UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Mario Mišić

Sistemi za upravljanje incidentov in varnostnih informacij

DIPLOMSKO DELO

VISOKOŠOLSKI STROKOVNI ŠTUDIJSKI PROGRAM PRVE STOPNJE RAČUNALNIŠTVO IN INFORMATIKA

MENTOR: doc. dr. Mojca Ciglarič

Ljubljana, 2013

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00347/2012
Datum: 05.09.2012

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MARIO MIŠIĆ**

Naslov: **SISTEMI ZA UPRAVLJANJE INCIDENTOV IN VARNOSTNIH INFORMACIJ**

SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEMS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Opišite širše področje varnosti in najpogostejše varnostne grožnje, ki pretijo današnjim informacijsko komunikacijskim sistemom. Navedite, na kakšne načine lahko zaznavamo ranljivosti sistemov in kako prepoznavamo napade in grožnje. Analizirajte področje orodij in sistemov, ki so namenjeni avtomatiziranemu spremljanju dogodkov v sistemih z varnostnega vidika in upravljanju varnostnih informacij (SIEM). Izbrani sistem opišite podrobneje in preizkusite njegovo delovanje v praksi. Ovrednotite njegovo namestitev in nastavljanje, nato pa tudi kritično komentirajte njegovo učinkovitost in uporabnost.

Mentor:
doc. dr. Mojca Ciglarič

Dekan:
prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko
UNIVERZA V LJUBLJANI
2

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani Mario Mišić, z vpisno številko **63050175**, sem avtor diplomskega dela z naslovom:

Sistemi za upravljanje incidentov in varnostnih informacij

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič;
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela;
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 19. marca 2013 Podpis avtorja:

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za strokovne nasvete pri izdelavi diplomske naloge. Hvala staršema, Suzani in vsem, ki so mi v času študija stali ob strani.

Kazalo

Seznam uporabljenih kratic in simbolov

CIA Confidentiality, Integrity, Availability – zaupnost, neokrnjenost, razpoložljivost
DoS Denial Of Service – zavrnitev storitve
HTTP HyperText Transfer Protocol – protokol za prenos podatkov preko spleta
HTTPS Hypertext Transfer Protocol Secure – varnejša različica standarda HTTP
IDS Intrusion Detection System – sistem za zaznavanje vdorov
IP Internet Protocol – internetni protokol
IPS Intrusion Protection Systems – sistem za preprečevanje vdorov
IS Imformation System – informacijski sistem
OSSIM Open Source Security Information Management – odprtokodno upravljanje varnostnih informacij
OSSEC Open Source Security – odprtokodni sistem za zaznavanje vdorov
PII Personally Identifiable Information – osebni podatki
PDF Portable Document Format – odprt standard za izmenjavo elektronskih dokumentov
SIEM System Information and Event Management – upravljanje varnostnih informacij in dogodkov
SSH Secure Shell – varna povezava oz. protokol za prijavo in izvajanje ukazov na oddaljenem sistemu

Povzetek

Hiter razvoj računalništva in elektronskih omrežij je pripomogel k vpeljavi informacijskih sistemov v različne gospodarske dejavnosti. S tem se je izpostavljenost varnostnim grožnjam in morebitnim vdorom v tovrstne sisteme zelo povečala. Vse bolj pogosta so bila vprašanja, kako učinkovito uporabiti ukrepe za varovanje informacijskih sistemov in te zaščititi. Zato sem v diplomski nalogi predstavil enega izmed ukrepov, ki predstavlja sistem za upravljanje varnostnih informacij in dogodkov (SIEM).

Osredotočil sem se na informacijsko varnost in na kakšen način jo je moč zagotoviti. Med drugim sem opisal varnostne grožnje, ki nam v današnjem času pretijo, tako v obliki zunanjih kot tudi tistih znotraj lokalnega omrežja. Pri tem je zelo pomembno, da grožnjo oziroma napad na sistem zaznamo v pravem času, jo ustrezno kvalificiramo in skušamo preprečiti njen vpliv. Predstavil sem različne vrste zlonamernih programskih kod, ki izkoriščajo ranljivost operacijskih sistemov.

Sistem za upravljanje varnostnih informacij in dogodkov (SIEM) nam v realnem času ter na enem mestu zagotavlja celovit pregled varnostnega stanja informacijskega sistema. Med tovrstne sisteme se uvršča tudi AlienVault. Predstavil sem njegovo zgradbo, funkcionalnost, uporabniški vmesnik in njegov položaj na tržišču. Opisal sem postopek namestitve sistema na strežnik, njegovo nastavitev za pravilno delovanje in način obveščanja sistema ob morebitnih poskusih napadov. Testiral sem tudi odziv sistema ob različnih grožnjah in analiziral pridobljene rezultate. Ugotovil sem, da so tovrstni sistemi zmogljivi in zelo učinkoviti, pa tudi, da lahko ob pravilnih nastavitvah veliko pripomorejo k informacijski varnosti organizacije.

Ključne besede: informacijska varnost, upravljanje varnostnih informacij in dogodkov (SIEM), AlienVault OSSIM.

Abstract

The fast development of computer technology and electronic networks has contributed to the introduction of information systems to different economic activities. This has significantly increased the exposure to security threats and potential intrusions into such systems. Questions of how to use measures for the safeguarding of information systems and how to protect them are becoming more and more common. Therefore, I presented one of the measures, which represents a system for managing security information and events (SIEM), in the Diploma thesis.

I focused on the information security and how to ensure it. Among other, I described security threats we face nowadays in the form of external threats as well as within the local network. Here, it is extremely important that we identify the threat or attack on the system at the right time, classify it appropriately and try to prevent its effects. I presented different types of malevolent programming codes that exploit the vulnerability of operating systems.

The security information and event management system (SIEM) provides a comprehensive overview of the security state of the information system in real time and in one place. One of such systems is also AlienVault. I presented its structure, functionality, user interface and its position on the market. I described the installation of the system on the server, its settings for proper functioning and the manner of alerting the system of potential attacks. I tested the system's response to different threats and analysed the obtained results. I found that such systems are high-performing, very efficient and can, with the correct settings, contribute significantly to the information security of the organisation.

Keywords: information security, security information and event management (SIEM), AlienVault OSSIM.

Poglavje 1

Uvod

Odkar se število kibernetskih napadov, kraje identitet in intelektualne lastnine povečuje, tudi potreba po ustrezni varnosti ter obrambnih sistemih raste. Obraniti se pred takšnimi grožnjami je za posameznika ali organizacijo ključnega pomena, a obenem zelo zahtevno, saj je napadalec zmeraj v rahli prednosti. Medtem, ko strokovnjak za varnost preučuje vse možne nevarnosti, da bi napadalcu preprečil vdor v sistem, je slednjemu pomembno le to, da se osredotoči na eno področje in ga temeljito razišče. To napadalcu daje boljši položaj in rahlo prednost. Z namenom, da bi kar najbolje zavarovali okolje, je ključnega pomena uporabiti vse informacije, ki so na voljo in ugotoviti, na kakšen način razporediti vire, ki so nam pri roki.

V diplomski nalogi se bom poglobil v informacijsko varnost in predstavil orodje, ki pripomore k zagotavljanju le te. V prvem delu bom razložil, zakaj je pomembna informacijska varnost in na kakšen način jo je možno zagotoviti. Opisal bom različne grožnje, ki nam v današnjem času pretijo na področju informacijskih sistemov. Zavedati se moramo, da fizično varovanje podatkov ni več dovolj. Če pogledamo s stališča navadnega uporabnika, lahko rečemo, da je že skoraj na vsakem osebnem računalniku nameščen protivirusni program za zaščito pred zlonamerno programsko kodo ali pa požarni zid. Pri večjih podjetjih in organizacijah pa se izkaže, da je tudi to premalo, zato posežejo po različnih sistemih za obrambo, ki so sposobni nadzorovati celotno omrežje, v katerem se nahajajo njihovi računalniki. Gre za sisteme za upravljanje varnostnih informacij in dogodkov, katerih delovanje ter zgradba bo prav tako opisana v nadaljevanju diplomske naloge. AlienVault je eden izmed takšnih sistemov, ki je sposoben nadzorovati omrežje in zaznavati različne dogodke oziroma grožnje v realnem času ter nas o tem tudi obveščati. Program bom nazorno tudi opisal in predstavil njegove funkcije. Ob koncu bom na primeru prikazal njegovo namestitev in delovanje, nastavitev različnih profilov za obveščanje ter analiziral varnostna obvestila.

Poglavje 2

Informacijska varnost

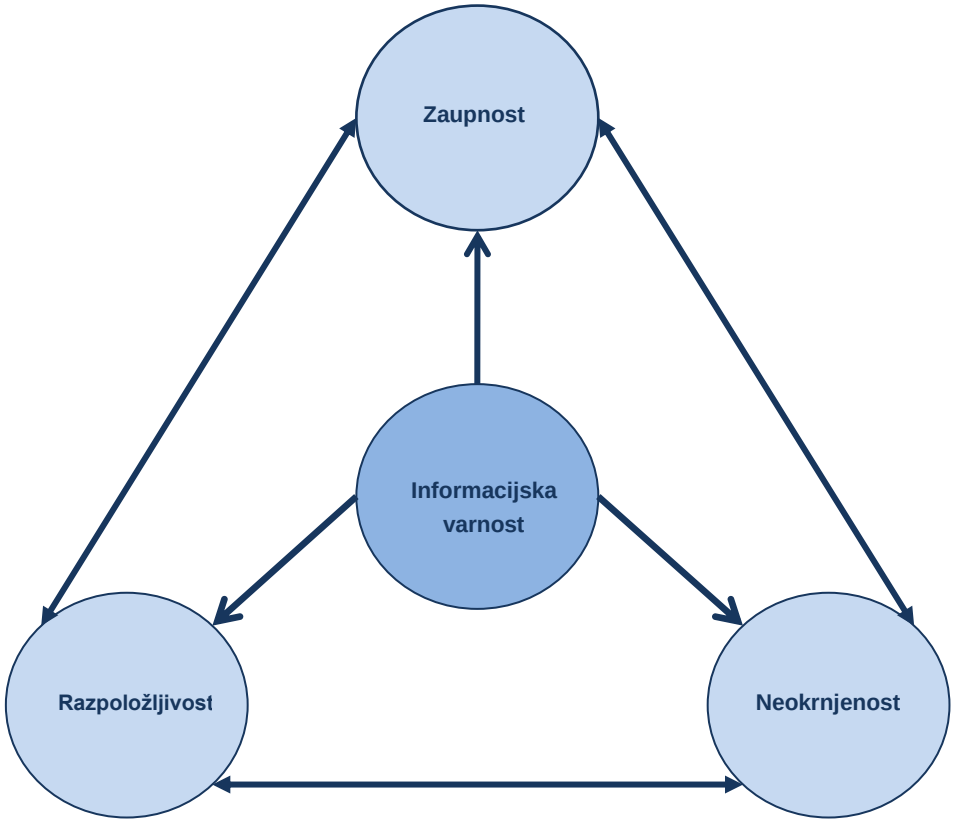
Vsakodnevno izhajajo članki, ki govorijo o novih ranljivostih v sistemih in podjetjih, ki so vse bolj ogrožena. Največkrat smo mnenja, da med najbolj ogrožena spadajo velika podjetja s pomembnimi skrivnostmi. To do neke mere drži, vendar manjša podjetja niso nič manj ogrožena in so lahko še bolj izpostavljena grožnjam, ker je tudi varnost v takih podjetjih manjša. Čeprav so najbolj ogrožene finančne informacije in poslovne skrivnosti podjetij, so v ospredju varnostnih strokovnjakov osebni podatki (PII) zaposlenih ali pa strank. Te informacije lahko vključujejo številki socialnega zavarovanja, vozniškega dovoljenja, davčno številko, poštni in elektronski naslov, datum rojstva itd. Vsak izmed naštetih podatkov je dragocen že sam po sebi, vendar je njihov skupek mogoče uporabiti tudi kot krajo identitete. Če bi napadalec pridobil davčno številko, stalni naslov in datum rojstva neke osebe, bi na primer z lahkoto lahko odprl tudi bančni račun z njegovo identiteto.

Na začetku so hekerji izvajali napade na sisteme, da bi preizkušali njihovo ranljivost in se obenem iz tega tudi učili. Danes pa gre povečini za krajo informacij in poizkus finančnega okoriščanja. Eno izmed pomembnih vprašanj je, kaj bo napadalec storil s podatki, ki jih je pridobil. To je odvisno od vrste podatkov, ki jih je uspel pridobiti. Če je uspel pridobiti poslovni načrt za prihodnje leto, ga lahko brez težav proda konkurenčnemu podjetju ali pa izsiljuje matično podjetje. Na ta način mu okradeno podjetje plača in podatki še naprej ostanejo zaupni. Prodaja ukradene intelektualne lastnine predstavlja velik posel na internetu. Za tem večinoma stojijo kriminalne organizacije in morda celo nekatere države. Te so glavni trg za ljudi, ki želijo prodati posameznikove osebne podatke in poslovne skrivnosti podjetja najboljšemu ponudniku. Drugi bolj razširjen razlog za napad pa nima nič opraviti s podatki. V tem primeru gre za dostop in nadzor računalniškega sistema. Ti sistemi se lahko nato uporabljajo tako za shranjevanje in distribucijo nezakonito pridobljenih podatkov, kot tudi avtorsko zaščitenih vsebin [1].

2.1 Zagotavljanje informacijske varnosti

Eno izmed pomembnih vprašanj, ki si ga moramo zastaviti pri načrtovanju varnosti, je: Kaj bi napadalec želel pridobiti iz našega računalnika oziroma informacijskega sistema? Lahko bi ga zanimale poslovne skrivnosti, finančni podatki, osebni podatki zaposlenih in strank ali pa kakšne druge informacije. Te bi lahko nato izkoristil na več načinov. Lahko bi jih prodal konkurenci ali pa ponaredil identiteto zaposlenega ali pa stranke. Kraja informacij iz podjetja je le eden od načinov, s katerim je moč oškodovati podjetje.

Pri zagotavljanju varnosti je zelo pomembno, da strokovnjaki razvijejo program, ki bo pri svojem delovanju imel tri cilje: zagotoviti zaupnost, neokrnjenost in razpoložljivost dragocenih informacij, ki so v ozadju sistema. Ti cilji so poznani kot trojček CIA (slika 2.1) in predstavljajo temeljna načela, na katerih naj bi varnost temeljila. Brez poznavanja teh pojmov in njihove povezave v okolju je težko določiti varnostne potrebe, ki bi jih takšen program moral vsebovati.



Slika 2.1: Trojček CIA

Zagotavljanje zaupnosti (angl. confidentiality) pomeni, da je dostop do podatkov in računalniških virov omogočen le pooblaščenim osebam. To lahko dosežemo z uporabo nadzora dostopa. Največkrat se uporabi kriptografija, ki zašifrira podatke in s tem zagotovi dostopnost podatkov ter informacij izključno pooblaščenim osebam.

Zagotavljanje neokrnjenosti (angl. integrity) pomeni, da bomo zaznali vsakršno spreminjanje, ustvarjanje ali brisanje podatkov brez pooblastila. Zamislimo si, da nek zaposleni v podjetju prejme sporočilo od sodelavca o naročilu 10.000 svinčnikov. Pri tem lahko prejemnik podvomi v verodostojnost sporočila. Obstaja možnost, da je bilo sporočilo spremenjeno med pošiljanjem in je pošiljatelj napisal, da naroči le deset svinčnikov. V tem primeru bi šlo za kršitev neokrnjenosti.

Zagotavljanje razpoložljivosti (angl. availability) pomeni zagotavljanje dostopnosti do IS takrat, ko ga pooblaščeni uporabniki potrebujejo [2].

2.2 Varnostne grožnje

Uporaba omrežja nam olajša komunikacijo in zabriše zemljepisne omejitve. Pri tem ne smemo pozabiti, da smo lahko ob uporabi spletnih tehnologij izpostavljeni različnim varnostnim grožnjam. Omrežje oz. varnostne luknje v sistemu omogočajo nepridipravom, da z nekaj znanja pridobijo nadzor nad našim računalnikom in na ta način pridejo do naših podatkov ali pa denarja.

2.2.1 Ranljivost protokolov

Računalniki, omrežja in protokoli, ki omogočajo komunikacije preko interneta, niso več tako novi. Številni protokoli, na katerih so se pokazale varnostne pomanjkljivosti, so zamenjani z varnimi različicami. Če bi želeli zavarovati notranje okolje, bi morali uporabljati protokole, ki niso ranljivi oz. ogroženi.

2.2.2 Napačne konfiguracije

Velikokrat je za vdor v informacijski sistem kriva napačna konfiguracija požarnega zidu ali pa orodij za preprečevanje vdorov. Dogaja se tudi, da strežniške storitve potekajo na sistemih, ki niso namenjeni temu. Tukaj je zelo pomembno, da varnostni oz. sistemski tehnik dobro pozna to področje, saj tudi sistemi za zaznavanje vdorov ne bodo sporočali napadov, če ne bodo pravilno nastavljeni.

2.2.3 Uporabniške napake

Pogosto je za ranljivost informacijskega sistema odgovoren končni uporabnik. Če gre za domače omrežje, je škoda, ki jo lahko utrpimo, zelo majhna v primerjavi s podjetjem ali organizacijo. Ena izmed rešitev bi bila, da bi uporabniku onemogočili dostop do interneta. To bi bilo najenostavnejše, vendar tega ne moremo storiti, saj je internet vir informacij za uporabnika. Čeprav določeni uporabniki želijo biti produktivni, delajo preproste napake, ki pa ogrožajo sistemsko varnost in povečujejo možnost vdorov.
Preprost primer je uporabnik, ki zapusti delovno mesto in pusti odklenjen računalnik oz. operacijski sistem. To izkoristi nepooblaščeni uporabnik, ki pobrska po omrežju ter poizkuša dostopati do vsebin, do katerih prvotni uporabnik nima dostopa. Največkrat naleti na opozorilo, da ima zavrnjen dostop do teh vsebin. Če ima takšno podjetje sistem za zaznavanje vdorov, bo ta prepoznal povečano število dostopov do zaščitenih vsebin in bo to tudi sporočil varnostnim strokovnjakom.

Drugi primer uporabniške napake bi bil, ko uporabnik prejme elektronsko sporočilo, ki je dejansko lažno predstavljanje nekega podjetja ali finančne institucije z namenom pridobitve najrazličnejših zaupnih podatkov. Takšno prevaro imenujemo ribarjenje (angl. phishing). V današnjih dneh pričakujemo, da so uporabniki bolj seznanjeni s takšnimi stvarmi, vendar je lahko tudi drugače. Če pogledamo na preprostem primeru, ko uporabniki brskajo po spletu, lahko pri tem kliknejo na povezavo, ki jim je bila poslana s strani lažnega pošiljatelja. S tem se v brskalniku odpre spletna stran, preko katere se na računalniški sistem naloži zlonamerna programska oprema. Veliko požarnih zidov je mogoče nastaviti tako, da blokirajo zahtevke za te spletne naslove s pomočjo dinamičnega posodabljanja IP-naslovov s črnih list.

K večji varnosti sistemov in preprečevanju uporabniških napak zelo pripomore tudi osnovno izobraževanje uporabnikov. Znotraj tega bi pridobili nasvete o upravljanju gesel,

varnemu spletnemu brskanju, neposrednemu sporočanju ter o uporabi e-pošte. K večji varnosti pripomorejo tudi redni elektronski poštni nasveti ali pa mesečne novice [3].

2.2.4 Notranje grožnje

V okviru notranjega oz. lokalnega omrežja se tipično uporabljajo manj ostri varnostni ukrepi. To pa zato, ker notranje omrežje smatramo kot varno omrežje in ga zato niti ni treba zaščititi. Vendar pa se vse bolj zavedamo, da temu ni tako. Prav notranje zlorabe so najpogostejši način izvajanja napadov. V večji raziskavi, ki je bila opravljena leta 2009, se je izkazalo, da je med 50 in 90 odstotkov vseh napadov prav notranjih. Ti so lahko storjeni s strani nezadovoljnih ali pa nelojalnih zaposlenih, ki imajo določene skrbniške pravice v sistemu. Osebja na visokih položajih in skrbnikov z neomejenimi pooblastili za dostop skoraj ni mogoče zaustaviti. Tudi slaba fizična varnost prostorov omogoči nepooblaščenim osebam lahek dostop do notranjega omrežja. Dodatna skrb so tudi dostavno osebje, začasni delavci in celo vratarji, ki jim je pogosto dovoljeno nemoteno gibanje po prostorih podjetja.

Čeprav ni mogoče doseči popolne zaščite, lahko z nekaterimi ukrepi bistveno zmanjšamo tveganje. Lahko porazdelimo sisteme in pooblastila tako, da nihče nima prevelikega nadzora. Posamezniku ne smemo dati vsa pooblastila, ampak jih je najbolje razdeliti med več ljudi. Zelo pomemben je tudi nadzor nad shranjenimi varnostnimi kopijami, arhivi in kopijami zbirk podatkov. Prav tako sta potrebna skrb in evidenca o tem, kdo uporablja prenosne računalniške naprave ter osveščanje uporabnikov glede zaščite naprav in podatkov v času službene poti. Pomembno je tudi, da zunanjim obiskovalcem ne dovolimo nenadzorovanega gibanja po pisarnah podjetja [4].

2.2.5 Zunanje grožnje

Zunanje grožnje je pogosto lažje odkriti in se jih ubraniti kot pa notranje, saj ima večina omrežij implementirane varnostne sisteme. Zunanje grožnje vključujejo ročne oz. človeške napade, kjer napadalec poizkuša vdreti v sistem ali pa vanj poslati viruse ali črve. Ročni napadi so počasnejši pri svojem napredovanju, so pa zato bolj osredotočeni. Samodejni napadi so hitrejši, bolj zaznavni in imajo veliko število neuspelih poizkusov.

2.3 Zaznavanje napadov in groženj

Ne glede na to, ali so notranji ali zunanji, ročni ali samodejni, usmerjeni ali neusmerjeni, številni napadi imajo prepoznavne značilnosti, ki jih je mogoče odkriti s sistemom za zaznavanje vdorov ter z varnostno ekipo. V nadaljevanju je opisanih več t. i. prepoznavnih dogodkov in napadov, pa tudi, kako jih lahko odkrijemo s sistemi SIEM.

Preden napadalec resnično napade sistem ali omrežje, ga dobro pregleda in odkrije, kakšni varnostni mehanizmi se skrivajo v ozadju. To lahko stori na več načinov, ki so opisani v nadaljevanju.

Preiskovanje (angl. fingerprinting ali footprinting) označuje različne akcije zbiranja podatkov o bodoči žrtvi napada. Najprej se ugotovi IP-naslov sistema, nato se razišče njegova struktura, katere domene gosti, kakšen operacijski sistem gosti, kakšna programska oprema poganja storitve itd.

Ko je enkrat oris omrežja že narejen in ima napadalec že vidna vozlišča v tem omrežju, se odloči za preiskovanje ter identificiranje le teh. Pri tem upa in išče takšne sisteme, ki so lahko ranljivi ter vsebujejo dragocene informacije. Preiskovanje se običajno izvaja iz enega IP-naslova in preiskuje le en ciljni IP-naslov, pri tem pa raziskuje več različnih vrat v tem sistem. Najbolj znani programi s katerimi lahko izvajamo preiskovanje so Nmap, Queso, Ettercap, in P0f [5].

2.4 Zlonamerna programska koda (angl. exploit)

Gre za programsko kodo oz. programe, ki izkoriščajo ranljivost operacijskega sistema. Ko ima napadalec vsaj grobo predstavo omrežja in je identificiral eno ali več tarč, takrat začne razpošiljati zlonamerno programsko opremo, ki se namesti v računalnik. Na ta način lahko napadalec pride do osebnih podatkov ali pa nadzoruje dejavnosti znotraj operacijskega sistema. Nekateri napadi so usmerjeni zlasti v preprečevanje dostopa do podatkov oziroma onemogočanje katerekoli storitve za legalne uporabnike. Ti so v nadaljevanju opisani in se imenujejo DoS-napadi. Drugi napadi poizkušajo pridobiti skriti nadzor nad sistemom za plenjenje in globlje penetracije. V nadaljevanju so podani opisi različnih napadov in idej o tem, kako opaziti njihovo navzočnost v sistemu ter omrežju.

2.4.1 Virusi

Računalniški virus je zlonameren algoritem, ki se je sposoben sam razmnoževati, spreminjati in se zna tudi sam zagnati, kar pomeni, da ni potrebna interakcija uporabnika. Ko se razmnoži, lahko prične s škodljivim vedenjem, kot je brisanje podatkov na trdem disku. Prav tako lahko poškoduje tudi strojno in programsko opremo. Ime virus je dobil, ker je njegovo vedenje zelo podobno biološkemu virusu. Gostitelj virusa pa je računalniški program.

Veliko virusov se širi s pomočjo elektronske pošte, kjer je pripet k sporočilu tako, da ga uporabnik pri odpiranju in branju pošte ne vidi.
Če od neznane osebe prejmemo elektronsko pošto s prilogo, je treba biti pazljiv ali pa jo kar takoj izbrisati. Žal varnost ni zagotovljena niti pri odpiranju prilog, ki jih pošljejo znanci ali prijatelji. Virusi znajo tudi krasti podatke iz programov za elektronsko pošto in tako pošljejo svoje kopije na vse naslove, ki so v adresarju oz. imeniku. Pri prejemanju elektronske pošte s sporočilom, ki ga ne razumemo ali pa ga nismo pričakovali, je obvezno treba povprašati pošiljatelja glede vsebine priloge, preden se ta odpre.

Drugi virusi se lahko širijo s programi, ki se prenesejo z interneta ali pa z okuženimi izmenljivimi diski [6].

2.4.2 Črvi

Črvi so programi, ki potujejo preko omrežij, in ponavadi množično izkoriščajo ranljivost sistemov. Črv je prav tako kot virus zasnovan z namenom širjenja v druge računalnike, vendar to naredi samodejno in tako, da prevzame nadzor nad računalniškimi funkcijami za prenos datotek ter podatkov. Ko se črv naseli v sistem, lahko potuje sam. Nevaren je prav zaradi izjemne sposobnosti hitrega širjenja. Svoje kopije lahko, na primer, pošlje na vse naslove, ki jih ima posameznik shranjene v imeniku, računalniki naslovnikov pa bi naredili isto, kar povzroči učinek domin. Velik omrežni promet, ki je posledica širjenja črva, lahko upočasni poslovna omrežja in celo internet kot celoto. Ko se pojavijo novi črvi, se razširijo zelo hitro in zasitijo omrežja, zato je potrebno včasih na ogled posameznih spletnih strani čakati dlje [7].

2.4.3 Pretvarjanje (angl. IP spoofing)

Pretvarjanje oziroma napad s prevaro se uporablja za pridobivanje nepooblaščenega dostopa do računalnikov. Napadalec pošlje računalniku sporočilo z lažnim IP naslovom izvora, kateri pripada zaupanja vrednemu pošiljatelju. Če želi napadalec izvesti IP prevaro, mora uporabili različne tehnike s katerimi bi prišel do zaupanja vrednega IP naslova. Ko ga enkrat pridobi, ga potem uporablja pri pošiljanju sporočil na ta način, da v IP datagramu spremeni izvorni IP naslov. Na ta način si lahko napadalec pridobi dostop do sistemov, kjer poteka avtorizacija na osnovi IP številke. Take vdore lahko opazimo s pomočjo orodij za opazovanje mrežnega prometa. Eno izmed njih je tudi program Netlog [8].

2.4.4 Zavrnitev storitve (angl. Denial-of-Service)

DoS napad ali zavrnitev storitve je proces, ki so ga razvili hekerji okoli leta 2000, svoj razcvet pa je doživel leta 2002, ko so hekerji za nekaj ur onesposobili strežnike kot so Amazon.com in Download.com. Tudi danes so DoS napadi zelo pogosti. Spomnimo se, da je skupina hekerjev z imenom Anonymous v preteklih nekaj letih na ta način onesposobila veliko strežnikov, med njimi tudi najbolj znanih organizacij kot so FBI, Amazon, Visa, MasterCard in PayPal. DoS napad se izvaja tako, da napadalec preko določenega protokola, pošlje tarči veliko število zahtev. Ker strežnik lahko v določenem trenutku obravnava le omejeno število zahtev, se na ta način preobremeni strežnik in ta ne more več obdelovati novih zahtev [9].

2.4.5 Porazdeljena zavrnitev storitve (angl. Distributed Denial-of-Service)

DDoS napad bi v prevodu pomenil porazdeljena zavrnitev storitve. Pri tem napadu se dogaja zelo podobno kot pri DoS napadu. Razlika je le v tem, da pri DDoS napadu napadalec izvaja napad z več računalnikov, ki sledijo njegovim ukazom. Večinoma je te računalnike pridobil z vdorom ali pa ima legalen dostop do njih. Napadalec sporoči svojim računalnikom, z določenimi ukazi ali pa kar s programom (TFN - Tribe flood Network), naj napadejo tarčo z določeno kapaciteto podatkov. Pri tovrstnem napadu je podatkov bistveno več kot pri DoS napadu, saj več računalnikov pošlje veliko več podatkov kot

eden. DoS in DDoS napadi na spletne strani lahko povzročijo velike izgube v podjetju, tudi, če trajajo le kratek čas [10].

2.4.6 Preplavljanje vmesnikov (angl. buffer overflow)

Preplavljanje oziroma prekoračitev vmesnika je eden izmed pogostih načinov vdora v sistem. Napadalec se napada loti tako, da na podlagi pregledovanja v žrtvinem sistemu odkrije aplikacijo, ki je občutljiva za napade tipa prekoračitev vmesnika. Naslednji korak takšnega napadalca je iskanje konkretnih skriptov, ki omogočajo vstop v sistem z izkoriščanjem občutljivosti, ki jo je napadalec odkril v fazi pregledovanja sistema. Takšni napadi so v zadnjem času zelo priljubljeni, saj napadalcu omogočijo vstop v sistem, hkrati pa tudi precejšen nadzor le tega.

Vsak sestavni del operacijskega sistema ali aplikacije, ki je slabo napisana, je lahko ranljiva za omenjene napade. Z raziskovanjem takšne aplikacije ali operacijskega sistema lahko napadalec v sistemu izvrši arbitrarne ukaze, na podlagi katerih prevzame sistem. V vseh primerih napada na podlagi prekoračitve vmesnika je metoda naslednja [11]:

- Napadalec vnese v aplikacijo več podatkov kot pa ima aplikacija rezerviranega prostora. Na ta način prepiše krajevne spremenljivke s strojno kodo, pri čemer se sistem ne ustavi ob koncu izvrševanja krajevnih spremenljivk, temveč procesorju naloži tudi izvršitev dodane strojne kode.

- Procesor izvrši dodano strojno kodo in s tem želeni arbitrarni ukaz napadalca.

2.4.7 Napad na gesla

Napadalci poskušajo razbiti oz. ugotoviti gesla in tako priti do nepooblaščenega dostopa do računalniških sistemov ter virov informacij. Pri tem preverjajo različne kombinacije znakov, da bi prišli do pravega gesla. Ti napadi so običajno vodeni s pomočjo aplikacije za odkrivanje gesel. Vsi računalniški sistemi bi zato morali imeti varnostni mehanizem, ki bi ob večjem številu neuspešnih poskusov prijave v sistem blokiral uporabniški račun.

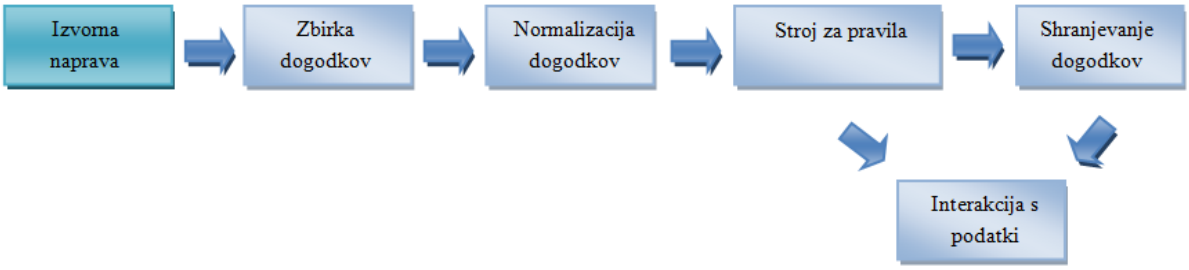
2.4.8 Napadi na sisteme IDS/IPS

Sistemi za odkrivanje in preprečevanje vdorov vsebujejo vzorce znanih napadov, na osnovi katerih spremljajo omrežje ter odkrivajo napade. Sistemi IDS/IPS na osnovi vedenjskih vzorcev spremljajo obnašanje sistema ali omrežja in se ob nepravilnostih ustrezno odzivajo. Lahko preprečijo promet preko omrežja, zabeležijo dogodek ali pa obvestijo skrbnika o dogodku. Sistemi IDS in IPS so znani po svojih številnih lažno pozitivnih opozorilih, ki pa jih je možno sčasoma zmanjšati. Takšni sistemi so lahko tarča za napadalce, saj ti lahko onemogočijo njihove senzorje za zaznavanje napadov. Zato je treba senzorjem omogočiti prejemanje paketkov (podatkov) samo iz znanih virov naprav. Paketki, poslani iz drugih naprav, bi lahko bili delo napadalca, ki želi onemogočiti senzorje in posledično delovanje sistemov IDS/IPS.

Poglavje 3

Upravljanje varnostnih informacij in dogodkov (SIEM)

Sistem za upravljanje varnostnih informacij in dogodkov (SIEM) omogoča celovit pregled varnostnega stanja informacijskega sistema v realnem času. Z zbiranjem in obdelavo podatkov iz strežniških, omrežnih in ostalih naprav nam zagotavlja učinkovito upravljanje varnostnih tveganj oz. sprotno alarmiranje ter ukrepanje ob varnostnih kršitvah. Osnovna filozofija delovanja takšnega sistema sloni na verigi, kjer ima vsak člen točno določeno nalogo, obenem pa sodeluje tudi s sosednjimi členi (slika 3.1).



Slika 3.1: Zgradba SIEM

Večina ljudi se niti ne zaveda, kaj vse se beleži v dnevniške datoteke pri izvajanju programov s strani uporabnika. Že samo odpiranje poljubne spletne strani sproži beleženje dogodkov iz različnih naprav. Računalnik se preko usmerjevalnikov, stikal in požarnih zidov poveže s strežnikom. Vse to se beleži v dnevniških datotekah. Prav tako tudi strežnik hrani podatke, kaj vse je uporabnik počel in kaj vse si je ogledal na spletni strani.

3.1 Zgradba SIEM

3.1.1 Izvorna naprava (angl. source device)

Prvi del, ki sestavlja SIEM, je izvorna naprava (angl. source device), ki je vir podatkov za SIEM. Izvorna naprava je lahko dejansko naprava, kot je usmerjevalnik, stikalo, strežnik ali pa kakršen koli dnevniški zapis dogodkov, katerega je izvedla aplikacija. Prav zato izvorna naprava ni del okolja SIEM, ki smo ga kupili, ampak je le ključnega pomena pri celotnem SIEM-procesu. Vsi sistemi in naprave v omrežju so tam, da bi obdelovale nekatere vrste informacij za uporabnike, vendar bi brez njih in dogodkov, ki jih generirajo, SIEM bil le preprost sistem, ki ne bi naredil ničesar.

3.1.2 Zbirka dogodkov (angl. log collection)

Vse zbirke dogodkov je treba posredovati tudi v SIEM. Sam prenos se lahko izvrši na dva načina. Prvi je ta, da izvorna naprava pošlje dnevniški zapis v SIEM (angl. push method). Drugi način pa je, da ga SIEM sam pridobi (angl. pull method). Oba načina sta v uporabi in imata prednosti ter slabosti, a sta oba uspešna pri pridobivanju in prenosu informacij v SIEM.

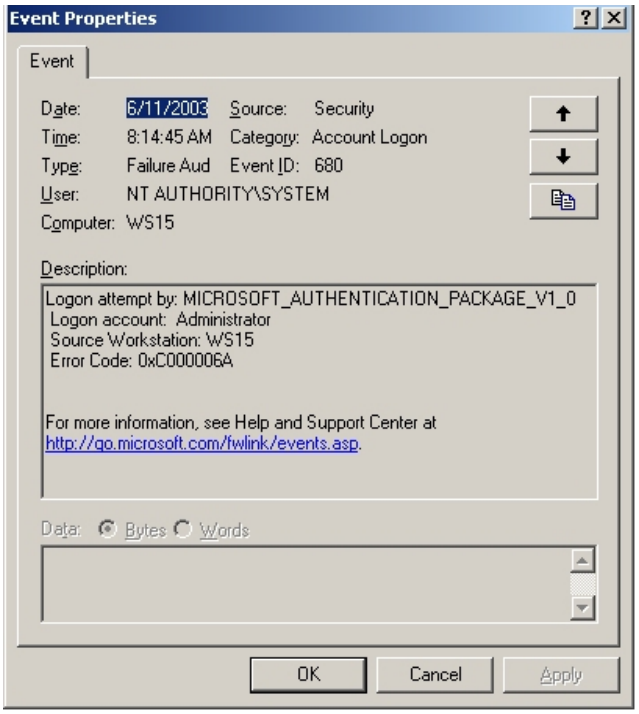
Prednost t. i. push metode je enostaven način vzpostavitve delovanja. Vse, kar je treba, je to, da nastavimo sprejemnika in nato usmerimo izhodno napravo proti njemu. Ta pošilja podatke preko UDP oz. nepovezanega protokola (angl. User Datagram Protocol). Pri tem protokolu odjemalec in strežnik ne vzpostavita povezave, ampak strežnik pošilja pakete odjemalcu in pri tem ne preverja, če je odjemalec pakete dobil. Prav to pa je slabost t. i. push metode, saj ob težavah na omrežju ni zagotovila, da bo SIEM podatke tudi prejel.

Pri t. i. pull metodi pa SIEM sam vzpostavi povezavo z izhodno napravo in na ta način prenese dnevniški zapis dogodkov. Slabost pri tej metodi je, da se je nek dogodek že zgodil in ga SIEM ni prejel v realnem času ter se nanj ustrezno odzval. Sam sprejem dnevnika dogodkov se izvaja periodično in se lahko ponovi vsako sekundo, ali pa vsako uro, glede na to, kakšen interval nastavi administrator. Če je časovni interval med nepošiljanjem daljši od privzetega, se SIEM ne more pravočasno odzivati ob večjem napadu.

3.1.3 Normalizacija dogodkov (angl. parsing/normalization of logs)

V tem delu so zbrani vsi dnevniki dogodkov, ki pa so še vedno zapisani v izvornem formatu, kot ga je posamezna naprava ali sistem zapisoval. Za to, da bi postali uporabni za SIEM, je potrebna pretvorba v enoten standardni format. Ta postopek pretvorbe se imenuje normalizacija. Normalizacija se bo znotraj SIEM-a izvajala na različne načine, vendar bo končni produkt enak zapisu, ki ga bo SIEM lahko bral in uporabljal.

Preprost primer je prikazan na slikah 3.2 in 3.3, kjer gre za prijavo uporabnika v napravo oz. sistem. Razvidno je, da različne naprave podajo različne načine zapisa dogodkov. Slika 3.4 prikazuje oba dogodka, ki jih SIEM po normalizaciji lahko prikaže uporabniku. Razvidno je, da sta dnevnika iz različnih naprav sedaj v enakem zapisu.



Slika 3.2: Windows - dnevnik dogodkov

Priority	Hostname	Message
Local4.info	192.168.1.1	:%ASA-sys-6-605005: Login permitted from 192.168.1.18/42925 to INSIDE:192.168.1.1/ssh

Slika 3.3: Cisco - dnevnik dogodkov

Time	Date	Source Device IP Address	Event Message	Event ID
22:54:53 CST	17-Jan-10	192.168.1.1	User login	ASA-sys-6-605005
22:54:53 CST	17-Jan-10	192.168.1.18	User login	Security: 680

Slika 3.4: Prikaz dogodkov po normalizaciji

3.1.4 Stroj za pravila (angl. rule engine/correlation engine)

Naslednji sestavni del sistema SIEM je t. i. stroj za pravila, ki po normalizaciji dogodkov iz različnih virov naprav sproži opozorila v SIEM zaradi posebnih pogojev v teh dnevnikih. Način pisanja pravil za obveščanje SIEM-a se običajno prične dokaj preprosto, vendar lahko postane tudi zelo kompleksen. Ta pravila običajno uporabljajo Boolovo obliko logike, kjer se ugotovi, ali so izpolnjeni določeni pogoji, preveri pa se tudi ujemanje vzorcev v podatkovnih poljih.

Zelo dober primer je takrat, ko želimo biti obveščeni o prijavljanju uporabnikov s skrbniškimi pravicami v strežnik. Če bi strežniki, ki jih uporabljamo, imeli različne operacijske sisteme, bi tudi pogoji za obveščanje bili različni. Pri Windowsovih operacijskih sistemih bi za pogoj uporabili uporabniško ime »administrator«, pri Linuxovih operacijskih sistemih pa »root«, ona pa označujeta, da je lokalni skrbnik prijavljen v strežnik. Prednost SIEM-a je v tem, da namesto takšnih dvojnih pravil uporablja notranjo logiko, ki temelji na več spremenljivkah.

3.1.5 Shranjevanje dogodkov (angl. log storage)

Ta del sistema SIEM je namenjen skladiščenju oz. shranjevanju dogodkov. Ti se lahko shranijo na tri načine: v podatkovno bazo, v tekstovno datoteko ali pa v binarno datoteko.

Podatkovna baza je najbolj uporabljan način za shranjevanje dogodkov. Lahko gre za platformo podatkovne baze Oracle, Microsoft SQL, IBM DB2 ali MySQL. V tem primeru je iskanje shranjenih podatkov precej enostavnejše in do njih dostopamo s pomočjo klicev,

ki so že del aplikacije. Edina slabost uporabe pa je, če se SIEM izvaja na lastni strojni opremi. V tem primeru je nujno potreben administrator podatkovne baze.

Tekstovna datoteka je preprosta datoteka z besedilom, ki shranjuje podatke v človeku razumljivi obliki. Sam zapis podatkov v datoteki mora biti lepo urejen oz. mora vsebovati presledke, tabulatorje ali vejice, da so podatki ločeni med seboj in lažje berljivi. Tovrstni način shranjevanja pa se ne uporablja zelo pogosto. Slabost v primerjavi z drugimi metodami je namreč v počasnem zapisovanju in branju podatkov iz takšnih datotek. Kot prednost pa je nedvomno lahka berljivost in analiza podatkov.

Binarna datoteka je datoteka s podatki, zapisanimi kot zaporedje bitov, ki jih ni mogoče smiselno razbrati.

3.1.6 Interakcija s podatki (angl. monitoring)

Zadnja faza v anatomiji sistema SIEM je način interakcije z dnevniki, ki so shranjeni v njem. Ko so enkrat vsi dnevniki v SIEM-u in so dogodki že obdelani, je treba narediti nekaj koristnega z informacijami, sicer bo SIEM služil le za skladiščenje teh dnevnikov.

SIEM ima vmesniško konzolo, ki deluje kot spletni vmesnik ali pa aplikacija, ki je naložena na delovni napravi. Oba vmesnika omogočata interakcijo s podatki, shranjenimi v SIEM-pomnilniku. Prav tako omogočata tudi upravljanje samega SIEM-a. Sistemskim in varnostnim inženirjem ni treba preverjati dnevnikov v različnih napravah, saj SIEM poskrbi za normalizacijo in so ti dnevniki v enem formatu.

Poglavje 4

Sistem AlienVault

AlienVault OSSIM (Open Source Security Information Management) je sistem, ki vsebuje zbirko orodij za pomoč skrbnikom omrežij pri zagotavljanju računalniške varnosti ter odkrivanju in preprečevanju vdorov. AlienVault ponuja učinkovit pristop k sistemu SIEM in je odprtokodna programska oprema, katero lahko brezplačno prenesemo in uporabljamo. Brezplačna različica ima nekaj omejitev, ki vključujejo zmogljivost, hrambo podatkov in podporo s strani tehničnega oddelka. V primeru potrebe po dodatni zmogljivosti pa je na voljo tudi profesionalna različica.

Cilj projekta je zagotoviti celovito zbirko orodij, ki bi skrbniku omogočala pregled vseh varnostnih vidikov njegovega sistema. AlienVault ima podrobno zgrajen uporabniški vmesnik, kot tudi učinkovito izgradnjo poročil o incidentih. Sposobnost, da deluje kot preprečevalec vdorov v sisteme, ki temelji na korelaciji podatkov, ga odlikuje kot uporabno varnostno orodje.

Danes je na voljo veliko preizkušenih odprtokodnih orodij in AlienVault jih združuje v celovito rešitev za varnostne operacije. Na vrh odprtokodnih orodij je dodano orodje za okvirno oceno tveganja, orodje za poročanje o dogodkih in orodje za upravljanje samega sistema. Rezultat tega je povezana platforma, ki na vizualni oz. posplošen način prikazuje podatke, ter omogoča varnostnim analitikom spremljanje na milijone dogodkov in možnost, da se osredotočijo na podatke, ki so zares pomembni. AlienVault prav tako omogoča izbiro orodij, ki bi bila za določenega uporabnika najbolj ustrezna.

4.1 Odprtokodna orodja

Orodja open source nudijo večjo prilagodljivost in omogočajo organizacijam zmanjšanje stroškov ter povečanje talenta na tisoče programerjev. Večina organizacij že uporablja neke vrste odprte varnostne aplikacije. Več kot 15 najboljših odprtokodnih

orodij je zbranih v sistemu AlienVault, nekaj bolj pomembnih pa je na kratko opisanih v nadaljevanju.

- **Snort** je odprtokodni omrežni paket za zaznavanje in preprečevanje vdorov. Uporablja se za zaznavanje več vrst napadov, kot so prekoračitev vmesnika, pregledovanje vrat, zbiranje sledi in preiskovanje ter veliko več. Omogoča sporočanje v realnem času, lahko pa ga uporabimo tudi kot sniferja ali kot omrežni sistem za preprečevanje vdorov. Prilagojena različica tega programa je vgrajena v AlienVault in zagotavlja opozorila ob poskusu napada na omrežje [12].

- **OpenVAS** je orodje, namenjeno testiranju ranljivosti omrežja. Podatke, ki jih pridobi, pošlje v SIEM. Predhodno se je OpenVAS imenoval Nessus in je bil odprtokoden, vendar so nato Nessus spremenili v novi zaprtokodni lastniški program, iz starega se je razvil OpenVAS [13].

- **Ntop** je odprtokodni program, ki omogoča spremljanje prometa znotraj omrežja.

- **Nagios** izvira iz grške besede »agios« (svetnik) in dodatka »n«, ki pomeni omrežje (networks). Nagios je brezplačen programski paket, namenjen spremljanju in nadzorovanju omrežnih naprav ter storitev.

- **PADS** je orodje za spremljanje prometa v omrežju. Na osnovi pridobljenih podatkov SIEM ugotavlja, če je prišlo do anomalije znotraj omrežja.

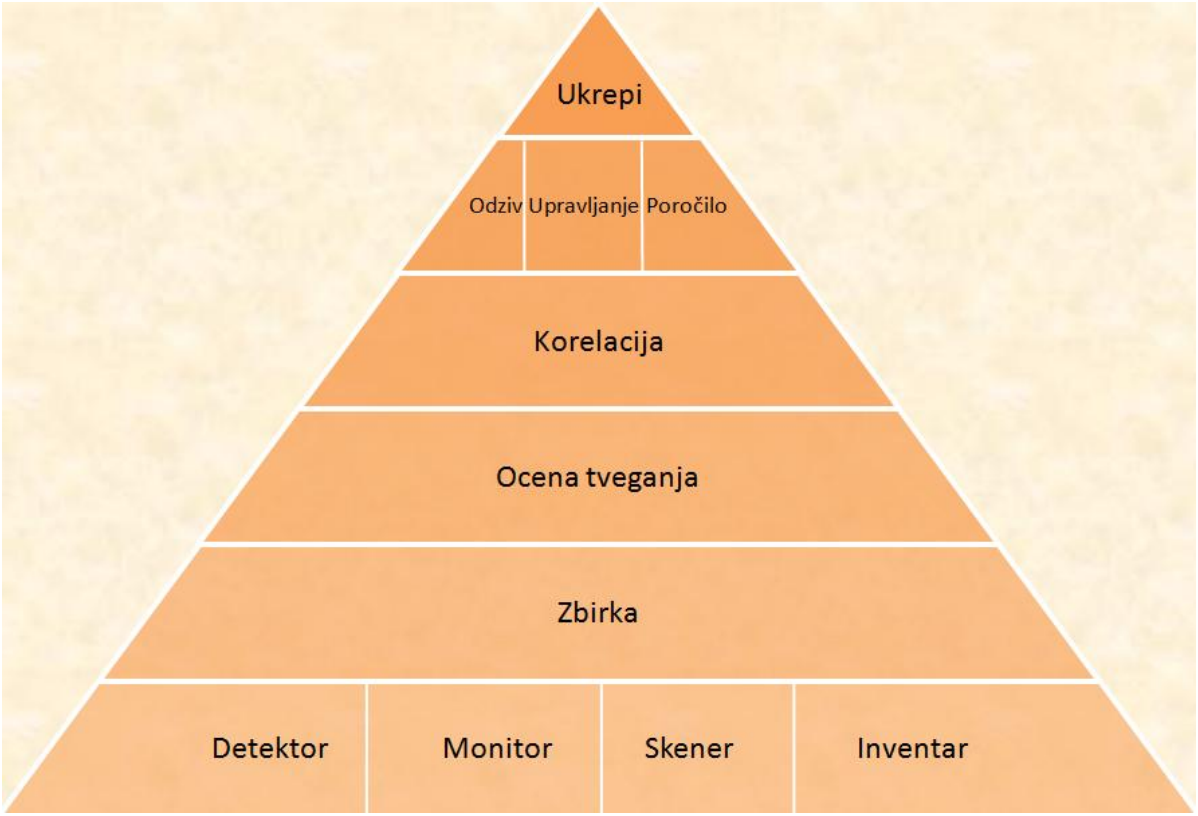
- **P0f** je program, ki se uporablja za pasivno preiskovanje in zaznavanje vrste ter različice operacijskih sistemov.

- **OSVDB** je odprtokodna podatkovna baza, ki hrani najnovejše podatke o ranljivosti sistemov in je vključena v AlienVault.

- **Inprotect** je spletni vmesnik za Nessus, OpenVAS in nmap. Dodan je v sistem AlienVault in ponuja možnost nastavitve profilov za skeniranje, urnik skeniranja ter izvoz rezultatov skeniranja v različnih formatih.

4.2 Funkcionalnost

OSSIM je več kot vsota vseh njegovih delov, saj je AlienVault ob združenju teh orodij ustvaril pravo sinergijo. Slika 4.1 prikazuje sodelovanje teh orodij od najnižje do najvišje ravni.



Slika 4.1: Struktura sistema OSSIM

4.2.1 Detektor (angl. detect)

Detektor lahko opišemo kot nek program, ki posluša na omrežju, spremlja datoteke ali dnevnike in preverja morebitne napade ter v takšnem primeru sproži alarm.

4.2.2 Monitor (angl. monitor)

OSSIM uporablja monitor za pregled omrežnega prometa in hitro iskanje sprememb oz. anomalij v omrežju. V uporabi so tri vrste monitorjev:

1. **Omrežni**: spremlja količino prenosa v bajtih (angl. bytes) skozi neko časovno obdobje.
2. **Monitor dosegljivosti**: služi za zaznavanje DoS napadov ali pa izpadov omrežja.
3. **Prilagodljiv monitor**: možno je nastaviti profil na ta način, da zazna vse, kar nas zanima.

4.2.3 Skener (angl. scan)

V tem primeru gre za pregledovanje oz. skeniranje ranljivosti omrežja. Ta izvede simulacijo napadov in ugotovi, ali je kakšna omrežna naprava občutljiva na določeno vrsto napada. V tem primeru se uporablja orodje OpenVAS.

4.2.4 Inventar (angl. inventory)

Inventar predstavlja samodejno ali ročno zbiranje podatkov, ki se shranjujejo na strežniku.

4.2.5 Zbirka (angl. collect)

Služi za zbiranje podatkov in informacij z varnostne naprave, ki se shranjujejo na strežniku za nadaljnjo obdelavo.
Obstajata dva načina pridobivanja informacij iz varnostne naprave:

- t. i. push metoda ali potisna metoda, ki »potisne« podatke iz varnostne naprave na strežnik v izvornem formatu;
- t. i. pull metoda ali magnetna metoda, predstavlja na varnostni napravi nameščeno programsko opremo, ki služi za prenos podatkov od varnostne naprave do strežnika.

4.2.6 Ocena tveganja (angl. risk assesment)

Ocena tveganja je postopek merjenja tveganj, ki poskuša ugotoviti, kaj je pomembno in kaj ne. Ocena tveganja se uporablja kot pripomoček pri procesu odločanja. OSSIM izračuna tveganje za vsak dogodek.

4.2.7 Korelacija (angl. correlation)

Najpomembnejši vidik katerega koli orodja SIEM je korelacijski proces. Njegova naloga je zmanjševanje lažnih alarmov in preprečevanje lažno negativnih alarmov.

4.2.8 Odziv (angl. respond)

AlienVault se lahko samodejno odzove na nek dogodek ali na niz dogodkov. Odzivi so lahko pošiljanje elektronske pošte ali pošiljanje nastavitev požarnim zidovom s prilagojenimi nastavitvami.

4.2.9 Upravljanje (angl. manage)

Ko je ugotovljeno, da gre za napad in je znana ocena tveganja, se ustvari zaznamek (ticket), ki spremlja incident.
Sam zaznamek je lahko kreiran iz več mest:

- iz alarmne konzole (alarm panel),
- forenzične konzole ali
- konzole tveganja (risk dashboard).

Vsak zaznamek vsebuje podatke o lastniku incidenta, dogodkih, pristnih v incidentu, trenutni status incidenta in zgodovino incidenta. Sam zaznamek je shranjen v podatkovni bazi, kateri se lahko uporabi za kasnejše analize in poročila.

4.2.10 Poročilo (angl. report)

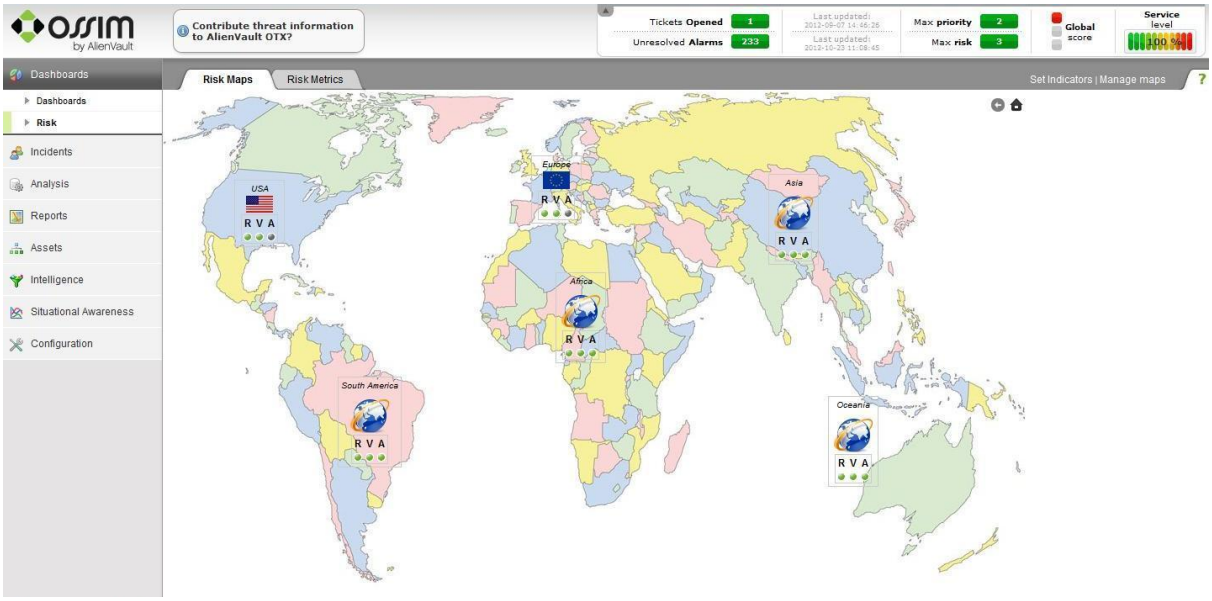
Sistem AlienVault omogoča izdelavo kakovostnih poročil, ki se kasneje uporabljajo za analizo. Poročila je mogoče generirati za različne tipe varnostnih groženj, različna časovna obdobja in za različna področja varnosti.

4.2.11 Ukrepi (angl. measure)

Nadzorne plošče so na voljo za vizualno predstavitev podatkov, ki je lažje razumljiva. AlienVault ima standardno nadzorno ploščo, ki pa jo lahko uporabnik prilagaja svojim potrebam. Vsak uporabnik lahko izbere nadzorno ploščo, ki mu omogoča, da izpolni zahtevane naloge bolj učinkovito.

4.3 Uporabniški vmesnik

Posebno pozornost pri razvoju sistema AlienVault je bil deležen spletni oz. uporabniški vmesnik. Grob oris uporabniškega vmesnika je prikazan na sliki 4.2. V nadaljevanju pa bodo nekoliko bolj podrobno predstavljene njegove funkcionalnosti.



Slika 4.2: Uporabniški vmesnik sistema OSSIM

4.3.1 Nadzorna plošča (angl. dashboard)

Nadzorna plošča omogoča pregled in analizo podatkov ter hiter pregled varnostne ogroženosti. Zato bi lahko rekli, da je izhodišče za bolj poglobljeno analizo. Širok nabor različnih pogledov in načinov predstavitve podatkov v vizualni obliki so resnično osupljivi. Nadzorna plošča ima dve podstrani:

- nadzorne plošče: te prikazujejo različne poglede nad varnostjo v omrežju ter najbolj napadane IP-naslove in vrata;
- ogroženost: tu je prikazan zemljevid najbolj ogrožanih območij in meritev ogroženosti.

4.3.2 Pripetljaji (angl. incident)

Stran s pripetljaji prikazuje dogodke, ki so bili zaznani oz. obravnavani kot grožnja. V ta namen je stran razdeljena na tri podstrani:

- Aarms: podstran prikazuje zaznane napade, ki jih je AlienVault kategoriziral kot možne napade;
- Tickets: dogodki, ki jih je skrbnik označil kot potencialne nevarnosti;
- Knowledge database: predstavlja bazo preteklih dogodkov, v kateri so opisane določene vrste napadov.

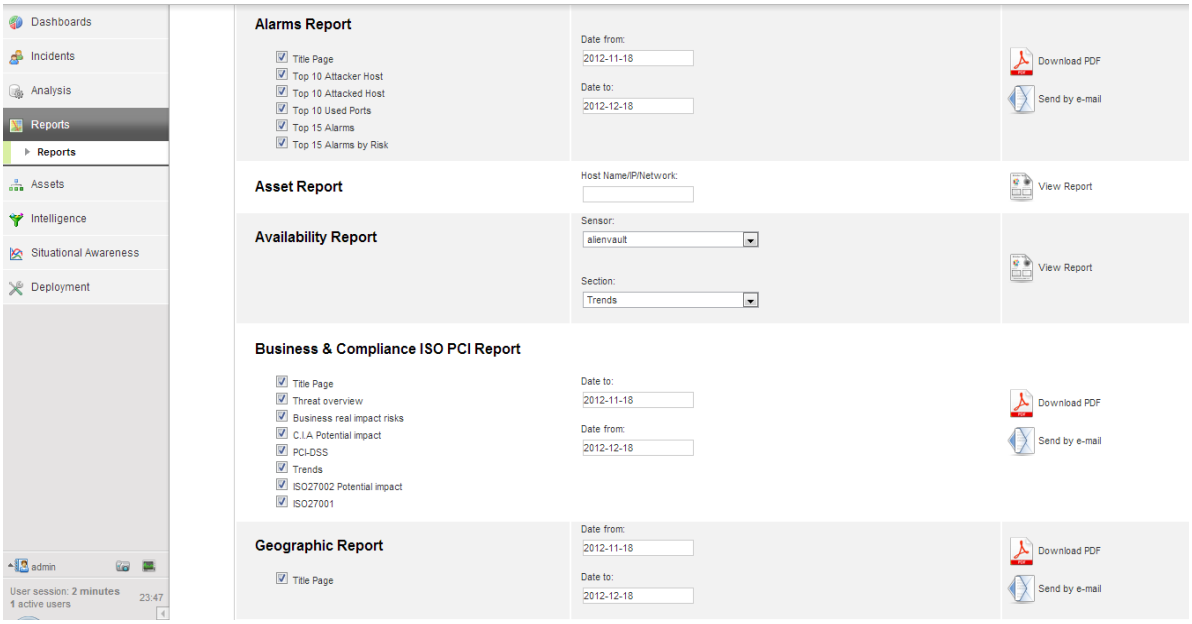
4.3.3 Analiza (angl. analysis)

Na tej strani si lahko ogledamo dogodke, ki so bili analizirani s sistemom AlienVault. Sama stran je razdeljena na več podstrani:

- Security events – prikazuje varnostne dogodke, zbrane iz različnih senzorjev;
- Vulnerabilities – prikazuje dogodke, ki so bili zaznani kot vdori oz. napadi;
- Anomalies – vsi dogodki, zbrani iz različnih detektorjev, vgrajenih v OSSIM, so zabeleženi na tej podstrani.

4.3.4 Poročila (angl. reports)

Na tej strani je mogoče generirati poročila po meri. Lahko izbiramo različne vrste napadov in časovna obdobja, za katere bi želeli, da nam sistem AlienVault ustvari poročilo (slika 4.3). Prav tako nam uporabniški vmesnik omogoča grafični ali pa tekstovni prikaz podatkov in izvoz poročil v obliki datoteke.



Slika 4.3: Prikaz možnosti za generiranje različnih tipov poročil

4.3.5 Sredstva oziroma viri (angl. assets)

Ta stran je poglavitna za določanje naprav ali omrežij, katere AlienVault nadzira s svojimi senzorji in poroča ob morebitnih napadih oziroma anomalijah. Če želimo, da AlienVault prejme dnevniške datoteke o dogodkih iz neke naprave, je tukaj potrebno to napravo dodati na seznam. Za to, da bi jo dodali, pa je treba vedeti njen IP-naslov, obenem pa izberemo še, na kateri senzor bo pošiljala dnevniške datoteke in kakšno bo njeno ime. Assets je glavno okno za dodajanje novih naprav ali pa povezovanje teh v večjo skupino. Prav tako omogoča tudi dodajanje omrežij in omrežnih vrat v sistem za nadzor [14].

4.3.6 Obveščanje (angl. intelligence)

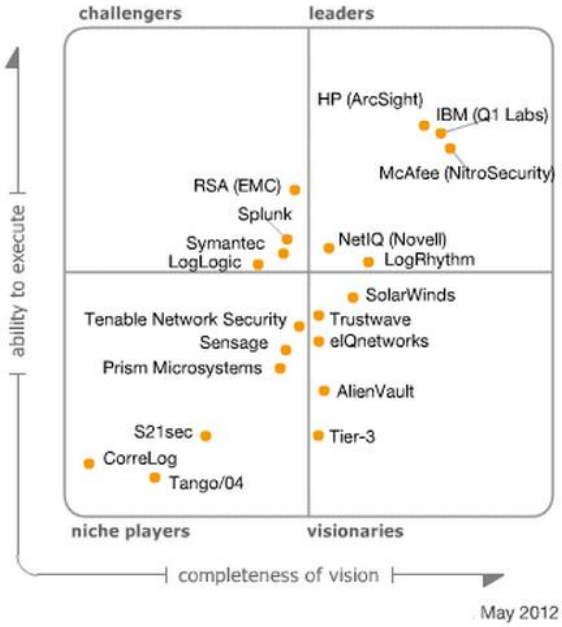
Tukaj je mogoče določiti pravila, ki jih AlienVault upošteva pri zaznavanju varnostnih groženj. Določimo lahko, kaj naj sistem naredi z dogodki, ki so bili zaznani kot morebitna grožnja. Ti se lahko shranijo v podatkovno bazo, določi se jim lahko stopnjo tveganja, zamenja prioriteto, pošlje elektronsko obvestilo ali pa se sproži nek izvršljiv ukaz.

4.4 Položaj na tržišču

Tehnologija metode SIEM podpira tri glavna področja uporabe. Ta so:

- zagotavljanje skladnosti - upravljanje z dogodki in poročanje o nepravilnostih;
- obvladovanje groženj - spremljanje aktivnosti uporabnikov v realnem času, upravljanje incidentov, izvajanje korelacij in analiz;
- polna SIEM-funkcionalnost - kombinacija obeh možnosti (zagotavljanje skladnosti ter obvladovanje groženj).

Na trgu je navzočih veliko sistemov za upravljanje informacij in dogodkov, ki pa se med seboj razlikujejo v zmogljivosti glede na omenjena področja uporabe. Družba Gartner je leta 2012 objavila analizo trenutnega stanja ponudnikov sistemov SIEM. Na sliki 4.4 je prikazan Gartnerjev magični kvadrant (angl. magic quadrant), ki je izdelan na podlagi že omenjene analiza, glede na dva kriterija. Prvi je zmožnost izvedbe (angl. ability to execute), ki je na osi y, in drugi vizija (angl. completeness of vision), ki je na osi x. Če kriterije še nekoliko bolj razdelimo, bi prvi zajemal storitve, ceno, splošno stanje, tržno odzivnost, operacije in uporabnikove izkušnje. Drugi kriterij pa sestavlja razumevanje trga, poslovni model, informativnost ter geografsko, proizvodno, prodajno in tržno strategijo [15].



Slika 4.4: Gartnerjev magični kvadrant ponudnikov sistema SIEM (maj 2012)

Magični kvadrant je razdeljen na štiri dele:

1. **Vodje (angl. leaders) -** imajo veliko število strank, večji tržni delež, boljšo prodornost in izdelano dolgoletno vizijo.
2. **Izzivalci (angl. challengers) -** imajo močan tržni položaj**,** vendar zaostajajo za vodji zaradi pomanjkanja vizionarstva
3. **Nišni ponudniki (angl. niche players) -** osredotočeni so na ponudbo z določenega geografskega področja.
4. **Vizionarji (angl. visionaries) -** osredotočeni so na prihodnost in uporabo nove tehnologije, vendar imajo manjšo finančno moč.

AlienVault se je poleg ostalih štirih sistemov (SolarWinds, Trustwawe, elQnetworks, Tier-3) to leto znašel med vizionarji, medtem ko je bil po raziskavi, opravljeni leta 2011, med nišnimi ponudniki.

Njegove prednosti na podlagi opravljene analize so: integriran SIEM, spremljanje celovitosti datotek, ocena ogroženosti ter zmožnost nadzora končnih točk in odkrivanje vdorov. Po mnenju strank je AlienVault precej cenejši od večine ostalih SIEM-ponudnikov. Slabosti so v tem, da nima upravljanja identitet in dostopa (angl. identity and access management) pri aktivnem spremljanju imenika ter možnost integracije sistema predvsem z odprtokodnimi aplikacijami.

Poglavje 5

Prikaz delovanja sistema AlienVault

V tem poglavju bom na konkretnem primeru predstavil delovanje sistema AlienVault. Opisal bom strojne zahteve za samo delovanje in namestitev sistema. Prikazal bom, kako se ga nastavi, da z določenih naprav prejema dnevniške datoteke. Opisal bom tudi postopek, kako sem generiral različna poročila o varnostnih grožnjah. Pri tem bom tudi prikazal, na kakšen način nas lahko sistem obvešča ob morebitnih poskusih vdora, ter katere naprave so najbolj ogrožene, katera vrata najbolj napadana in kateri IP-naslovi so največkrat izvor napadov. Pred tem bom na kratko povzel glavne značilnosti sistema OSSIM.

Zunanje naprave in aplikacije beležijo dogodke v dnevniške datoteke, ki se kasneje posredujejo v sistem AlienVault. Ta jih shrani v zbirko dnevniških zapisov, nad katero se opravi filtracija dogodkov. Vsak dogodek mora iti še skozi normalizacijo, da se ga pretvori v standardno obliko in se mu določi prioriteta. Nato se dogodke pošlje v osrednji strežnik (SIEM). Ta poskrbi, da se izvede ocena tveganja za posamezen dogodek in se jih shrani v podatkovno bazo.

Poleg zbiranja informacij, s pomočjo dnevniških datotek iz zunanjih aplikacij in naprav, AlienVault omogoča še spremljanje prometa znotraj omrežja, s pomočjo senzorjev. Ti z različnimi metodami pregledujejo promet znotraj omrežja, pri tem pa ne vplivajo na učinkovitost delovanja samega omrežja. Senzorji omogočajo zaznavo vdorov, anomalij, ranljivosti in pregled sistemov.

Potem je tukaj še spletni vmesnik, ki zagotavlja učinkovit sistem sporočanja, opravljanja meritev, izdelovanja poročil, spremljanje ranljivosti na omrežju v realnem času ter še mnogo uporabnih funkcij. Dostop do spletnega vmesnika je varovan z vnaprej določenim uporabniškim imenom in geslom. Dostopati je možno tudi zunaj lokalnega omrežja, preko varne povezave.

5.1 Sistemske zahteve in namestitev sistema AlienVault

AlienVault je brezplačna odprtokodna programska oprema, ki je na voljo na uradni spletni strani http://www.alienvault.com. Sistem lahko prenesemo s klikom na neposredno povezavo za prenos datoteke, ki je shranjena v formatu ISO. To je oblika datotečnega zapisa, ki predstavlja sliko optičnega medija.

Sistem je uporabnikom dostopen že nekaj let, zato je izdan v več različicah. Zadnja različica je 4.0, katero sem tudi sam namestil na strežnik v laboratoriju za računalniške komunikacije. Prva razlika, ki sem jo opazil v primerjavi s prejšnjo 3.0, je bila ta, da nima možnosti za namestitev na napravah, ki imajo vgrajen 32-bitni procesor. Tako, da je prvi pogoj za delovanje sistema 64-bitni procesor. Ostale strojne zahteve pa so odvisne predvsem od števila dogodkov na sekundo in prepustnosti omrežja, ki ga želimo zavarovati. Priporočljivo je imeti vsaj 4 GB RAM-a in mrežno kartico, ki je podprta z gonilnikom e1000.

Namestitev sistema je dokaj preprosta in ponuja dva tipa namestitev, in sicer samodejno ali uporabniško. Pri samodejni namestitvi so določene funkcije in lastnosti vnaprej določene, kar uporabniku občutno olajša namestitev. V tem primeru je poleg jezika in države treba določiti le še IP-naslov, masko omrežja, privzeti prehod, DNS-strežnike in geslo za dostop. Sam sem izbral samodejno namestitev, bolj izkušeni uporabniki pa lahko izberejo uporabniško namestitev, kjer je mogoče nastaviti različne profile delovanja, dodatke ipd.

5.2 Prijava v sistem

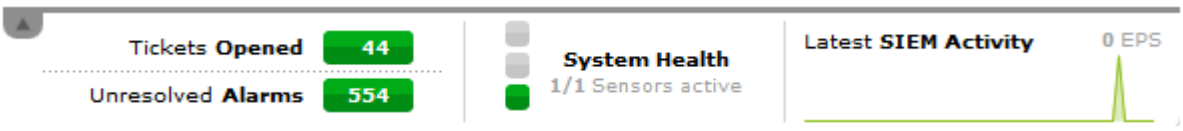
Po uspešni namestitvi sistema je sledila prijava preko spletnega vmesnika. To storimo tako, da v brskalnik vpišemo IP-naslov, ki je dodeljen strežniku. V mojem primeru je bil to zunanji IP, tako da sem lahko dostopal do sistema AlienVault tudi iz drugih lokacij, brez dodatnih nastavitev za oddaljeni dostop. Po vnosu IP-naslova in potrditvi se odpre vpisna stran (slika 5.1), ki za nadaljevanje zahteva pravilen vnos uporabniškega imena ter gesla.

Slika 5.1: Prikaz strani za prijavo v sistem

5.3 Pregled varnostnih groženj in opozoril

Po uspešni prijavi v spletni vmesnik se takoj pojavi nadzorna plošča, na kateri je prikazano varnostno stanje omrežja, ki ga nadzoruje AlienVault.

Na sliki 5.2 je prikazano število odprtih zaznamkov, ki so bili dodeljeni uporabnikom. V mojem primeru jih je bilo 44. V spodnjem delu slike je navedeno število še nerešenih alarmov, ki niso bili posredovani uporabnikom v reševanje. Ugotovimo lahko, da je številka kar precej visoka in je število nerešenih alarmov kar 554. Tukaj moram opomniti, da je ta številka seštevek vseh alarmov, ki jih je AlienVault zabeležil v enem mesecu. Poleg je navedeno število aktivnih senzorjev. V mojem primeru je le eden, saj sem sistem namestil le na en strežnik. Povsem na desni strani slike pa vidimo zadnje SIEM-aktivnosti.

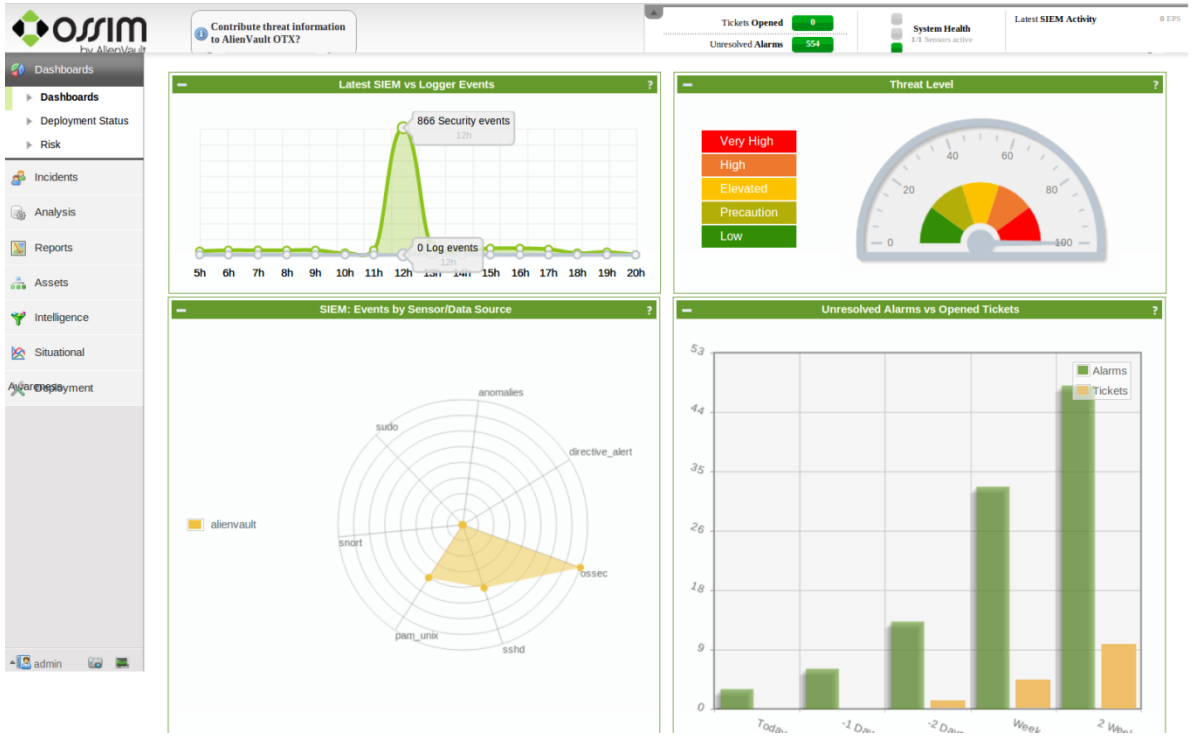


Slika 5.2: Hitri prikaz varnostnega stanja

Na sliki 5.3 lahko vidimo graf varnostnih dogodkov, ki jih je AlienVault zaznal v preteklih urah ali pa so mu bili posredovani v obliki dnevniških datotek iz sistemov in aplikacij. V mojem primeru je vidno, da je bilo ob 12. uri zabeleženih 866 dogodkov, pri

tem pa ni bilo prejetega nobenega dogodka iz dnevniških datotek s strani naprav v omrežju. Takoj poleg je graf, z imenom Threat Level, ki predstavlja stopnjo ogroženosti naprav v omrežju. Ta prikazuje najvišjo stopnjo, kar uporabniku takoj pove, da je treba ukrepati. Sledi krožni diagram, ki prikazuje število dogodkov, ki so jih zabeležili različni senzorji ali pa so bili posredovani kot dnevniške datoteke v podatkovno skladišče. V mojem primeru je največ dogodkov zaznal OSSEC, ki je zabeležil vpise v sistem z neveljavnim uporabniškim imenom.

Poleg krožnega diagrama je stolpičast diagram, ki prikazuje število nerešenih alarmov in odprtih zaznamkov. Iz slike lahko razberemo, koliko je še odprtih alarmnih obvestil v primerjavi z obvestili, ki so bili že posredovani v preverbo.



Slika 5.3: Nadzorna plošča z grafičnim prikazom

5.4 Analiza varnostnih obvestil in kreiranje »zaznamkov«

Alarmi (angl. alarms)

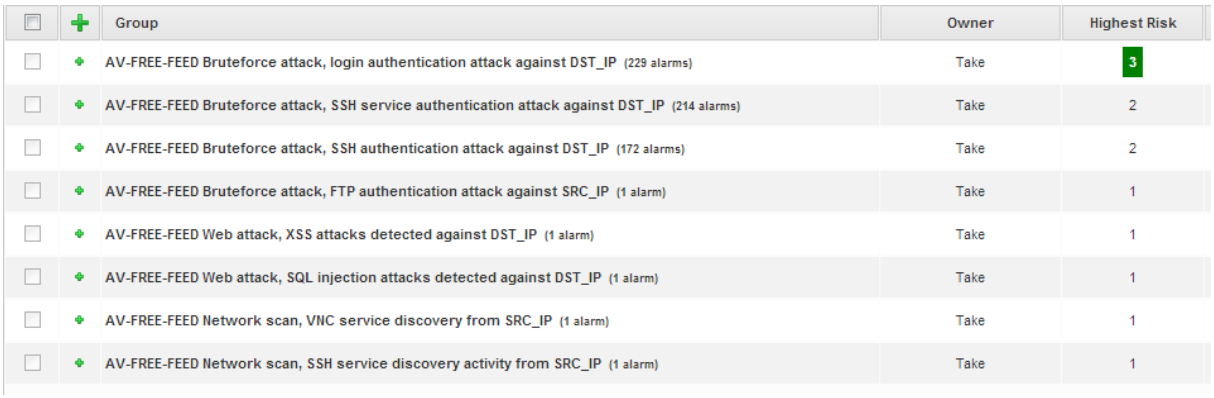
Alarmi so dogodki, ki imajo oceno tveganja večjo od 1. Lahko gre le za en dogodek ali pa celo serijo dogodkov, ki so zajeti v neko celoto. Če se nek dogodek zabeleži v SIEM, to še ne pomeni, da se bo kreiralo alarmno obvestilo. Najprej se bo izračunala ocena tveganja nad dogodkom oz. množico dogodkov in če bo ta višja kot 1, se bo sprožil tudi alarm. Slika 5.4 prikazuje zadnje alarme, ki so bili sproženi. Vsak vsebuje neke splošne lastnosti, kot so ime, število dogodkov, ocena tveganja, trajanje napada, izvorni IP, napadeni IP in pa status, ki je lahko odprt ali pa zaprt.

View Grouped (1-50) Next 50 >> Apply label to selected alarms

Signature	Events	Risk	Duration	Source	Destination	Status
Thursday 21-Feb-2013 [Delete]						
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	214	1	13 mins	125.63.72.118:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	116	1	3 hours	125.63.72.118:58705	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	7	1	10 mins	125.63.72.118:54276	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	139	1	16 mins	113.107.101.234:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	3	1	2 mins	216.19.223.55:48792	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	328	1	18 mins	216.19.223.55:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	328	1	18 mins	216.19.223.55:58830	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	28	1	3 mins	117.79.91.214:59609	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	43	1	5 mins	117.79.91.214:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	1	1	1 sec	117.79.91.214:42807	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	2	1	1 min	61.115.240.23:35151	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	29	1	2 mins	61.115.240.23:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	29	1	2 mins	61.115.240.23:59909	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	1	1	2 secs	121.8.154.35:45081	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	81	1	8 mins	121.8.154.35:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	41	1	4 mins	121.8.154.35:43007	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	128	1	6 mins	212.11.92.28:45379	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH authentication attack against 88.200.24.236	1	1	1 sec	212.11.92.28:42539	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	128	1	6 mins	212.11.92.28:ANY	88.200.24.236:ANY	open
Wednesday 20-Feb-2013 [Delete]						
AV-FREE-FEED Bruteforce attack, login authentication attack against 88.200.24.236	31	1	2 mins	198.7.63.104:ANY	88.200.24.236:ANY	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	31	1	2 mins	198.7.63.104:46016	88.200.24.236:ssh	open
AV-FREE-FEED Bruteforce attack, SSH service authentication attack against 88.200.24.236	166	1	13 mins	211.110.6.148:48991	88.200.24.236:ssh	open

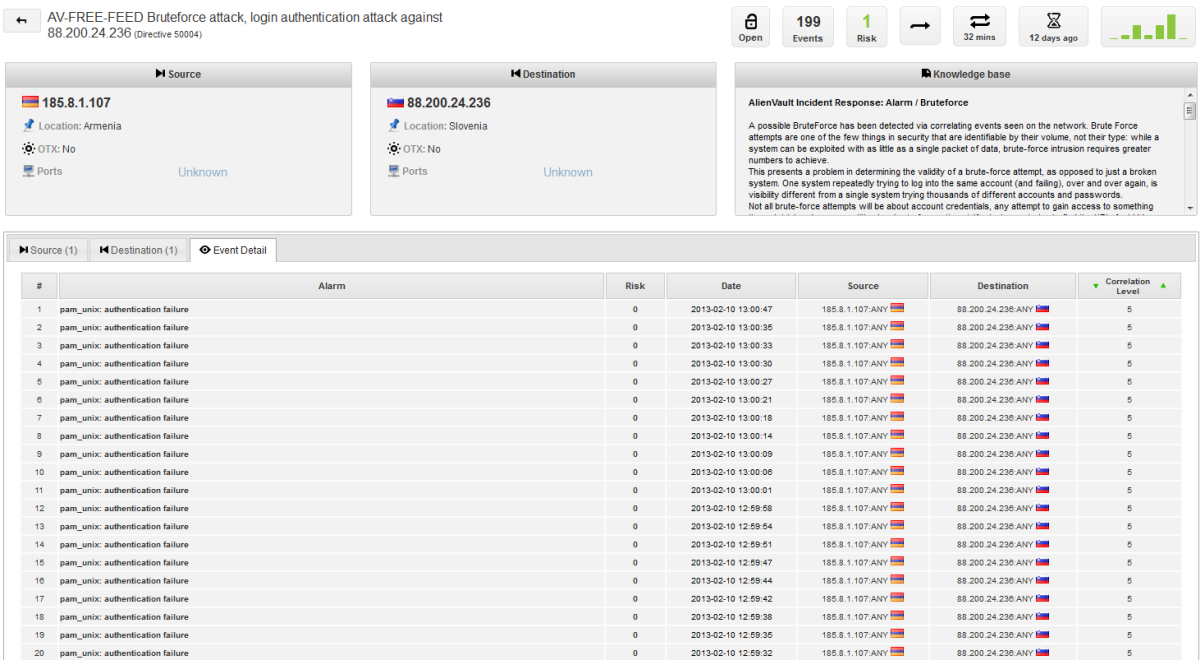
Slika 5.4: Časovni pregled alarmnih obvestil

Poleg tega, da je možno preko filtra poiskati točno določene alarme, jih je prav tako možno porazdeliti tudi v skupine, glede na tip varnostne grožnje. Na sliki 5.5 so prikazane varnostne grožnje, ki jih je v mojem primeru zaznal AlienVault.



Slika 5.5: Prikaz zaporednega pogleda obvestil

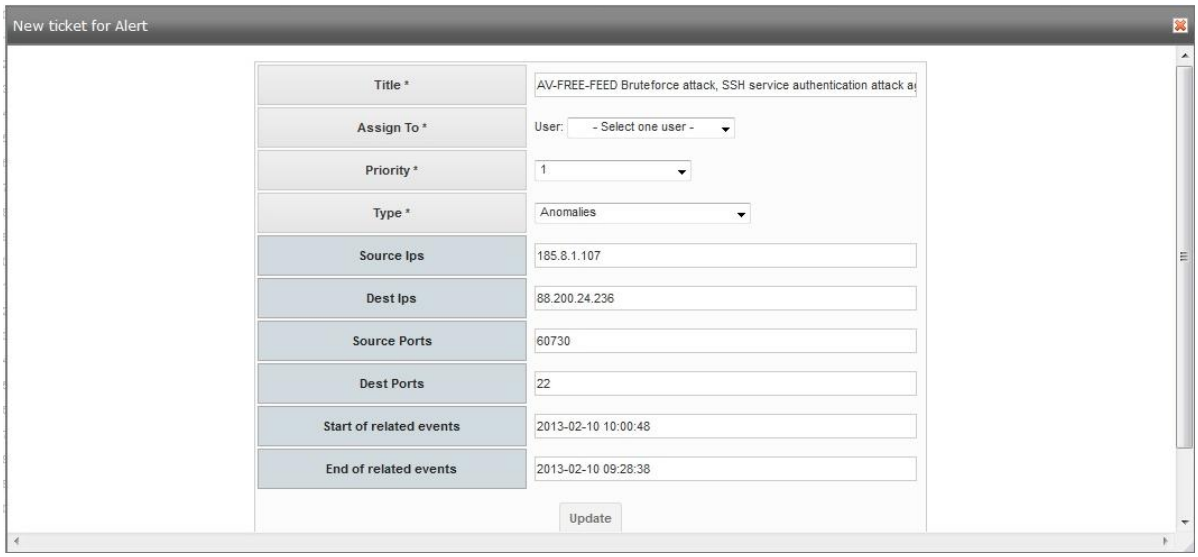
Ko izberemo določen alarm, ki nas zanima, se odprejo vse podrobnosti o njem. Slika 5.6 prikazuje zaznan alarm na sistemu AlienVault, ki sem ga imel nameščenega v laboratoriju za računalniške komunikacije. Vidimo lahko, da je izvor napada IP-naslov 185.8.1.107 in da pripada IP-rangu, ki je dodeljen za Armenijo. Trenuten status je odprt, ker še ni bil obravnavan. Dolžina trajanja napada je bila 32 minut in minilo je že 12 dni, od kar je bil sprožen. Takoj poleg nam AlienVault prikaže še kratek opis problema oz. predstavitev, za kakšno vrsto grožnje gre. V spodnjem delu okna je zabeležen vrstni red dogodkov in če bolj nazorno pogledamo, opazimo, da gre za veliko število le teh in da je časovna razlika med njimi le tri sekunde. To nam že v samem opisu potrjuje, da gre za napad z grobo silo (angl. brut force attack), kjer se je napadalec s poskušanjem različnih kombinacij gesel želel vpisati v sistem. Povsem na dnu okna pa imamo možnost zapreti alarm, v kolikor gre za lažnega oz. nepomembnega, ali pa kreirati zaznamek, ki se ga dodeli uporabniku, da bolj natančno razišče nastalo situacijo in dodatno preveri možnost varnostnega tveganja. V nadaljevanju je opisan postopek, na kakšen način lahko to storimo.



Slika 5.6: Prikaz zaporednega pogleda obvestil

Zaznamki (angl. tickets)

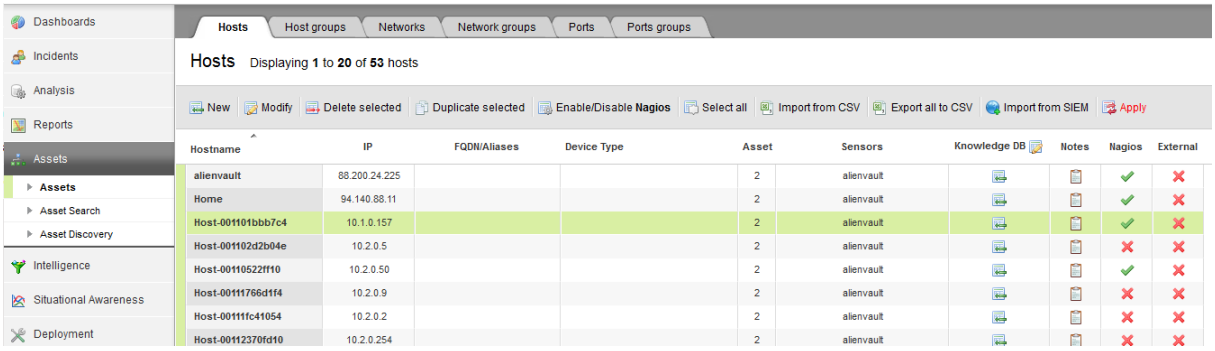
Sistem zaznamkov omogoča uporabnikom, da se poglobijo in raziščejo težave, odkrite s sistemom AlianVault. V nadaljevanju bom opisal postopek, kako sem na osnovi alarma kreiral zaznamek. Zaznamek se lahko odpre in dodeli uporabniku ročno ali pa samodejno ob zaznani nevarnosti. Na prvem mestu je že samodejno vpisan naslov, v katerem je zabeležena vrsta varnostne grožnje, in ime senzorja, ki jo je zaznal (slika 5.7). Vsakemu zaznamku je treba določiti, komu ga dodeljujemo. Naslednji korak je določitev prioritete. Ta se označuje s številkami od 1 do 10, slednja pomeni, da je prioriteta najvišja in je treba takoj ukrepati. Potem sledita IP-naslov in številka vrat izvora grožnje ter ogrožene naprave. V mojem primeru je ogrožena naprava kar sistem AlienVault in vrata številka 22. Na koncu je zabeležen še čas in datum začetka ter konca zaznane grožnje. Lahko vidimo, da je šlo za napad, ki je trajal dobre pol ure. Vse skupaj pa se po kliku na gumb »update« pošlje dodeljenemu uporabniku z možnostjo dopisa obrazložitve problema.



Slika 5.7: Prikaz kreiranja zaznamka

5.5 Nastavitev delovanja sistema AlienVault

Omenjeno je že bilo, da ima AlienVault vgrajene mehanizme za nadzorovanje omrežja in zaznavanje varnostih groženj. Vendar, če želimo, da senzorji sistema AlienVault nadzorujejo določeno omrežje ali napravo v omrežju in sprejemajo dnevniške datoteke iz teh naprav, potem je treba to tudi nastaviti v sistemu. Tako ima uporabniški vmesnik meni z imenom »Assets«, kar bi v prevodu pomenilo »viri« (slika 5.8). Notri lahko dodajamo naprave, skupine naprav, omrežja, skupine omrežij, vrata in skupine vrat, ki jih AlienVault nadzoruje. Za vsako izmed teh je mogoče določiti ime naprave, njen IP-naslov, senzor, način pregledovanja in mnoge druge lastnosti.



Slika 5.8: Prikaz okna za dodajanje naprav in omrežij v SIEM

Če želimo dodati novo napravo v bazo AlienVault, izberemo zavihek »host«. Odpre se nam okno, v katerem napišemo njeno ime, IP-naslov, ime domene, kratek opis in izberemo senzor, ki bo spremljal njeno delovanje. Naprave lahko v poljubnem vrstnem redu tudi urejamo in brišemo. AlienVault prav tako omogoča dodajanje več naprav v skupino. Na ta način je delo z njimi bolj poenostavljeno in pregledno. Ena izmed prvih stvari, ki jih je treba že v začetku nastaviti, je dodajanje vseh omrežij na seznam, ki jih bo AlienVault nadzoroval. Na ta način bo imel krajši čas za procesiranje dogodkov, ki so nastali v teh omrežjih. Vsako omrežje mora biti povezano z najmanj enim senzorjem. Vsak senzor pa bo zbiral dogodke ali pa spremljal promet izbranega omrežja.

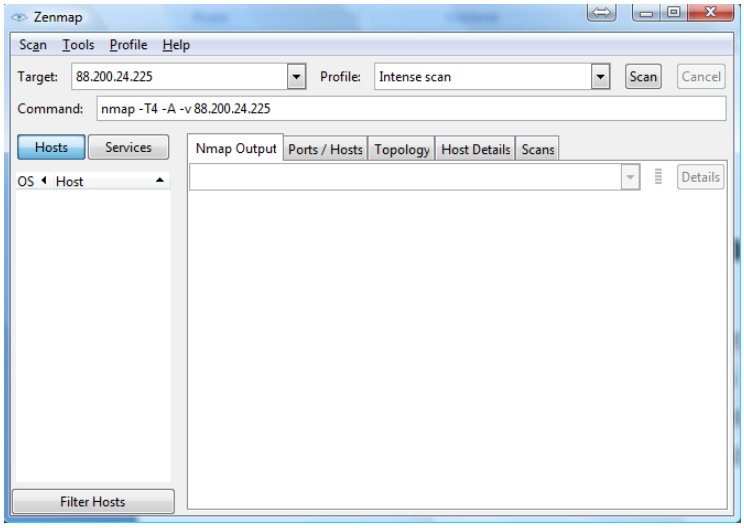
Dodajanje omrežij je na voljo pod zavihkom »networks«. Omrežju dodamo ime, IP-naslov in masko omrežja ter mu prav tako določimo senzor, ki ga bo spremljal. Tako kot naprave je tudi omrežja možno dodajati v skupine, jih urejati in brisati.

AlienVault omogoča tudi nadzorovanje vrat, ki jih lahko dodajamo tako, da določimo njihovo številko in izberemo protokol.

5.6 Uporaba programa za penetracijsko testiranje

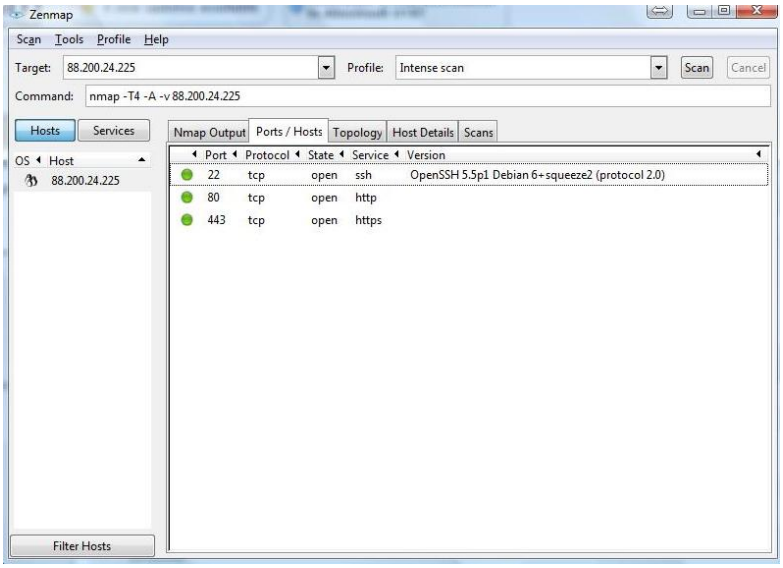
S programom Nmap, ki služi penetracijskemu testiranju, sem poskusil odkriti čim več lastnosti, ki jih imata sistem ali omrežje za javnim IP-jem. Program lahko na destinacijskem IP-naslovu preveri, katera vrata so odprta in kakšni protokoli so v njihovem ozadju, kateri operacijski sistem uporabljajo ter še veliko podrobnosti, ki bi napadalcu bile v veliko korist pri kasnejšem napadu. S programom Nmap sem preveril, ali AlienVault takšno pregledovanje naprav lahko zazna, kajti sama naprava brez dodatnih programov takega početja ne zaznava.

Po zagonu programa Nmap se odpre glavno okno programa (slika 5.9). V polje z imenom »Target«, v prevodu cilj, sem vnesel IP-naslov, nad katerim želimo izvesti pregledovanje. Uporabil sem IP-naslov, ki ga je uporabljal strežnik, na katerem je bil nameščen AlienVault. Potem sem izbral še profil oziroma določil tip pregledovanja. V tem delu je na voljo več različnih profilov. Sam sem izbral temeljito pregledovanje, ki vsebuje pregled odprtih vrat in vrsto protokola, tip operacijskega sistema, shematičen prikaz vozlišč do destinacijskega IP-naslova ipd.



Slika 5.9: Program Nmap

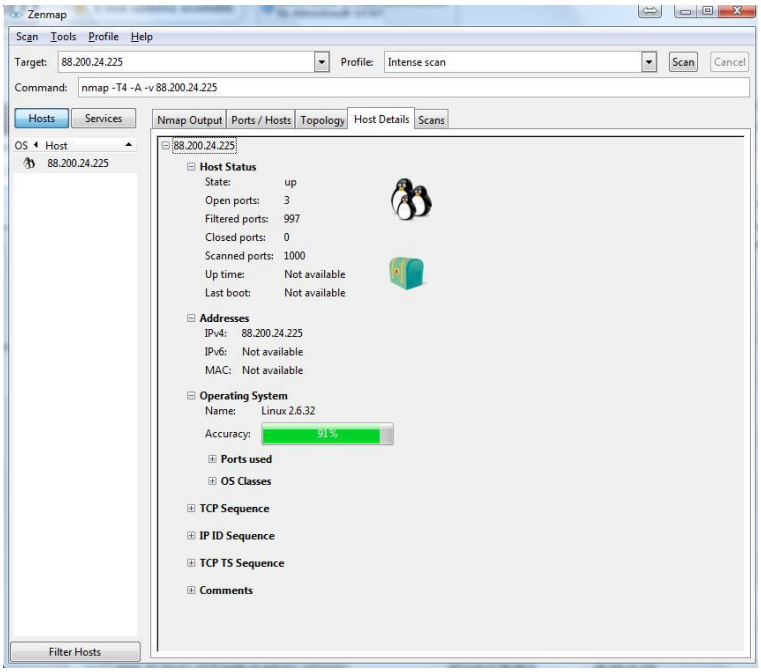
Po končanem pregledovanju mi je program Nmap kot rezultat prikazal odprta vrata na destinacijskem IP-naslovu. Na sliki 5.10 lahko vidimo, da gre za standardna vrata s številkami 22, 80 in 443. Na vratih s številko 22 vidimo, da so rezervirana za »ssh« storitev, vrata s številko 80 za »http« storitev in vrata s številko 443 za »https« storitev. To so tudi standardi, ki jih uporabljajo drugi strežniki in omrežne naprave.



Slika 5.10: Prikaz odprtih vrat

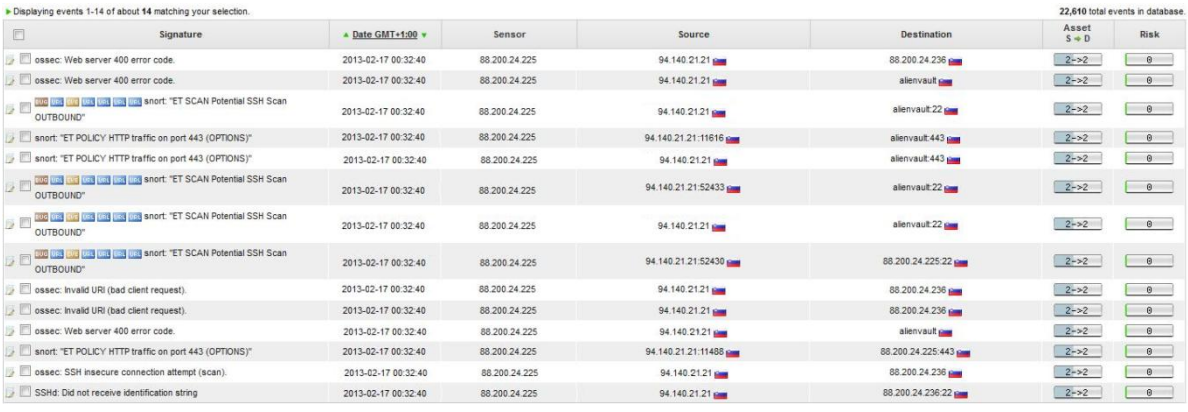
Na sliki 5.11 lahko vidimo še druge podatke o napravi. Vidno je, da je naprava

dosegljiva, število odprtih vrat je 3, število pregledanih vrat je 1.000, operacijski sitem, ki je nameščen, pa je Linux 2.6.32. Tukaj gre res za sistem Linux, saj je AlienVault razvit na različici Debian.



Slika 5.11: Prikaz podatkov o strežniku

Na sliki 5.9 vidimo, da AlienVault takšno pregledovanje tudi zazna in nas ustrezno opozori, da se na IP-naslovu 88.200.24.238 nekaj dogaja oziroma se na določenih vratih vrši pregledovanje.

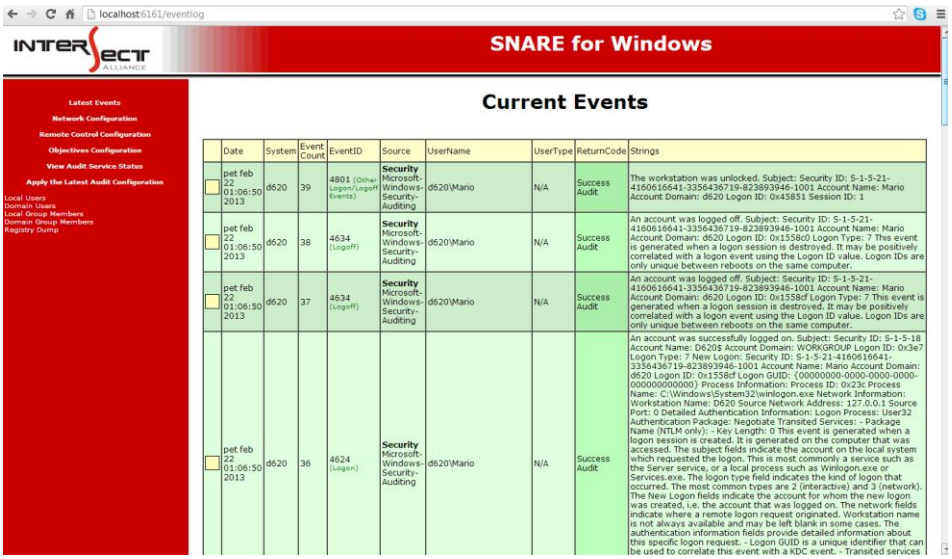


Slika 5.12: Poročilo o dogodkih

5.7 Pošiljanje dnevniških datotek v sistem AlienVault

V nadaljevanju je opisan postopek, kako sem nastavil operacijski sistem Windows, da pošilja dnevniške datoteke strežniku AlienVault. Za operacijski sistem Windows sem se odločil, ker je trenutno po odstotkih uporabnikov daleč pred vsemi ostalimi operacijskimi sistemi. Ker sistem Windows ne omogoča samodejnega načina pošiljanja dnevniških datotek, je edina rešitev uporaba programa SNARE (System iNtrusion Analysis and Reporting Enviroment) (slika 5.9). Gre za odprtokodno programsko opremo, ki se uporablja za zbiranje in pošiljanje dnevniških datotek iz različnih operacijskih sistemov. SNARE jih pošlje senzorjem iz sistema AlienVault, ki jih razčlenijo in posredujejo strežniku AlienVault. (http://www.netmarketshare.com/)

SNARE ni na voljo znotraj sistem Windows, zato ga je treba prenesti z interneta. Povezavo do strani za prenos najdemo kar na AlienVaultovem spletnem vmesniku (od 3.0 različice naprej), pod zavihkom Configuration in nato zavihkom Collection. Za starejše različice sistema AlienVault pa je na voljo pod zavihkom Tools in potem izberemo Downloads. Prenesemo obe datoteki: »Snare for Windows« in »Snare config file«. Ko sta datoteki preneseni, zaženemo »Snare setup.exe« in namestimo program. Nato pa v registru »snare_takeover.reg« preverimo, da je destinacijski IP pravilen in kaže na naš AlienVault-strežnik. Potem zaženemo »cmd« ali slovensko »ukazno vrstico« in izvršimo dva ukaza: »net stop snare« in nato še»net start snare«. Kar se tiče nastavitev v sistemu Windows, je to vse, kar je treba narediti. Sedaj je potrebno še na AlienVaultovem vmesniku nastaviti, da senzorji sprejemajo dnevniške datoteke, ki jih pošlje SNARE.

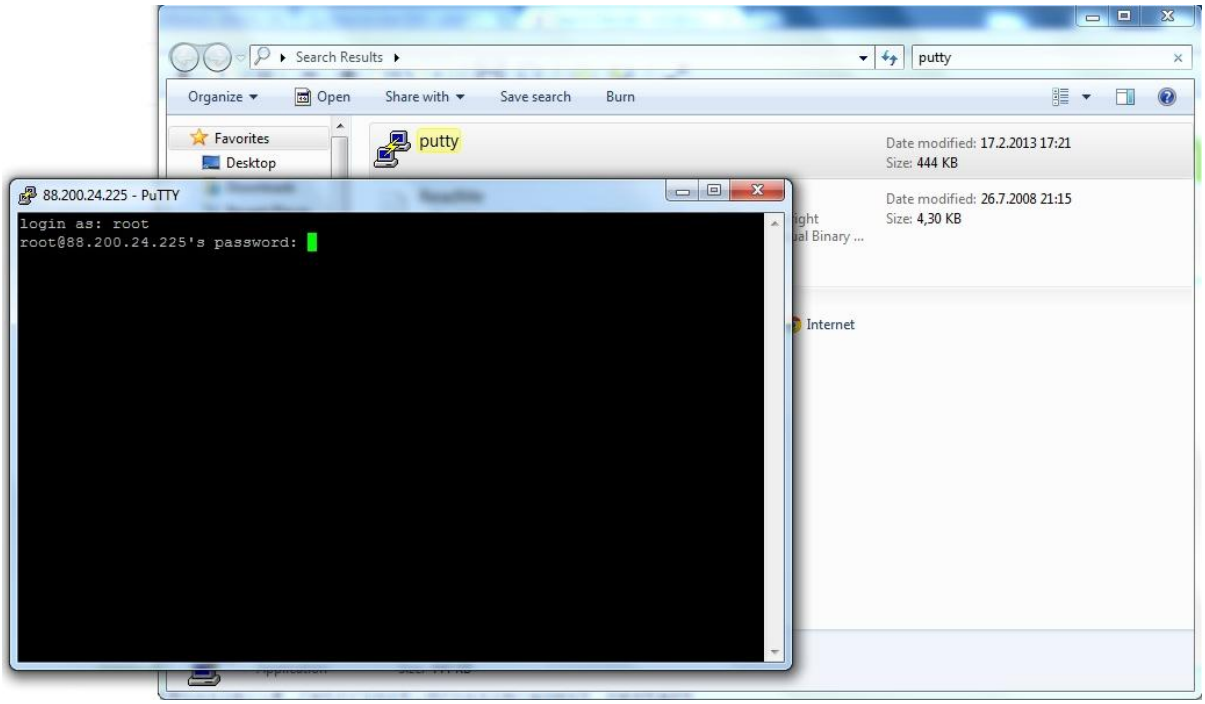


Slika 5.13: Program SNARE

Za povezavo s strežnikom sem uporabil program Putty (slika 5.10). Ta omogoča, da se preko SSH-protokola povezujemo z oddaljenimi strežniki. Za povezavo z AlienVaultovim senzorjem je treba poznati IP-naprave. Potem, ko je povezava vzpostavljena, v ukazno vrstico vnesemo ukaz »ossim-setup«. Odpre se nam glavni meni, kjer je viden »Change Sensor settings«, nato »Enable/Disable detector plugins« in na koncu označimo »snare«. To potrdimo in shranimo. Potem dodamo še Windowsov IP v datoteko /etc/host in ponovno zaženemo AlienVault.

Sedaj je AlienVault prejemal dogodke iz sistema Windows, ki jih drugače ne bi mogel pridobiti. Tudi uporabniki sistema Windows teh dogodkov ne vidijo, če ne uporabljajo dodatnih programov. Ko sem naslednjič zagnal AlienVault sem pod zavihkom »Analysis« videl IP naslov računalnika z operacijskim sistemom Windows. Dogodki, ki so bili zabeleženi so se navezovali na prijavo v sistem. AlienVault je dobil podatke, kdaj sem se prijavil v sistem, ali sem pravilno vnesel uporabniško ime in geslo, kolikokrat je bila prijava zavrnjena zaradi napačnega uporabniškega imena in gesla, ipd..

.



Slika 5.14: Vzpostavitev povezave s strežnikom

Poglavje 6

Zaključek

Iz leta v leto se ogroženost informacijskih sistemov povečuje in tega se tudi vse bolj zavedamo. Za to, da bi zagotovili varnost, so različni protivirusni programi, požarni zidovi, IDS- in IPS-sistemi premalo. Tudi delo varnostnih inženirjev je na takšen način oteženo, saj morajo za vsak produkt posebej preko njegove nadzorne plošče pregledovati in upravljati incidente. Glavni razlog za namestitev sistema SIEM je zagotovo možnost upravljanja z dnevniškimi datotekami na enem mestu, ne glede na vrsto izhodne naprave in format zapisa dnevniških datotek. Dejstvo je tudi, da vse grožnje ne prihajajo samo iz zunanjega sveta, ampak so prisotne tudi znotraj omrežja. Ravno zato nam SIEM omogoča spremljanje aktivnosti uporabnikov znotraj informacijskega sistema in sprotno alarmiranje ob anomalijah.

Vzpostavitev sistema SIEM je za večje organizacije zelo obširen projekt, ki zahteva obsežne priprave in načrtovanja. Poleg usposobljenega kadra je treba zagotoviti še denarna sredstva za nakup sistema SIEM, katerega cena za vzpostavitev delovanja je lahko precej visoka. Prav zato sem v diplomski nalogi izbral eno izmed odprtokodnih orodij, ki ponuja učinkovit pristop k sistemu SIEM. Večina odprtokodnih orodij, ki so danes na voljo, ne vsebuje vseh funkcionalnosti in zato niso primerna za večje informacijske sisteme. Predstavljeno je tudi že bilo, da sistem AlienVault OSSIM dobro pokriva funkcionalnosti sistema SIEM, za večje organizacije pa je na voljo še plačljiva oziroma profesionalna različica, ki je nekoliko bolj zmogljiva in nudi še tehnično podporo s strani AlienVaulta.

Skozi proces izdelave diplomske naloge sem se osredotočil na varnost informacijskih sistemov. Spoznal sem veliko varnostnih groženj, ki jim v današnjem času pretijo. Ugotovil sem, da večino teh groženj lahko zaznamo le z uporabo dodatne programske opreme oziroma sistemov za upravljanje z incidenti. Enega izmed sistemov, AlienVault OSSIM, sem tudi sam namestil na strežnik in vzpostavil okolje, ki ga je OSSIM nadziral. Naučil sem se tudi nastaviti računalnik tako, da bo pošiljal dnevniške datoteke sistemu OSSIM. Spoznal sem, kako se analizira prejete dogodke, jih ovrednoti, izdela poročila,

dodeli v nadaljnje pregledovanje itd. Če se postavim v vlogo uporabnika takšnega sistema, bi kot glavno stvar izpostavil preprostost uporabe. Ta se odraža skozi pregleden uporabniški vmesnik, ki ponuja širok pogled nad varnostnim stanjem informacijskega sistema, ter možnost upravljanja in nastavitev preko uporabniškega vmesnika. Sama namestitev sistema ne zahteva veliko predznanja, saj samodejen način izbere veliko privzetih vrednosti in uporabniku olajša proces namestitve. OSSIM bi priporočil uporabnikom ali organizacijam, ki potrebujejo širok nabor integriranih varnostnih zmogljivosti ali pa želijo komercialno podprt izdelek, ki temelji na odprti kodi.

Seznam slik

Literatura

[1] D. R. Miller, S. Harris, A. A. Harper, S. Vandyke, C. Blask, *Security Information and Event Management (SIEM) Implementation*, New York: McGraw-Hill, 2011, pogl. 1.

[2] (2012) Načini varovanja ter zdravljenja podatkov. Dostopno na: http://colos1.fri.uni-lj.si/eri/informatika/RACUNALNISKA_OMREZJA/NaciniVarovanjaZdravljenjaPodatkov.

[3] (2012) Varnostne grožnje. Dostopno na: http://www.cert.si/varnostne-groznje.

[4] (2012) Varnostne napake pri upravljanju IT. Dostopno na: http://www.microsoft.com/business/smb/sl-SI/varnost/Izogibanje-pogostih-napak-pri-IT.

[5] G. Vigna, E. Jonsson, C. Kruegel, *Recent Advances in Intrusion Detection*, Pittsburgh, RAID, 2003, str. 192-197.

[6] (2012) Računalniški virusi. Dostopno na: http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.

[7] (2012) Računalniški črvi. Dostopno na: http://www.lu-rogaska.si/si/444/Strokovni_predmeti.

[8] (2012) Pridobitev dostopa s pretvarjanjem. Dostopno na: http://66.14.166.45/sf_whitepapers/tcpip/IP%20Spoofing%20%20An%20Introduction.

[9] (2012) Napad z zavrnitvijo storitve. Dostopno na: http://www.us-cert.gov/ncas/tips/ST04-015.

[10] (2012) DDoS napadi. Dostopno na: http://link.springer.com/article/10.1007%2Fs11235-004-5581-0.

[11] T. Bratuša, *Hekerski vdori in zaščita, druga, razširjena izdaja*, Ljubljana, Pasadena, 2006, str. 165-167.

[12] (2012) Program Snort. Dostopno na: http://www.izascita.si/index.php?option=com_content&view=article&id=46.

[13] (2012) Program OpenVAS. Dostopno na: http://wiki.dsms.net/w/OpenVAS.

[14] (2012) Advanced attack detection using OSSIM. Dostopno na: http://risk.management6.com/Advanced-Attack-Detection-using-OSSIM---Alienvault-Labs-pdf-e21323.

[15] (2012) Magic quadrant for security information and event management. Dostopno na: http://www.gartner.com/technology/reprints.do?id=1-1ANUJF3&ct=120525&st=sb.