gdje može doći do interakcije. Uklanjanje izravne interakcije s imovinom će prepoloviti broj načina na koji se može ukrasti.
Povjerenje (eng. *Trust*)	Povjerenje kao dio operacijske sigurnosti se gleda kao svaki postojeći odnos ondje gdje meta otvoreno prihvaća interakcije od druge mete unutar opsega napada. Iako povjerenje može biti rupa u sigurnosti, često se koristi kao zamjena za autentikaciju te racionalni i ponovljivi način procjenjivanja odnosa. Dakle, preporuča se korištenje metrike Povjerenja u svrhu računanja pouzdanosti povjerenja.

Tablica 2. *Kategorije poroznosti*

3.1.2. Kontrole

Da bi imovina stvarno bila sigurna, potrebni su različiti tipovi kontrola. No, s obzirom da kontrole istovremeno povećavaju broj mogućih interakcija, odnosno površinu za napad, preporuča se koristiti različite tipove kontrola radije nego samo više njih. Potrebno je kategorizirati kontrole po njihovim funkcijama u operacijama kako bi bilo jasno koliko zaštite pružaju.

„Samo zato što nemaš direktnu kontrolu nad nečim ne znači da se time ne može upravljati. Kontroliraš li okolinu, kontroliraš sve u njoj.“ - Pete Herzog, OSSTM 3

- **KONTROLE INTERAKCIJA**

  Kontrole interakcija čine klasu A i pola svih operacijskih kontrola. One direktno utječu interakcije koje se tiču vidljivosti, pristupa i povjerenja. Kategorije klase A su:

  1. **Autentikacija** (eng. *authentication*) ispituje osobne podatke pojedinca bazirano na identifikaciji i autorizaciji.
  2. **Odšteta** (eng. *indemnification*) je kontrola kroz ugovor između vlasnika imovine i stranke u interakciji. Ugovor može biti u obliku vidljivog upozorenja na zakonske mjere koje će biti poduzete ako se pravila ne poštuju - konkretna i javna zakonska zaštita ili s neovisnim pružateljem osiguranja u slučaju štete.
  3. **Otpornost** (eng. *resilience*) je kontrola svih interakcija kako bi se održala zaštita imovine u slučaju kvara ili pogreške.
  4. **Pokoravanje** (eng. *subjugation*) je kontrola koja osigurava da se interakcije odvijaju isključivo slijedeći proces kojeg je vlasnik definirao. Vlasnik imovine određuje kako će se intarakcije odvijati čime se uklanja sloboda izbora, ali i odgovornost stranke u interakciji ako dođe do gubitka.
  5. **Kontinuiranost** (eng. *continuity*) je kontrola svih interakcija kako bi se održala dostupnost imovine u slučaju kvara ili pogreške.

- **KONTROLE PROCESA**

  Drugi dio operacijskih kontrola sačinjavaju klasu B i koriste se za stvaranje obrambenih procesa. Ove kontrole ne utječu direktno na interakcije već štite dobra kad je prijetnja već prisutna. Kategorije klase B su:

  6. **Neporecivost** (eng. *non-repudiation*) sprečava stranku u interakciji da porekne svoju ulogu u bilo kojoj aktivnosti.
  7. **Povjerljivost** (eng. *confidentiality*) je kontrola kojom se osigurava da se imovina koja se prikazuje ili izmjenjuje među strankama u interakciji ne može obznaniti drugim strankama.
  8. **Privatnost** (eng. *privacy*) osigurava da se način na koji je imovini pristupljeno, na koji je prikazana ili izmjenjena među strankama ne može obznaniti drugim strankama.
  9. **Cjelovitost** (eng. *integrity*) osigurava da stranke u interakciji znaju kad su se imovina i procesi promijenili.
  10. **Alarm** (eng. *alarm*) je kontrola koja upozorava da se interakcija odvija ili se dogodila.

3.1.3. Ograničenja

Nemogućnost funkcioniranja zaštitnih mehanizama znači da su oni ograničeni. Stoga se stanje sigurnosti u odnosu na poznate pogreške i ograničene mogućnosti zaštite unutar operacijskog opsega u OSSTM priručniku naziva Ograničenjem. Ograničenja su podijeljena u 5 kategorija koje određuju tip ranjivosti, greške ili krive konfiguracije. Kategorije su:

1. **Ranjivost** (eng. *Vulnerability*) - nedostatak ili greška koja:
    a. onemogućava pristup imovini autoriziranim korisnicima ili procesima,
    b. dopušta povlašteni pristup imovini neautoriziranim korisnicima ili procesima ili
    c. dopušta neautoriziranim korisnicima ili procesima da sakriju imovinu ili svoju prisutnost unutar operacijskog opsega.
2. **Slabost** (eng. *Weakness*) - nedostatak ili greška koja remeti, smanjuje, zloupotrebljava ili poništava efekte pet interaktivnih kontrola: autentikacije, odštete, otpornosti, pokoravanja i kontinuiranosti.
3. **Zabrinutost** (eng. *Concern*) - nedostatak ili greška koja remeti, smanjuje, zloupotrebljava ili poništava tok izvršavanja pet kontrola procesa: neporecivost, povjerljivost, privatnost, cjelovitost i alarm.
4. **Izloženost** (eng. *Exposure*) - neopravdana akcija, nedostatak ili greška koja omogućuje izravnu vidljivost mete ili imovine unutar kanala odabranog opsega.
5. **Anomalija** (eng. *Anomaly*) - bilo koji neodredivi ili nepoznati element koji nije pod kontrolom i čije se ponašanje u normalnim operacijama ne može predvidjeti.

Tablica 3 prikazuje način na koji su Ograničenja povezana s operacijskom sigurnosti.

<table>
<tr><th colspan="2">Kategorija</th><th>Komponenta OpSec-a</th><th>Ograničenje</th></tr>
<tr><td colspan="2" rowspan="3">Operacije</td><td>Vidljivost (eng. visibility)</td><td>Izloženost (eng. exposure)</td></tr>
<tr><td>Pristup (eng. access)</td><td rowspan="2">Ranjivost (eng. vulnerability)</td></tr>
<tr><td>Povjerenje (eng. trust)</td></tr>
<tr><td rowspan="10">Kontrole</td><td rowspan="5">Klasa A – interaktivne</td><td>Autentikacija (eng. authentication)</td><td rowspan="5">Slabost (eng. weakness)</td></tr>
<tr><td>Odšteta (eng. indemnification)</td></tr>
<tr><td>Otpornost (eng. resilience)</td></tr>
<tr><td>Pokoravanje (eng. subjugation)</td></tr>
<tr><td>Kontinuiranost (eng. continuity)</td></tr>
<tr><td rowspan="5">Klasa B – procesi</td><td>Neporecivost (eng. non-repudiation)</td><td rowspan="5">Zabrinutost (eng. concern)</td></tr>
<tr><td>Povjerljivost (eng. confidentiality)</td></tr>
<tr><td>Privatnost (eng. privacy)</td></tr>
<tr><td>Cjelovitost (eng. integrity)</td></tr>
<tr><td>Alarm (eng. alarm)</td></tr>
<tr><td colspan="4">Anomalije (eng. anomalies)</td></tr>
</table>

Tablica 3. *Prikaz smještaja Ograničenja u kompleksu operacijske sigurnosti*

3.2. Pripremanje revizije

3.2.1. Definiranje testa sigurnosti

Da bi se propisno definirao test sigurnosti, potrebno je proći sljedećih 7 koraka:

1. Definirati što se želi zaštititi. To je imovina (eng. *assets*). Mehanizmi zaštite imovine su **Kontrole** kojima će se ustanoviti **Ograničenja**.
2. Identificirati područje oko imovine koje uključuje zaštitne mehanizme i procese ili usluge izgrađene oko imovine. Tu će se odvijati interakcija s imovinom. To se smatra **zonom susreta** (eng. *Engagement Zone*).
3. Definirati sve oko zone susreta što je potrebno da bi imovina ostala operativnom. To može uključivati stvari izvan kontrole pojedinca kao što su struja, hrana, voda, zrak, stabilna podloga, informacije, zakonodavstvo, pravila i stvari na koje se može utjecati kao što su suhoća, toplina, hladnoća, bistrina, izvođači radova, kolege, stvaranje brenda, partnerstva itd. Također treba uzeti u obzir stvari koje održavaju infrastrukturu operativnom kao što su procesi, protokoli i kontinuirani resursi. To sve se smatra **opsegom**.
4. Definirati unutarnje i vanjsko međudjelovanje opsega. Logički podijeliti imovinu unutar opsega po smjeru interakcija – iznutra prema van, izvana prema unutra, iznutra prema unutra, odjel A prema odjelu B itd. To su **vektori**. Svaki vektor bi idealno trebalo testirati odvojeno kako bi se za vrijeme testiranja promijenilo što manje utjecaja u okolini.
5. Identificirati opremu koja će biti potrebna za svaki test. Unutar svakog vektora, na raznim razinama, se mogu odvijati interakcije. Te razine se mogu klasificirati na mnoge načine, no po funkciji su podijeljene na 5 **kanala**. To su Ljudski, Fizički, Bežični, Telekomunikacijski i Podatkovne Mreže (Tablica 4). Svaki kanal se mora odvojeno testirati za svaki vektor.
6. Odrediti koji podaci se žele otkriti ispitivanjem. Hoće li se ispitati interakcije s imovinom ili i reakcije aktivnih sigurnosnih mjera? **Tip testa** mora biti pojedinačno određen za svaki test. Šest je standardnih tipova: Slijepi (eng. *Blind*), Dvostruki Slijepi (eng. *Double Blind*), Siva kutija (eng. *Gray Box*), Dvostruka Siva Kutija (eng. *Double Gray Box*), Serijski (eng. *Tandem*) i Preokret (eng. *Reversal*).
7. Uvjeriti se da je definirani test sigurnosti u skladu s Pravilima Odnosa (eng. *Rules of Engagement*), smjernicama za osiguravanje procesa ispravnog sigurnosnog testiranja bez izazivanja nesporazuma, zabluda ili lažnih očekivanja.

3.2.2. Kanali interakcija

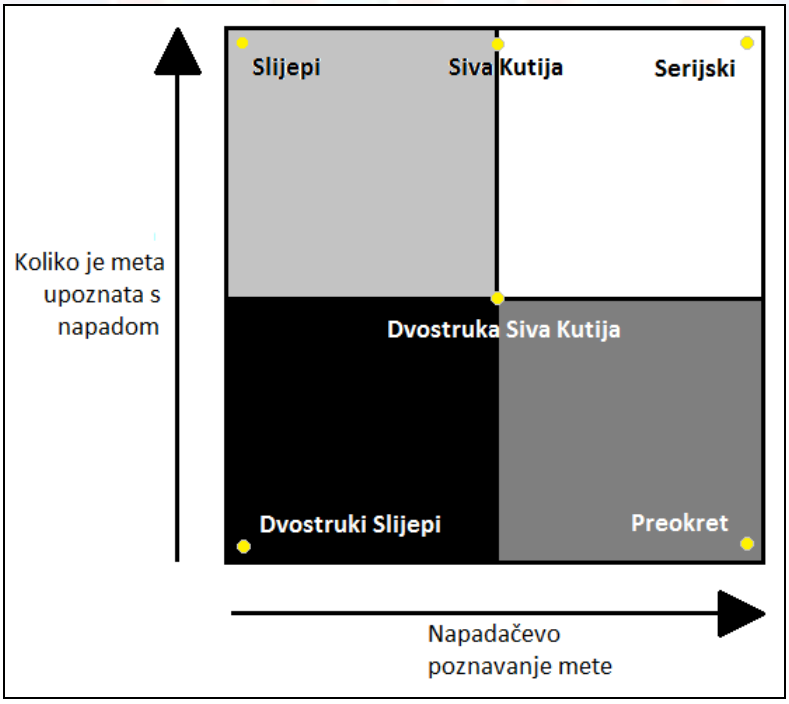
Iako se kanali i njihove podjele mogu predočiti na bilo koji način, u ovom priručniku su organizirani kao prepoznatljivi načini komunikacije i interakcije. Takvo uređenje je osmišljeno da se ubrzaju testni procesi dok se minimizira neefikasni višak operacija često povezan sa strogim metodologijama.

Klasa	Kanal	Opis
Fizička sigurnost (eng. *Physical Security* – PHYSSEC)	Ljudski	Sačinjava ljudski element komunikacije gdje su interakcije fizičke ili psihičke.
	Fizički	Fizičko testiranje sigurnosti gdje je kanal i fizički i ne-električan po prirodi. Sačinjava opipljivi element sigurnosti gdje je za interakciju potreban fizički trud ili odašiljač električne energije kojim se može upravljati.
Sigurnost spektra (eng. *Spectrum Security* – SPECSEC)	Bežični	Sačinjava sve elektronske komunikacije (ELSEC), signale (SIGSEC) i zračenja (eng. emanations – EMSEC) u poznatom elektromagnetskom spektru.
Sigurnost komunikacija (eng. *Communications Security* – COMSEC)	Telekomunikacije	Sačinjava sve telekomunikacijske mreže, digitalne i analogne, u kojima se interakcija odvija preko telefonskih i sličnih mrežnih linija.
	Podatkovne mreže	Sačinjava sve elektroničke sustave i podatkovne mreže u kojima se interakcija odvija putem postavljenog kabla i žičanih mrežnih linija.

Tablica 4. *Podjela kanala interakcija*

3.2.3. Tipovi sigurnosnih revizija

Kao što je već spomenuto, 6 je najčešćih tipova sigurnosnih testova koji se razlikuju po tome koliko ispitivač zna o meti, koliko meta zna o testu te o zakonitosti testa. Valja obratiti pažnju na to da prilikom izvještavanja o reviziji treba spomenuti i tip poduzete revizije. Ukoliko nije spomenut tip, osoba koja pregledava izvještaj bi trebala smatrati da je test bio Slijepog tipa – s najmanje podataka o spremnosti i stanju mete.



Slika 1. *Najčešća klasifikacija tipova testova*

Šest najčešćih tipova testiranja su:

1. **Slijepi** (eng. *Blind*)

   Analitičar pristupa meti bez prethodnog poznavanja njenih obrana, imovine ili kanala. Meta je spremna za reviziju i unaprijed je upoznata sa svim detaljima testa. Slijepa revizija primarno testira vještine analitičara. Širina i dubina slijepe revizije je onolika koliko dopušta primjenjivo znanje i efikasnost analitičara. Po pitanju sigurnosti spektra i komunikacija, ovaj tip ispitivanja se često naziva Etičnim Hakiranjem, a u fizičkoj sigurnosti **Ratnim igrama** (eng. *War Gaming*) ili **Igranjem Uloga** (eng. *Role Playing*).

2. **Dvostruki Slijepi** (eng. *Double Blind*)

   Analitičar pristupa meti bez prethodnog poznavanja njenih obrana, imovine ili kanala. Meta nije obavještena o reviziji ni o njenom opsegu, ispitivanim kanalima i vektorima. Dvostruka Slijepa revizija testira vještine analitičara kao i spremnost mete na nepoznate načine uznemiravanja. Širina i dubina bilo koje slijepe revizije ovisi o primjenjivom znanju i efikasnosti analitičara. Ovakav tip testa se još zove i **Test Crne Kutije** (eng. *Black Box test*) te **Penetracijski Test** (eng. *Penetration test*).

3. **Siva Kutija** (eng. *Gray Box*)

   Analitičar pristupa meti s ograničenim poznavanjem njenih obrana i imovine te s potpunim poznavanjem kanala. Meta je spremna za test i zna sve detalje testa unaprijed. Ovaj tip revizije testira vještine analitičara. Poanta testa je u efikasnosti. Širina i dubina revizije ovise o kvaliteti podataka danima analitičaru prije početka testa kao i o primjenjivom znanju analitičara. Drugi naziv je **Testiranje Ranjivosti** (eng. *Vulnerability Test*) i često ga traže same mete kao oblik procjene vlastitog stanja.

4. **Dvostruka Siva Kutija** (eng. *Double Gray Box*)

   Analitičar pristupa meti s ograničenim poznavanjem njenih obrana i imovine te s potpunim poznavanjem kanala. Meta je unaprijed upoznata s opsegom i o vremenu testiranja, ali ne i s ispitivanim kanalima i vektorima. Ovaj tip revizije testira vještine analitičara kao i spremnost mete na nepoznate načine uznemiravanja. Širina i dubina revizije ovise o kvaliteti podataka danima analitičaru prije početka testa kao i o primjenjivom znanju analitičara. Drugi naziv je **Test Bijele Kutije** (eng. *White Box test*).

5. **Serijski** (eng. *Tandem*)

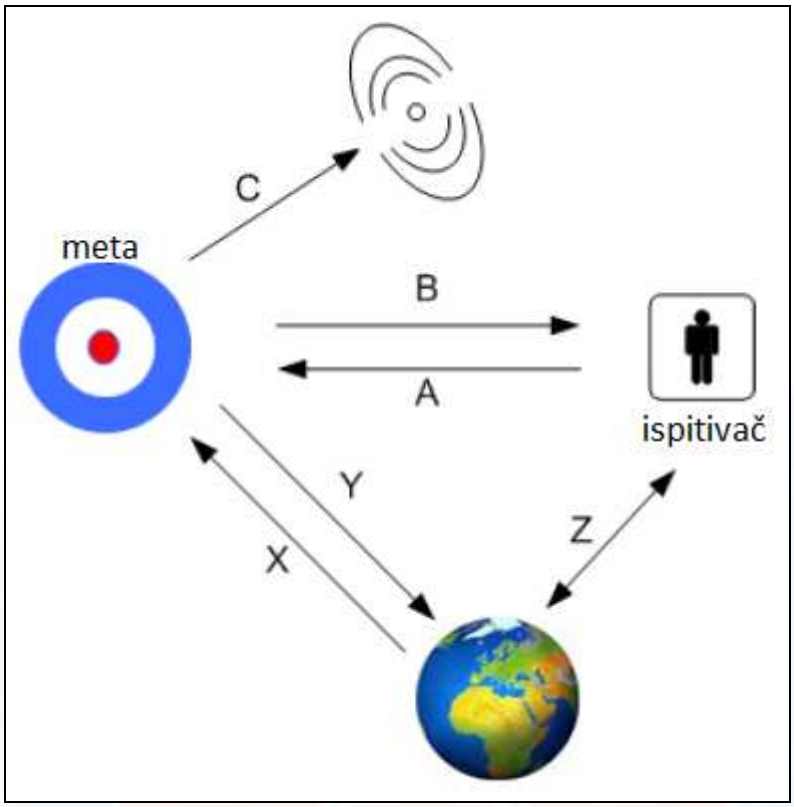
   I analitičar i meta su posve upoznati sa svim detaljima revizije. Serijska revizija provjerava zaštitu i kontrole mete, no ne može testirati spremnost mete na nepoznate varijable napada. Poanta testa je u temeljitosti analitičara s obzirom da ima sve podatke o testovima i njihove rezultate. Širina i dubina revizije ovise o kvaliteti podataka danima analitičaru prije početka testa (transparentnost) kao i o primjenjivom znanju analitičara. Drugi naziv je ***In-House*** **Revizija** ili **Test Kristalne Kutije** (eng. *Crystal Box test*), a analitičar je često dio sigurnosnog procesa.

6. **Preokret** (eng. *Reversal*)

   Analitičar pristupa meti potpuno upoznat s procesima i operacijskom sigurnošću mete, ali meta ne zna što, kako ni kada će se test provoditi. Poanta testa je provjera pripravnosti mete na nepoznate varijable i vektore napada. Širina i dubina revizije ovise o kvaliteti podataka danima analitičaru prije početka testa kao i o primjenjivom znanju i kreativnosti analitičara. Drugi naziv za ovaj tip testa je **Vježba Crvenog Tima** (eng. *Red Team exercise*).

3.2.4. Proces Četiri Točke

Proces Četiri Točke (eng. *The Four Point Process*) ili 4PP razbija proces testiranja na djeliće od početka do kraja. Iskusni testni timovi već koriste ovaj proces. U izvještaju nije potrebno navoditi svaki korak testa, ali je potrebno razumjeti kako se došlo do pojedinih nalaza.



Slika 2. *Interakcije Procesa 4 Točke*

Koraci 4PP su:

1. **Indukcija** (eng. *induction*) – Z

   Utvrđivanje osnovnih istina o meti iz zakona i činjenica. Analitičar određuje principe rada s metom ovisno o okolini u kojoj se meta nalazi (država, grad). Pošto će okolina utjecati na metu, njeno ponašanje se može odrediti kroz taj utjecaj. U slučaju gdje okolina ne utječe na metu postoji anomalija koju treba razmotriti.

2. **Istraga** (eng. *inquest*) – C

   Istraživanje bežičnog zračenja mete. Analitičar istražuje zračenja mete i sve tragove ili pokazatelje zračenja. Sustav ili proces će standardno ostaviti svoj potpis prilikom interakcija s okolinom.

3. **Interakcija** (eng. *interaction*) – A / B

   Standardne i nestandardne interakcije s metom koje izazivaju odgovore. Analitičar će se informirati ili će sam izazvati metu da mu pošalje odgovore kako bi ih analizirao.

4. **Intervencija** (eng. intervention) – X / Y / Z

   Mijenjanje resursnih interakcija s metom ili među metama. Analitičar će mijenjati dostupnost resursa iz okoline i s drugih lokacija koje su potrebne meti kako bi provjerio ekstremne uvjete u kojima je meta može funkcionirati.

4. Certificiranje

ISECOM nudi mogućnost izlaska svojih stručnjaka na teren i sudjelovanje u treninzima i ispitnim procesima na nepristranim lokacijama. Zadatak stručnjaka je da provjere da su ispitna pitanja dovoljno stručna kao i da se ocjenjivanje provodi nepristrano.

ISECOM certifikati su prestižne potvrde o vještinama i znanju pojedinca. Certficirane osobe čine dio elitne grupe sigurnosnih profesionalaca koji su na nekoliko načina dokazali da su etični, obrazovani i snalažljivi za testiranje i analizu sustava. Certificiranje zahtjeva od profesionalaca sposobnost da sagledaju cijelu sliku, često na međunarodnoj razini, što uključuje poznavanje sigurnosnih zakona i zakona o privatnosti različitih država. A međunarodno iskustvo je vrlo tražena vještina među organizacijama koje prelaze granice jedne države.

Tvrtkama revizija certificirana OSSTMod ISECOM-a pruža sljedeće koristi:

- dokaz da je obavljen test na temelju konkretnih činjenica,
- analitičar koji je izveo test se smatra odgovornim za njega,
- klijenti imaju jasnu sliku rezultata,
- lakše se shvaća ovakav pregled nego sažeci izvršnog osoblja i
- uvodi se razumljiva metrika.

4.1. Certifikati za pojedince

Bilo tko može provesti OSSTM reviziju ako koristi metodologiju za testiranje sigurnosti i analizu te ako popuni odgovarajući STAR izvještaj (poglavlje 4.2). No dostupna je i ISECOM certifikacija za primjenjive vještine individualaca u profesionalnom testiranju sigurnosti, analizi, metodičnim procesima i profesionalnim standardima. Obrazovanje i službeni ispiti su dostupni kod ovlaštenih partnera u raznim dijelovima svijeta. Trenutno dostupni certifikati su:

- **OPST** (eng. *OSSTM Professional Security Tester*)

  Potvrđuje da pojedinac ima vještine i znanje za izvođenje precizne i efikasne revizije sigurnosti u podatkovnim mrežama.
- **OPSA** (eng. *OSSTM Professional Security Analyst*)

  Potvrđuje se da pojedinac može precizno i efikasno primjeniti principe sigurnosne analize i metriku površine za napad (eng. *attack surface*).
- **OPSE**(eng. *OSSTM Professional Security Expert*)

  Potvrđuje da je pojedinac naučio sve koncepte sigurnosti iz aktualnog, javno dostupnog OSSTM priručnika te da je savladao podlogu istraživanja.
- **OWSE** (eng. *OSSTM Wireless Security Expert*)

  Potvrđuje da pojedinac ima vještine i znanje za preciznu i efikasnu analizu i testiranje operacijske sigurnosti bežičnih tehnologija cijelog elektromagnetnog spektra.
- **CTA** (eng. *Certified Trust Analyst*)

  Potvrđuje da pojedinac ima vještine i znanje da efikasno procjeni karakteristike povjerenja pojedinih osoba, lokacija, predmeta, sustava i procesa te da precizno i efikasno donosi odluke o povjerenju.

4.2. Certifikati za tvrtke

Osim certifikata za pojedince, ISECOM nudi i certificiranje tvrtki, infrastruktura i proizvoda. Dostupni certifikati su:

- **STAR** (eng. *Security Test Audit Report*)

  STAR je izvještaj o reviziji sigurnosti u skladu s OSSTM metodologijom. OSSTM certifikati su dostupni tvrtkama ili dijelovima tvrtki koji ovjeravaju svoju sigurnost STAR

izvještajem. Ovjeravanje testova sigurnosti je podložno ISECOM-ovim zahtjevima što osigurava visoku razinu pouzdanosti tvrtke.

Security Test Audit Report
OSSTMM 3.0 Security Verification Certification
OSSTMM.ORG - ISECOM.ORG

Report ID		Date	
Lead Auditor		Test Date Duration	
Scope and Index		Vectors	
Channels		Test Type	

I am responsible for the information within this report and have personally verified that all information herein is factual and true.

SIGNATURE	COMPANY STAMP/SEAL

OPST Certification #		OPSA Certification #	

OPERATIONAL SECURITY VALUES		CONTROLS VALUES	
Visibility		Authentication	
Access		Indemnification	
Trust		Resilience	
		Subjugation	
LIMITATIONS VALUES		Continuity	
Vulnerability		Non-Repudiation	
Weakness		Confidentiality	
Concern		Privacy	
Exposure		Integrity	
Anomaly		Alarm	
OpSec		True Controls	
Limitations		Security Δ	

True Protection		Actual Security	

Slika 3. *STAR izvještaj o reviziji sigurnosti*
izvor: *ISECOM*

- **ILA** (eng. *ISECOM Licensed Auditors*)

  Revizori s ISECOM licencom su oni koji su dokazali da imaju sposobnosti i kapacitete izvoditi OSSTM revizije sebi i drugima. To pruža jednostavan i efikasan način za održavanje STAR izvještaja u skladu s vremenima u kojima se testovi provode i njihovo certificiranje od strane ISECOM-a.

- **OSSTM Seal of Approval**

  OSSTM evaluacijski pečati se mogu koristiti za proizvode, usluge ili poslovne procese. Ovaj pečat predstavlja operacijsko stanje sigurnosti, osiguranja, povjerenja i privatnosti. Uspješno ocjenjeni proizvodi, usluge i procesi nose sa sobom pečat i rezultat procjene u ravima. Na taj način kupci mogu vidjeti količinu i različite tipove sigurnosti predstavljenih rješenja.

Slika 4. *OSSTM pečat odobrenja*

5. Usporedba s drugim metodologijama

U području testiranja sigurnosti, OSSTM nikako nije jedina metodologija dostupna javnosti. Ono što je čini drugačijom od drugih je to što cijeli postupak testiranja dijeli na komadiće kako bi se lakše vidjela cijela slika. Za razliku od ovog pristupa, drugi se priručnici više usmjeravaju na konkretne alate, pravila i primjere iz prakse. Slijede opisi nekih od zastupljenijih metodologija u području testiranja sigurnosti.

5.1. NIST: Computer Security

Ovaj priručnik [13] je preporučen od američkog Nacionalnog Instituta za Standarde i Tehnologiju (NIST). Riječ je o 90-ak stranica s opisom koraka za ispitivanje mrežne sigurnosti. Priručnik pokriva:

- uloge i odgovornosti pojedinaca prilikom testiranja,
- skeniranje mreže,
- skeniranje ranjivosti,
- probijanje lozinki,
- pregledavanje dnevničkih datoteka,
- alate za utvrđivanje cjelovitosti datoteka,
- detektore virusa,
- *war dialing*[7],
- testiranje bežičnih mreža (tzv. *war driving*),
- penetracijska testiranja,
- akcije nakon testa te
- općenite principe infomacijske sigurnosti.

Uz konkretne upute o postupcima, na kraju priručnika se nalazi popis određenog broja dostupnih alata za operacijske sustave Windows, Unix/Linux i Mac OS te kratki opisi njihovog načina rada i funkcija.

Za razliku od OSSTM-a, ovaj priručnik se bavi samo mrežnom sigurnošću. Osim po sadržaju, razlikuju se i po tome što OSSTM daje detaljne upute o tome kako pristupiti pojedinom problemu, odnosno više je nalik metodologiji, dok NIST-ov priručnik daje konkretne korake koje je potrebno slijediti kako bi se analizirao svaki kutak mreže, odnosno prije bi ga se moglo smatrati uputama.

5.2. OISG: Information Systems Security Assessment Framework (ISSAF)

ISSAF je detaljan priručnik od preko 800 stranica koji u dubinu obrađuje sljedeće teme:

- metodologija penetracijskog testiranja,
- mrežno testiranje:
  - lozinke,
  - preklopnici,
  - usmjeritelji,
  - vatrozid,
  - detekcija upada,

[7] *War dialing* je napad u kojem se koristi automatizirana aplikacija za biranje telefonskih brojeva u danom rasponu kako bi se otkrilo da li neki od tih brojeva koriste modemi.

  - virtualne privatne mreže,
  - antivirusi,
  - mrežni prostor za pohranu podataka,
  - bežične mreže,
  - Internet korisnici,
  - sigurnost Lotus Notes klijentske aplikacije,
- sigurnost računala domaćina:
  - Unix/Linux sigurnost,
  - Windows sigurnost,
  - sigurnost Novell [15] programskih rješenja,
  - sigurnost web poslužitelja,
- sigurnost aplikacija:
  - web aplikacije,
  - SQL injekcije,
  - revizija izvornog kôda,
  - binarna revizija
- sigurnost baze podataka te
- socijalni inženjering.

Za razliku od OSSTM-a, ISSAF ulazi u duboke detalje svakog pokrivenog područja. Usporedbom s prethodna 2 priručnika, ISSAF ostavlja dojam da ga koriste tvrtke koje žele da se testiranje provede svaki put na isti način po istim pravilima, bez odstupanja. NIST-ov priručnik daje malo više slobode prilikom analize, a OSSTM pritom nalikuje na ideologiju koja analitičarima dopušta kreativnu slobodu, dajući im pritom tek smjernice o tome što ne smiju zaboraviti tijekom revizije.

6. Zaključak

OSSTM metodologija nije samo priručnik s koracima za obavljanje revizije sigurnosti. Metode koje se preporučaju za sigurnosno testiranje mogu se primijeniti i na situacije druge prirode. Npr. razbijanje problema na sve manje i manje dijelove dok ti dijelovi ne budu dovoljno jednostavni da se direktno rješenje može primijeniti na razne vrste problema.

Stoga bi se moglo reći da OSSTM uči one koji ga koriste o tome kako razmišljati analitično, kako pojednostavniti probleme te na koji način donositi nepristrane zaključke, uz same postupke analize sigurnosti istraživanih sustava.

ISECOM kao organizacija neumorno radi na prenošenju metodologije široj publici. S projektima koji su usmjereni na djecu u osnovnim i srednjim školama, ISECOM stvara podlogu za razvijanje osjećaja sigurnosti u glavama budućih „kompjuteraša“. Malo koji priručnik o sigurnosti je napisan na način da ga i laici mogu shvatiti.

Od svog nastanka 2001. godine, ISECOM se proširio na desetke velikih projekata od kojih svi za podlogu koriste OSSTM metodologiju. Od prve inačice koja je imala tek 12 stranica, danas je aktualna treća inačica, narasla na 213 stranica. S obzirom da je riječ o *open source* proizvodu, mišljenja, pronalasci i ideje svakoga zainteresiranog za ovu tematiku se mogu uzeti u obzir i pridonijeti oblikovanju sljedeće inačice, OSSTM 4.

Svojim pogledom na svijet i društveno odgovornim ponašanjem, ISECOM si je stvorio poziciju među popularnim metodologijama koja se samo učvršćuje svakim novim projektom.

7. Leksikon pojmova

NIST

Nekada poznata pod imenom NBS (National Bureau of Standards), NIST je agencija koja se bavi mjeriteljstvom, standardim i tehnologijama u cilju poboljšanja ekonomske sigurnosti i kvalitete života.
http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

SQL injection napad

Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika.

http://en.wikipedia.org/wiki/SQL_injection

OSSTMM

OSSTMM (eng. *The Open Source Security Testing Methodology Manual*) je metodološki priručnik za provođenje sigurnosnih testova i određivanje univerzalne sigurnosne metrike.

http://www.isecom.org/osstmm/

ISECOM

ISECOM (eng. *Institute for SECurity and Open Methodologies*) je organizacija nastala oko OSSTMM priručnika, bavi se širenjem metodologije kroz mnoge projekte i društveno odgovoran rad.

http://www.isecom.org/

RAV

Rav je dio metrike OSSTMM priručnika. Predstavlja mjeru površine napada te količinu nekontroliranih interakcija sa sustavom koji se pokušava zaštititi.

http://www.isecom.org/research/ravs.shtml

Autentikacija

Autentikacija (eng. *authentication*) je proces potvrđivanja identiteta podatka ili osobe.

http://en.wikipedia.org/wiki/Authentication

Test Crne Kutije

Test Crne Kutije (eng. *Black Box test*) je metoda testiranja sustava kao zatvorene kutije bez poznavanja unutarnje strukture sustava.

http://www.faqs.org/faqs/software-eng/testing-faq/section-13.html

Test Bijele Kutije

Test Bijele Kutije (eng. *White Box test*) je metoda testiranja sustava uz poznavanje unutarnje strukture sustava. Isto što i *Crystal Box testing*, *Clear Box testing*.

http://www.faqs.org/faqs/software-eng/testing-faq/section-13.html

Penetracijski Test

Penetracijsko testiranje (eng. *Penetration test*) je metoda procjene sigurnosti sustava ili mreže simulacijom zlonamjernog napada.

http://en.wikipedia.org/wiki/Penetration_test

OISG

Organizacija kojoj je cilj integrirati alate za upravljanje i tehnike unutarnje kontrole u područje informacijske sigurnosti.

http://www.oissg.org/

ISSAF

Information Systems Security Assessment Framework (ISSAF) je OISG-ov projekt čiji je cilj pružiti jedinstveni izvor praktičnog znanja po pitanju sigurnosnih procjena namijenjen profesionalcima u području sigurnosti.

http://www.oissg.org/issaf

8. Reference

[1] Pete Herzog: OSSTM 3, http://www.isecom.org/mirror/OSSTM.3.pdf, prosinac 2010.

[2] ISECOM, http://www.isecom.org/, travanj 2011.

[3] Wikipedia: Open Source, http://en.wikipedia.org/wiki/Open_source, travanj 2011.

[4] Wikipedia: Creative Commons, http://en.wikipedia.org/wiki/Creative_Commons, travanj 2011.

[5] Wikipedia: OML, http://en.wikipedia.org/wiki/OML, travanj 2011.

[6] ISECOM: SCARE, http://www.isecom.org/research/scare.shtml, travanj 2011.

[7] ISECOM: HSM, http://www.isecom.org/hsm/, travanj 2011.

[8] ISECOM: Hacker Highschool, http://www.hackerhighschool.org/, travanj 2011.

[9] ISECOM: The Bad People Project, http://www.isecom.org/bpp/bpp.html, travanj 2011.

[10] ISECOM: SOMA, http://www.isecom.org/research/soma.shtml, travajn 2011.

[11] ISECOM: BIT, http://www.isecom.org/research/bit.shtml, travanj 2011.

[12] ISECOM: The Seminar Series, http://www.isecom.org/seminars.shtml, travanj 2011.

[13] John Wack, Miles Tracy, Murugiah Souppaya: NIST SP 800-42, Computer Security, Guideline on Network Security Testing, http://www.albany.edu/acc/courses/acc661/spring2004/NIST-SP800-42.pdf, listopad 2003.

[14] OISSG: Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B, http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1b/download.html, svibanj 2006.

[15] Novell, http://www.novell.com/, travanj 2011.