SVEUČILIŠTE U RIJECI
FILOZOFSKI FAKULTET
ODSJEK ZA POLITEHNIKU

SIGURNOST OS X SUSTAVA

DIPLOMSKI RAD

Ivan Stipetić

Rijeka, 2015.

SVEUČILIŠTE U RIJECI
FILOZOFSKI FAKULTET
ODSJEK ZA POLITEHNIKU

SIGURNOST OS X SUSTAVA

DIPLOMSKI RAD

Ivan Stipetić

Mentor diplomskog rada:
dr.sc. Božidar Kovačić

Rijeka, 2015.

I. AUTOR

Ime i prezime: Ivan Stipetić

Mjesto i datum rođenja: Ogulin, 19. veljače 1991.

Adresa: 47300 Ogulin, Kut 8

FILOZOFSKI FAKLUTET U RIJECI

ODSJEK ZA POLITEHNIKU

Datum završetka nastave: 13.06.2014.

Sadašnje zaposlenje: Nema

II. DIPLOMSKI RAD

Naslov: Sigurnost OS X sustava

Broj stranica: 68 , slika: 20 , tablica: - , priloga: 2 , bibliografskih izvora: 14 .

Ustanova u kojoj je rad izrađen: FILOZOFSKI FAKULTET U RIJECI

Postignut akademski naziv: Magistar edukacije politehnike i informatike

Voditelj rada: dr.sc. Božidar Kovačić

Obranjeno na Filozofskom fakultetu u Rijeci

Oznaka i redni broj rada: _____

III. OCJENA I OBRANA

Datum preuzimanja zadataka: 20.03.2015. .

Datum predaje rada: 19.06.2015. .

Datum sjednice Povjerenstva za ocjenu i obranu diplomskog rada na kojoj je rad prihvaćen: _____ .

Datum obrane rada: _____ .

Povjerenstvo za ocjenu i obranu diplomskog rada pred kojim je rad obranjen: dr.sc. Božidar Kovačić .

_____ .

_____

Datum promocije: _____ .

SVEUČILIŠTE U RIJECI
Filozofski fakultet
Odsjek za politehniku
Rijeka, Sveučilišna avenija 4
Povjerenstvo za završni diplomski ispit

U Rijeci, 20.03.2015.

ZADATAK DIPLOMSKOG RADA

Pristupnik: Ivan Stipetić

Zadatak: Sigurnost OS X sustava

Rješenjem zadatka potrebno je obuhvatiti slijedeće:

1. Uvod
2. Opis Mac OS X sustava
3. Osnove sigurnosti
4. Testiranje sigurnosti
5. Opis programa
6. Metodički dio
7. Zaključak

U diplomskom se radu obvezno treba pridržavati **Pravilnika o diplomskom radu i Uputa za izradu diplomskog rada sveučilišnog diplomskog studija.**

Zadatak uručen pristupniku: 20.03.2015

Rok predaje diplomskog rada:

Datum predaje diplomskog rada: 19.06.2015

Koordinator povjerenstva za diplomske ispite:

Zadatak zadao:

dr.sc. Božidar Kovačić

I Z J A V A

Izjavljujem da sam diplomski rad izradio samostalno, koristeći se vlastitim znanjem, literaturom i provedenim eksperimentima.

U radu mi je pomagao savjetima i uputama mentor završnog rada dr.sc. Božidar Kovačić te mu iskreno zahvaljujem. Također zahvaljujem povjerenstvu što je prihvatilo i odobrilo predloženu temu rada.

Osim mentoru i povjerenstvu, jedno veliko hvala moram reći svim djelatnicima Odsjeka za politehniku Filozofskog fakulteta u Rijeci koji su mi od moje prve godine studiranja pa sve do završetka prenijeli znanje koje se na neki način očitovalo i jako mi pomoglo u realizaciji ovog rada.

_____

(Potpis pristupnika)

SAŽETAK

U radu je analizirana sigurnost OS X operativnog sustava. Kroz povijesni razvoj OS X sustava, predstavljene su sigurnosne značajke koje su uvedene sa pojedinom verzijom. Dotaknuo sam se tranzicije iz Mac OS Classic-a, preko NeXSTEP-a do današnjeg OS X sustava. Arhitektura OS X-a objašnjena je na razumljiv i slikovit način. Kroz poglavlje osnove sigurnosti detaljno su objašnjeni važni sigurnosni mehanizmi sustava. U istom poglavlju pojašnjene su korisničke sigurnosne značajke koje omogućavaju sigurnost korisničkih podataka i jednostavnu kontrolu sigurnosti za krajnjeg korisnika.

Testiranje sigurnosti pojedinog sustava odvija se u fazama, te je pruženo objašnjenje pojedine faze. Pojašnjena je važnost pojedine faze, izvršene radnje i programski alati koji se koriste u pojedinoj fazi. Procjena ranjivosti sustava provedena je korištenjem alata Nessus na verziji 10.9 Mavericks, te je provedena u dva dijela. U prvom dijelu objašnjeno je i prikazano provođenje procjene ranjivosti, dok su u drugom dijelu analizirani rezultati i objašnjene sigurnosne preporuke za rješavanje pronađenih ranjivosti sustava. Testiranjem ranjivosti potvrđujemo mogućnost iskorištavanja pronađenih ranjivosti sustava. Za provođenje testiranja ranjivosti korišten je poznati alat Metasploit koji sadrži brojne funkcionalnosti za iskorištavanje pronađenih ranjivosti sustava.

U zadnjem poglavlju pružen je opis korištenih alata za testiranje sigurnosti Nessus i Metasploit. Opisan je njihov nastanak i razvoj, glavni dijelovi, način funkcioniranja i njihova uloga u današnjem svijetu računalne sigurnosti.

Ključne riječi: sigurnost sustava, testiranje sigurnosti, procjena ranjivosti, testiranje ranjivosti

ABSTRACT

This study analyzes the security of the OS X operating system. Through the historical development of OS X are presented security features that were introduced with each version. I touched the transition from Mac OS Classic, trough NeXSTEP to modern OS X systems. Architecture of OS X is explained in an understandable and picturesque way. Throughout the chapter the basics of security I detailed important security mechanisms of the system. In the same chapter are explained the user security features that provide security of user data and easy control of safety for the end user.

Testing the security of a particular system is achieved in stages, and there is an explanation of each phase. There is an explanation of the importance of each phase, completed actions and software tools used in each phase. Vulnerability assessment of system was carried out using a Nessus tool on OS X version Mavericks, and was conducted in two parts. The first part is explained and illustrated conduct of vulnerability assessments, while the second part analyzes the results and explains safety recommendations to address found systemic vulnerabilities. Vulnerability testing has purpose to confirm the possibility of exploiting vulnerabilities found with vulnerability assessment. To carry out the vulnerability testing we used famous Metasploit tool that contains a number of functionalities to exploit found vulnerabilities in system.

In the last chapter we provide a description of the tools Nessus and Metasploit, which we used to test the security of the OS X system. It describes their creation and development, the main components, how they work and theirs role in today's world of computer security.

Keywords: security of systems, security testing, vulnerability assessment, vulnerability testing

SADRŽAJ

1 UVOD

U današnjem svijetu mrežno povezanog i oblačnog računalstva, sigurnost je vrlo bitan aspekt odgovarajućeg razvoja softvera. Potrebno je shvatiti da sigurnost nije samo još jedna točka u razvojnom procesu. Potrebno je svjesno razvijati siguran softver od početka razvojnog procesa, od početnog dizajna preko implementacije softvera, njegovog testiranja i objave.

Mac OS X zbog svoje UNIX arhitekture je relativno siguran i pouzdan operativni sustav odmah nakon instalacije. UNIX je prema prvotnoj namjeni dizajniran za zahtjevnu serversku arhitekturu, web servere i sličnu uporabu. Zbog ovog razloga sigurnost je bitan dio UNIX-a.

U svijetu operativnih sustava postoji balans između ugodnijeg korisničkog iskustva i sigurnosti sustava. Ovo je vidljivo kod operativnih sustava koji zahtijevaju odobravanje svake promjene uz dodatna upozorenja, što može biti frustrirajuće. Zbog ovog razloga prilikom Appleovog redizajna OS-a, uz razvoj sigurnosnih značajki, potrebno je bilo uzeti u obzir korisničko iskustvo. U velikoj većini slučajeva odlučeno je u korist ugodnijeg korisničkog iskustva, zbog kojeg danas OS X pruža jedno od najboljeg korisničkog iskustva. Ovo ne znači da OS X nije siguran jer korisnik može implementirati naprednije sigurnosne mjere prema potrebi.

Napomenimo da je Mac OS napredovao strahovito od svojeg skromnog početka. Od operativnog sustava za kultne poklonike, polako je stjecao sve veću popularnost među korisnicima računala, što je vidljivo u trenutno velikoj popularnosti Macbook Pro i Macbook Air prijenosnika. Osim što polako preuzima dio tržišta osobnih računala, Mac OS sa svojom mobilnom inačicom – iOS – koja prema nekim procjenama ima najviše tržišnog utjecaja, nastavlja borbu za tržišni udio sa Android mobilnim sustavom, inačicom Linux sustava.

2 OPIS MAC OS X SUSTAVA

Mac OS X od nedavno samo OS X je serija operativnih sustava sa grafičkim korisničkim sučeljem temeljena na UNIX-u i razvijena od strane tvrtke Apple. Slovo X u nazivu predstavlja rimski broj deset, te stavlja naglasak na povezanosti ovog operativnog sustava sa UNIX sustavom na kojem se temelji. Nakon Windows OS-a najpopularniji operativni sustav prošao je kroz razne promjene od svojih skromnih početaka. U ovom poglavlju kratko se dotičem povijesnog razvoja, arhitekture operativnog sustava, te kratak opis pojedine verzije OS X uz naglasak na Lion verziju sustava.

2.1 POVIJESNI RAZVOJ

Kratak opis povijesnog razvoja operativnih sustava za Macintosh računala. Od samih početaka uz Mac OS Classic preko NeXTSTEP-a, do OS X i verzija Lion i Mountain Lion.

2.1.1 Mac OS Classic

Naziv Mac OS Classic odnosi se na verzije Mac OS-a prije pojavljivanja OS X sustava. Operativni sustav nije bio za pohvalu, jedina posebnost ovog operativnog sustava je njegovo grafičko korisničko sučelje ili GUI (eng. Graphical User Interface). Upravljanje memorijom je bilo loše izvedeno, a multitasking je bio kooperativan, što se po današnjim standardima smatra primitivnim. Kooperativni multitasking se primjenjuje tako da svaki proces dobrovoljno daje svoje CPU vrijeme ostalim procesima kada ga zatrebaju, ovo odlično funkcionira prilikom normalnog ponašanja procesa. Ako samo jedan od procesa odbije suradnju, dolazi do zastoja sustava. Iako primitivan ovaj sustav unio je temelje nekih značajki modernog OS X sustava, kao što je Finder GUI, te podrška za sistemske pozive (forks) u prvoj generaciji HFS datotečnog sustava. Ove značajke su bitne za rad modernog OS X sustava.

2.1.2 NeXTSTEP

NeXTSTEP je naziv za objektno orijentirani operativni sustav s podrškom za multitasking, razvijen od strane tvrtke NeXT Computer za njihova računala poput NeXTcube radne stanice. NeXTSTEP je donio velike promjene:

- Bazira se na Mach mikrokernelu, razvijenom od strane Carnegie Mellon Sveučilišta (CMU). Novost je bila u samom konceptu mikrokernela koji se rijetko implementira i danas.
- Programski jezik korišten pri razvoju je Objective-C, koji je u odnosu na C++ više objektno orijentiran jezik.

- Upravljački programi su mogli sadržavati ostale upravljačke programe, te na taj način proširujući njihovu funkcionalnost. Razvojno okružje za upravljačke programe bilo je objektno orijentirano pod nazivom DriverKit.

- Aplikacije i programske biblioteke su bile distribuirane u nezavisnim paketima. Paketi su imali unaprijed određen datotečni sustav, koji je bio korišten za pakiranje softvera zajedno sa povezanim datotekama, te je instaliranje i brisanje aplikacija bilo jednostavno kao micanje obične mape.

- PostScript je bio dosta korišten, uključujući funkciju display postscript koja je omogućavala renderiranje slika kao postscript. Ovo je omogućavalo ispis u formatu 1:1, za razliku od ostalih operativnih sustava koji su morali konvertirati u format pogodan za ispis.

NeXTSTEP sustav unatoč mogućnostima koje je donio nije stekao veliku popularnost, te se danas ne koristi. Tvrtka Apple je 1997 godine kupila tvrtku NeXT Computer, te je zajedno uz kupnju sustava NeXTSTEP ponovno zaposlila vizionara Steve Jobsa. Nasljedstvo NeXTSTEP operativnog sustava nalazi se u današnjem OS X.

2.1.3 Dolazak OS X-a

Kao rezultat kupnje NeXT-a, Apple je dobio pristup novim tehnologijama poput Mach mikrokernela, programskog jezika Objective-C te ostalim dijelovima NeXTSTEP arhitekture. Nakon preuzimanja prestaje razvoj NeXTSTEP sustava, ali su glavne tehnologije korištene u razvoju OS X. Zapravo OS X možemo nazvati spojem Mac OS Classica i NeXTSTEP-a, većim dijelom potonjeg. Tranzicija Mac OS bila je postupna, uz razvojnu inačicu nazvanu Rhapsody koja nije javno objavljena. Međutim ta razvojna inačica je kroz konstantan razvoj postala prva verzija Max OS X, a njezin kernel je postao osnova za današnji Darwin.

Po implementaciji i dizajnu Mac OS X je sličniji NeXSTEP sustavu nego Appleovoj vlastitoj OS 9 verziji. Glavne značajke OS X poput Cocoa, Mach, IOKit, XCode i ostalih, proizlaze iz NeXTSTEP sustava. Spoj ova dva operativna sustava, jednog sa odličnim sučeljem i lošim dizajnom, a drugog sa odličnim dizajnom a lošim korisničkim sučeljem, rezultirao je novim operativnim sustavom sa popularnošću većom nego zajednička popularnost njegovih prethodnika.

2.1.4 Darwin

Postoje određene razlike između termina OS X i Darwin, te veze između ova dva termina. Naziv OS X predstavlja ime za cijeli operativni sustav, dok je Darwin samo jedna od mnogih komponenti od kojih se sastoji.

Darwin je jezgra operativnog sustava slična UNIX-u, koja se sastoji od kernela, XNU-a (akronim značenja „ X nije UNIX “) te runtime-a. Darwin je otvorena koda, dok su ostali dijelovi OS X-a intelektualno vlasništvo tvrtke Apple. Postoji povezanost između verzije OS X i verzije Darwina. Povezanost između verzija može se opisati funkcijom:

```
If ( OSX.version = = 10.x.y )
Darwin.version = ( 4+x ) .y
```

Tako verzija Mountain Lion, brojčano 10.8.0, sadržava Darwin 12.0. Verzija Snow Leopard, brojčano 10.6.8, sadržava Darwin 10.8. Na početku zbunjujuće, ali je konzistentno. [1]

2.2 VERZIJE OS X SUSTAVA

Od prvog pojavljivanja, OS X je prošao kroz nekoliko verzija sustava. Od novoga sustava, za neke nedovršenog, prošao je transformaciju u platformu bogatu mogućnostima u verziji Lion i Mountain Lion. U ovom poglavlju navodi se kratak opis pojedine verzije, njezine specifičnosti, posebno one koje se odnose na promjene u arhitekturi i kernelu sustava.

2.2.1 Verzija 10.0 – Cheetah

Ova verzija je poznata pod nazivom Cheetah ili u prijevodu Gepard, te je prva javno objavljena verzija OS X sustava. Godinu dana nakon beta verzije pod nazivom Kodiak, objavljena je u ožujku 2001 godine. Sa integriranim funkcionalnostima iz NeXTSTEP sustava i slojevite arhitekture, predstavlja veliki odmak od starih verzija Mac OS sustava. Osim možda sučelja Carbon predstavlja odmak od verzije Mac OS 9, te s njom ne dijeli nikakvu sličnost. Predstavljene su podverzije od 10.0 do 10.0.4 uz manje modifikacije.

2.2.2 Verzija 10.1 – Puma

Iako je verzija 10.0 donijela preventivni multitasking i zaštitu memorije, bila je nedovršena, nestabilna te dosta spora pri radu. Nekih 6 mjeseci kasnije izlazi verzija Mac OS X 10.1 pod nazivom Puma, koja je treba biti odgovor na slabe performanse i probleme sa stabilnosti koje je imala verzija Cheetah. Uz navedene promjene trebala je donijeti i promjene u korisničkim funkcionalnostima sustava. Ubrzo nakon izlaska verzije Puma Apple javno iznosi vijest o napuštanju razvoja Mac OS 9 sustava, te svoje resurse usmjerava prema OS X-u kao svome

novom operativnom sustavu. Puma je imala podverzije od 10.1 do 10.1.5, dok je XNU kernel bio u verziji 201.

2.2.3 Verzija 10.2 – Jaguar

Godinu dana nakon Pume izlazi verzija Jaguar koja donosi zreliji operativni sustav uz poboljšanja korisničkog iskustva, te uvođenjem Quartz Extreme kostura za bolju grafiku. Nova funkcionalnost je bila Apple Bonjour tehnologija i UPNP (Universal Plug and Play) protokol koji je omogućavao lakši pronalazak Apple uređaja na lokalnoj mreži. Darwin je nadograđen na verziju 6.0 kasnije do 6.8, a izašlo je devet podverzija Jaguar verzije, od 10.2 do 10.2.8, dok je XNU kernel bio u verziji 344.

2.2.4 Verzija 10.3 – Panther

Apple verziju Pantera objavljuje 2003 godine, uz dodatna poboljšanja korisničkog iskustva. Razvijen je vlastiti web preglednik pod nazivom Safari, izbacivši Microsoftov Internet Explorer. Uvedena je sigurnosna funkcionalnost FileVault za transparentnu enkripciju diskovnog sustava. Izdano je deset podverzija od 10.3 do 10.3.9, Darwin je imao verzije 7.0 do 7.9, a XNU kernel je bio u verziji 517.

2.2.5 Verzija 10.4 – Tiger

Tiger verzija je najavljena u svibnju 2004 godine, ali je tek nakon godinu dana razvoja službeno izdana. Razlog duljeg razvoja su bile važne promjene arhitekture sustava, primarno podrška za Intelove x86 procesore. Do verzije 10.4.4 Mac OS zahtijevao je PowerPC arhitekturu. Došlo je do promjena u dizajnu sučelja, predstavljen je Spotlight koji omogućava lakše pretraživanje sustava, te je uvedena mogućnost korištenja stvarčica (Widgets) unutar kontrolne ploče (Dashboard). U verziji 10.4.4 uveden je koncept univerzalnih binarnih grupa (Universal binaries) koji je funkcionirao na PowerPC i x86 arhitekturi.

Bitne funkcionalnosti za razvojne programere se odnose na četiri kostura (framework): CoreData, Image, Video i Audio. Core Data omogućava manipulaciju podacima (save/undo/redo), a Core Image i Core Video omogućavaju ubrzanje grafike boljim iskorištenjem grafičkog procesora GPU-a. Core Audio je omogućio ugradnju audio funkcionalnosti direktno u OS, te mogućnost prepoznavanja govora uz funkcionalnost Voice Over. Tiger je bio u uporabi preko dvije godine uz dvanaest podverzija od 10.4.0 / Darwin 8.0 do 10.4.11 / Darwin 8.11, dok je XNU kernel bio u verziji 792.

2.2.6 Verzija 10.5 – Leopard

Verzija Leopard najavljena je u lipnju 2006 godine, ali je izdana tek u listopadu 2007 godine s mnogo novih funkcionalnosti. Neke od važnijih uključuju:

- Core Animation za lakše procesuiranje animacija
- Nove verzija programskog jezika Objective-C 2.0
- OpenGL 2.1 – nova verzija aplikacijskog programskog sučelja ili API-a za grafiku
- Poboljšane skripte i podrška za nove programske jezike, uključujući Python i Ruby
- Podrška za alat Dtrace i njegovo sučelje – omogućava dijagnostiku i praćenje problema s kernelom ili aplikacijama u realnom vremenu
- Leopard verzija je potpuno usklađena s UNIX/POSIX standardom
- Uvedena podrška za FSEvents

Izdano je devet verzija od 10.5 do 10.5.8, Darwin u verzijama 9.0 do 9.8, a XNU kernel je napredovao do verzije 1228. [1]

2.2.7 Verzija 10.6 – Snow Leopard

Verzija Snježni Leopard izlazi u kolovozu 2009 godine, te donosi nekoliko promjena, uglavnom na samoj arhitekturi sustava. S perspektive korisnika promjene su minimalne, prelazak na 64-bitne aplikacije, ali s perspektive razvojnog programera neke od bitnijih promjena uključuju:

- Potpuna 64-bitna funkcionalnost
- Kompresija sistemskih datoteka – većina datoteka, a posebno sistemske se sažimaju radi uštede diskovnog prostora
- OpenCL – omogućava preusmjeravanje dijela radnog opterećenja na grafički procesor ili GPU, iskorištavajući tako procesorsku moć novih grafičkih kartice za ostale zadatke. Tvrtka Apple je prva razvila ovu funkcionalnost, dok je kasniji razvoj predan Khronos grupi, konzorciju tvrtki poput AMD-a, Intela, Nvidie i mnogih drugih tehnoloških tvrtki. Konzorcij isto razvija OpenGL za grafiku i OpenSL za zvuk.

Ova verzija Mac OS X završila je proces migracije sa PowerPC arhitekture na x86/x64 arhitekturu koja je započela s verzijom 10.4.4. Ovo je omogućilo uštedu diskovnog prostora, zbog smanjenja broja binarnih datoteka.

Snow Leopard je imao verzije od 10.6 do 10.6.8, Darwin u verziji 10.8.0, a XNU kernel u verziji 1504.

2.2.8 Verzija 10.7 – Lion

Većina promjena koje donosi verzija Lion odnose se na korisničko iskustvo. Nekolicina njih razvijena je na temelju funkcionalnosti koje se nalaze u iOS-u, mobilnom sustavu za iPhone i iPad uređaje. Bitne funkcionalnosti koje verzija Lion donosi su:

- iCloud – Appleovo rješenje za lak i siguran smještaj podataka u oblaku, odnosno njihovim serverima. Ovo je rješenje je dobro integrirano u OS, te tako aplikacijama omogućuje lako spremanje dokumenata i datoteka u oblak.
- Poboljšanja ugrađenih aplikacija – poboljšanja se odnose na aplikacije Mail, Finder i Preview, dok su zanimljive nove aplikacije FaceTime i LaunchPad
- Bolja sigurnost – u skladu s poboljšanjima u iOS sustavu, uvedena su sigurnosna poboljšanja poput sandboxinga aplikacija i odjeljivanje povlastica
- Core Storage – sloj koji se smješta između particije na disku i datotečnog sustava, omogućujući nove funkcionalnosti pri stvaranju particije. Korisna funkcionalnost je proširenje datotečnog sustava na više particija.
- Sustavne funkcionalnosti – od poboljšanja grafičkog sučelja, auto ispravka teksta kao u iOS-u, upravljanja govorom do promjene dizajna klizača
- FileVault2 – omogućava enkripciju datotečnoga sustava, sve do korijenskog direktorija, omogućavajući tako enkripciju cijelog diska (Full Disk Encryption–FDE) Ovo se nadograđuje na enkripcijske mogućnosti Core Storage funkcionalnosti. Enkripcija je AES–128 u XTS modu, što je posebno optimizirano za enkripciju tvrdog diska.
- Air Drop – Omogućava brzo dijeljenje datoteka između povezanih računala putem WiFi mreže, proširujući dodatno već postojeće mogućnosti dijeljenja datoteka koje OS X sadržava.
- 64 – bitni sustav – Na najnovijim Mac modelima omogućen automatski. Iako je Snow Leopard imao 64 bitni kernel, sa izuzetkom Mac Pro modela, korišten je 32 bitni kernel.

Ova inačica OS X sustava brzo je zamijenjena novom verzijom, te su izdane podverzije od 10.7 do 10.7.5 koje su ispravljale pojedine pogreške i sigurnosne propuste.

2.2.9 Verzija 10.8 –Mountain Lion

Vrlo brzo nakon verzije Lion u srpnju 2012 izlazi Mountain Lion ili Puma verzija, preuzimanje je moguće jedino kroz Mac App Store kao dio strategije da nova verzija OS X-a izlazi online i godišnje. Mountain Lion nastavlja trend koji je započela Lion verzija, uvođenje funkcionalnosti s iOS sustava, te tako smanjujući razliku između OS X sustava i iOS-a. Zanimljiva je reklamna rečenica za ovu verziju: „ Inspiriran iPadom, redizajniran za Mac“ Većina promjena odnosi se na korisničko iskustvo, uz određene promjene na kernelu:

- Notification Center – Ova funkcionalnost omogućava prikaz notifikacija od strane raznih aplikacija. Notifikacija ostaje prikazana dok korisnik ne obavi zadanu akciju. Korisnik može birati koje aplikacije mogu slati notifikacije, i na koji način se prikazuju. Notifikacije su podijeljene na Banners koji su prikazani kratko u gornjem kutu ekrana te nestaju udesno, na Alerts koje nestaju s ekrana tek nakon obavljanja zadane akcije, te Badges koje su prikazane kao crvene obavijesti na ikoni aplikacije.

- Notes – Notes ili Bilješke aplikacija prenesena je s iOS-a te podržava unos bilješki direktno s radne površine. Bilješke mogu biti organizirane u direktorije ili prikazane na radnoj površini. Stvorene bilješke sinkroniziraju je na sve uređaje povezane s korisničkim iCloud računom.

- Messages – Aplikacija za slanje poruka koja zamjenjuje dotadašnji iChat. Omogućeno je slanje tekstualnih poruka, audio i video razgovora kroz FaceTime. Podržava iMessage aplikaciju dostupnu na iOS sustavu, te mogućnost povezivanja s Yahoo Messengerom i Google Talkom.

- Game Center – Aplikacija je prenesena s iOS sustava i omogućava mrežno igranje s prijateljima , praćenje i usporedbu postignutih rezultata. Bodovi se dodjeljuju kroz ugrađen sustav praćenja, koji dodjeljuje bodove na temelju ostvarenih zadataka u igrama. Omogućeno je stvaranje profila koji su povezani a Apple ID računom.

- Poboljšanja ugrađenih aplikacija – Aplikacije koje dolaze uz OS X su nadograđene s novim funkcionalnostima. Mail dobiva VIP funkcionalnost za spremanje čestih kontakata, Preview ima mogućnost ispunjavanja PDF dokumenata. Reminders postaje nova aplikacija za organiziranje zadataka uz sinkronizaciju s iOS uređajima. Kod Safarija adresna traka omogućuje pretraživanje, a Reader ikona omogućava čitanje samo teksta bez slika i reklama.

Osim ovih nadogradnji uvedene su nove funkcionalnosti za kineske korisnike, dodana je direktna podrška za Facebook i Twitter, uvedena je Gatekeeper aplikacija za borbu protiv zloćudnih aplikacija. Funkcionalnost Air Play Mirroring omogućava direktan prijenos zaslona na Apple TV. Nadogradnje za aplikacija se automatski instaliraju putem Mac App Trgovine. Korisničko sučelje iCloud-a integrirano je u operativni sustav, omogućeno je korištenje njegovog API-a i u ostalim aplikacijama. [2]

Izdane su nadogradnje kroz verzije 10.8.1 do 10.8.5, a Darwin je bio u verzijama 12.0 do 12.5.

2.2.10 Verzija 10.9 – Mavericks

Deseta verzija OS X sustava izdana je u listopadu 2013, kao besplatna nadogradnja u Mac App Storeu. Naglasak je na produljenju trajanja baterije kod prijenosnih računala, daljnja integracija iClouda, uz nove iOS aplikacije na OS X platformi. Dolazi do promjenu u nazivu OS X-a i napuštanja imenovanja prema velikim mačkama. Nove verzije dobivaju imena prema mjestima u državi California. Neke od novih i poboljšanih funkcionalnosti koje ova verzija donosi:

- Nove aplikacije – aplikacija za čitanje knjiga iBooks, Maps aplikacija za zemljopisne karte
- Poboljšanja ugrađenih aplikacija – Finder dobiva kartice i podršku za cijeli zaslon, nadogradnje Mission Controla, Calendara, Notification Centra. Poboljšana privatnost kod Safari aplikacije, anonimno pretraživanje.
- Funkcionalnost Timer coalescing – tehnika koja poboljšava energetsku učinkovitost smanjenjem iskorištenja procesora do 72%.
- Compressed Memory – sistem sažimanja RAM memorije koji automatski sažima podatke od nekorištenih aplikacija, u trenucima kada dolazi do maksimalnog iskorištenja RAM memorije.

Izdane su nadogradnje kroz verzije 10.9.1 do 10.9.5, dok je Darwin izdan u verzijama 13.0 do 13.4. [3]

2.2.11 Verzija 10.10 – Yosemite

Najnovija verzija OS X sustava izdana je u listopadu 2014, i dobila je naziv prema nacionalnom parku smještenom u državi California. Došlo je do velike promjene izgleda sučelja, uvodeći ravni dizajn. Ove promjena prate grafički dizajn iOS sustava, te su pojedine ikone dobile isti dizajn kao kod iOS-a.

Nastavlja se daljnja integracija Appleovih proizvoda poput iClouda i iOS sustava. Funkcionalnost Handoff omogućuje integraciju s iOS 8 uređajima putem Bluetooth i Wi-Fi tehnologije. Ovo omogućava primanje poziva, tekstualnih poruka, stvaranje hotspota i prebacivanje trenutnog rada s mobilnih aplikacija na njihove desktop inačice. Aplikacija Photos zamijenila je iPhoto i Aperture, te koristi iCloud za sinkronizaciju korisničkih fotografija.

Spotlight dobiva veću ulogu i sada omogućuje pretraživanje internetskih servisa, uključujući Bing pretraživač , Mape i Wikipediju. Safari aplikacija ima novi opcije privatnosti, lakše brisanje povijesti pretraživanja, integracija DuckDuckGo tražilice za privatnije pretraživanje interneta. JavaScript for Automation (JXA) je nova sistemska podrška za JavaScript, razvijena na temelju JavaScriptCore tehnologije i Open Scripting Arhitekture. Ovime je dobivena je mogućnost razvoja Cocoa aplikacija koristeći JavaScript. [4]

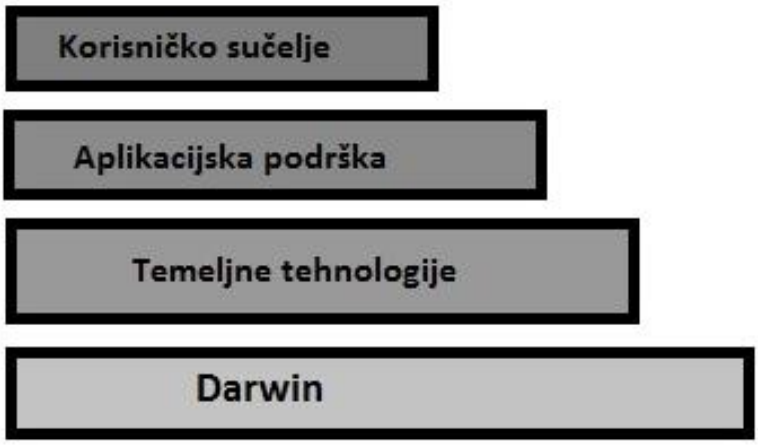
Do sada su izdane nadogradnje kroz verzije 10.10.1 do 10.10.3, dok je Darwin izdan u verzijama 14.0 do 14.3.

2.3 ARHITEKTURA SUSTAVA

U odnosu na prethodnika OS 9, OS X je potpuno redizajniran, s ciljem da postane jedan od najinovativnijih operativnih sustava. Posebno s novim funkcionalnostima koje donosi u korisničkom sučelju (GUI) i aplikacijskom programskom sučelju (API), koje brzo bivaju prenesene na Windows i Linux platformu. Službena dokumentacija predstavlja elegantno i jednostavno objašnjenje arhitekture kroz pojedine slojeve:

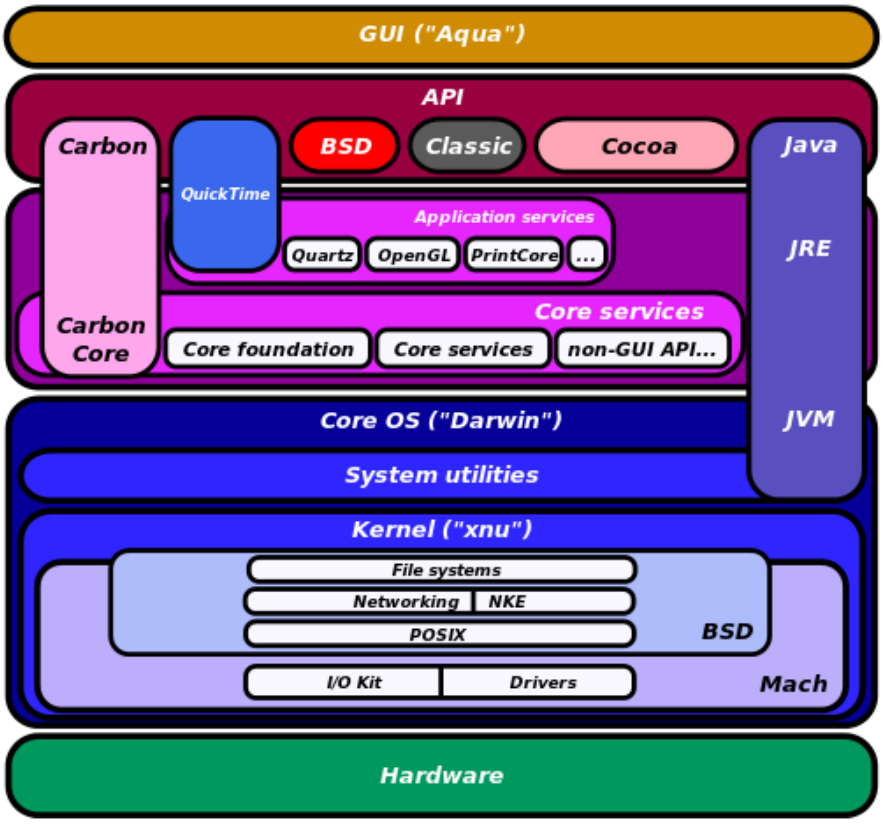
- Sloj korisničkog sučelja: uključuje komponente Aqua, DashBoard, Spotlight i funkcionalnosti pristupačnosti.
- Sloj aplikacijske podrške: uključuje komponente Cocoa, Carbon i Java.
- Sloj temeljnih tehnologija: naziva se još sloj medija i grafike. Sadrži tehnologije Open GL i QuickTime.
- Darwin: jezgra operacijskog sustava — sadrži kernel i UNIX ljusku.

Jezgra sustava Darwin je otvorenog koda i služi kao osnova sustava, dok su gornji slojevi zaštićene tehnologije u vlasništvu Applea.



Slika 2.1 Dijagram arhitekture sustava [1]

Slika 2.1 prikazuje jednostavan pregled arhitekture sustava i prethodno objašnjene slojeve. Svaki pojedini sloj može se prikazati razdvojen na pojedine komponente koje ga sačinjavaju, kao što je vidljivu na sljedećem prikazu arhitekture OS X.



Slika 2.2 Detaljan prikaz arhitekture OS X sustava [5]

3 OSNOVE SIGURNOSTI

Apple već dulje reklamira OS X kao sustav gdje su virusi i maliciozan softver rijetka pojava, posebno u seriji zanimljivih reklama „ Mac VS PC“. Ali razlog takvoj situaciji je u prevlasti Windows sustava na stolnim i prijenosnim računalima. Jednostavno objašnjeno, sa stajališta programera malicioznog softvera, želimo li svoje vrijeme i trud uložiti u maliciozan softver koji može napasti 90% računala u svijetu ili samo 5%. Ovo je jednostavan razlog zašto OS X i Linux sustav nemaju velikih problema s malicioznim softverom. S rastom udjela OS X sustava ovo se polako mijenja, te se u novije vrijeme pojavljuju opasniji virusi. Pojedini stručnjaci na polju sigurnosti kritiziraju Apple, zbog loših sigurnosnih mehanizama koji su neefektivni i zastarjeli.

U stvarnosti sigurnost OS X i iOS sustava je dosta naprednija od konkurenata. Kontrola korisničkih računa (UAC) koju nalazimo u Windows sustavu prisutna je dosta dugo u OS X sustavu. Većina navedenih virusa su zapravo Trojanci, maliciozan softver koji zahtijeva suradnju korisnika računala. Određene promjene po pitanju sigurnosti su uvedene s Leopard verzijom, uz uvođenje novih i unapređenje postojećih sigurnosnih značajki sa svakom novom verzijom.

OS X je izgrađen na komponentama koje su otvorenog koda, te su prošle ispitivanje od strane Apple-a, raznih razvojnih programera i sigurnosnih stručnjaka. Apple aktivno sudjeluje u zajednici podrške otvorenom kodu, kroz dijeljenje informacija o razvojnom procesu mnogih komponenti OS X sustava. Ovaj napor donio je ugradnju preporučenih poboljšanja i pruža transparentnost, koja je potrebna za potvrdu sigurnosti mnogih kritičnih komponenti OS X sustava.

3.1 SIGURNOSNI MEHANIZMI SUSTAVA

Apple ulaže napore da OS X pruži sigurnost sustava, softvera i podataka bez potrebe za naprednim podešavanjima ili posebno prilagođenim softverskim alatima. OS X je dizajniran da pruži obranu od raznih sigurnosnih prijetnji kroz obrambene sisteme i pristupe, koji imaju zadaću da identificiraju potencijalne prijetnje i proaktivno štite sustav od tih istih prijetnji. Osim navedenog, implementirane su mnoge sigurnosne funkcionalnosti za zaštitu povjerljivosti korisničkih i poslovnih podataka.

3.1.1 Potpisivanje programskog koda

Prije nego što se može potvrditi sigurnost određenog softvera, potrebno je potvrditi sigurnost izvora. Softver lako može biti zloćudan ako je preuzet s nepoznate stranice na Internetu. Rizik se

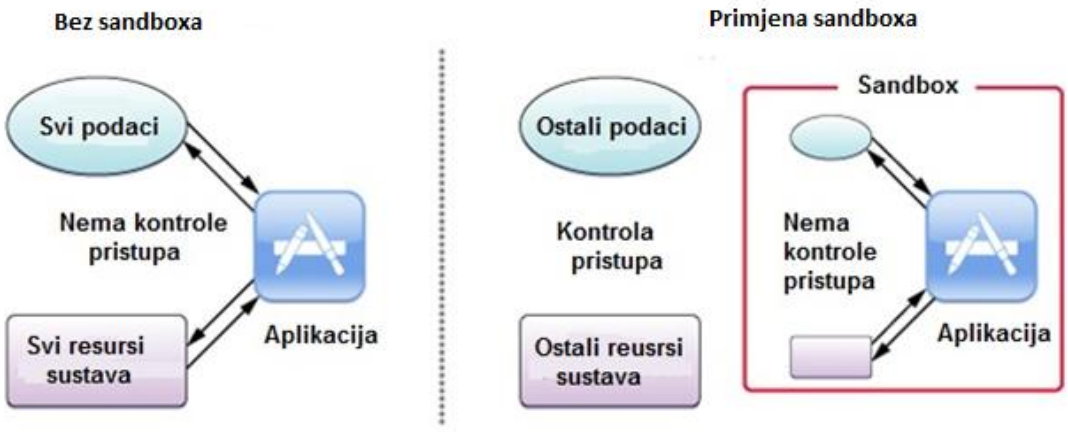
lako može umanjiti tako da potvrdimo sigurnost izvora, dodatno kroz potvrdu da softver nije izmijenjen prilikom preuzimanja.

Potpisivanje programskog koda omogućava prije navedeno koristeći se X.509v3 certifikatom, koji SSL koristi pri određivanju identiteta web stranice (uspoređujući njihov javni ključ s privatnim ključem korisnika). Apple potiče razvojne programere na potpisivanje programskog koda softvera za lakše utvrđivanje njihove identiteta. Jedna od bitnih stvari koda potpisivanja programskog koda je ta, da javni ključ mora biti poznat odobravatelju koda. Apple ugrađuje certifikate u OS X i iOS sustave, slično kao i Microsoft kod Windows sustava, dostupne samo root korisniku.

Iako potpisane aplikacije mogu sadržavati zlćudan kod, one krše uvjete korištenja te bi ubrzo bile maknute iz Mac App Storea, uz zabranu za razvojnog programera. Pošto prilikom registracije navode osobne podatke, ta osoba ili tvrtka može dobiti i tužbu od strane Apple. Ovo je jedan od razloga zašto nalazimo tako mali broj zlćudnih aplikacija u Mac App Storeu.

3.1.2 Sandboxing

Na početku smatrana zanimljivom funkcionalnosti, kompartmentalizacija ili sandboxing postaje integralan dio OS X i iOS sustava. Ideja je jednostavna, ali je ona važan princip za sigurnost aplikacija. Neprovjerene aplikacije moraju biti pokrenute u posebnom odjeljku, poput karantene u kojoj su sve operacije podložne restrikcijama. Prijašnji naziv za funkcionalnost je seatbelt, kasnije preimenovana u sandbox, u Lion verziji postaje jedna od glavnih prednosti OS X sustava.



Slika 3.1 Prikaz sandbox funkcionalnosti [6]

Strategija sandbox funkcionalnosti:

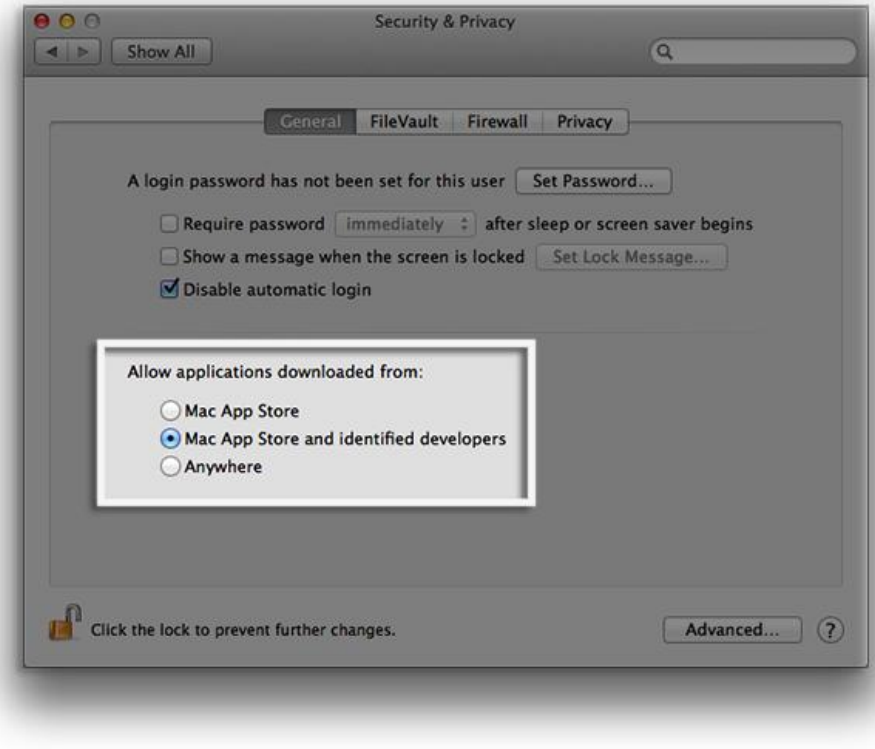
- Razvojnom programeru omogućava opis interakcije koju aplikacija ima sa sustavom. Sustav zatim dodjeljuje aplikaciji prava da izvrši svoj zadatak i ništa više.

- Korisniku daje pravo da omogući dodatne pristupe alokacijama kroz poznate interakcije i korisničko sučelje.

Nakon biranja aplikacije od strane korisnika, prije pokretanja, OS X provjerava da li je aplikacija smještena u sandbox. Ako sandbox kontejner postoji u direktoriju *Library/Containers* aplikacija se odmah pokreće, dok u slučaju da ne postoji sustav kreira sandbox kontejner i obavlja migraciju datoteka navedenih u posebnoj listi pripremljenoj za ovu situaciju. Ova migracija je jednosmjeran proces, te nema vraćanja datoteka koje ulaze u sandbox. [6]

Prednost ovako čvrstog sanboxa je u tome da korisnik može pokrenuti nesigurnu aplikaciju u sanboxu, bez straha da će zloćudni softver učiniti neku štetu podacima ili samom sustavu.

Sandbox mehanizam jedan je od boljih sigurnosnih mehanizama u operativnim sustavima, ali to ne podrazumijeva savršenstvo. Efikasnost sistema „crnih listi“ ovisi o tome koliko su liste restriktivne. Istraživanje iz 2011 provedeno od Core Labs tvrtke, pokazalo je da jednostavna zloćudna aplikacija može pokrenute AppleScript, te na taj način pristupiti mreži kroz proces izvan kontrole sanboxa. Ovo je jedan od razloga zašto je sandbox izmijenjen u Lion verziji i preimenovan u funkcionalnost GateKeeper. GateKeeper je kombinacija postojećih mehanizama, HFS+ karantene, uz korištenje „bijele liste“ koja ima za cilj umanjiti važnost „crne liste“ kod sandbox mehanizma. Aplikacije preuzete s Interneta imati će oznaku karantene, koja aktivira obavijest korisniku. Sa GateKeeper mehanizmom potpis programskog koda aplikacije prolazi kroz provjeru identiteta izdavatelja aplikacije, za utvrđivanje mogućnosti da sadrži zloćudni kod. GateKeeper korisniku pruža veću kontrolu kod instaliranja novih aplikacija. Korisnik može odabrati najsigurniju opciju koja dopušta samo aplikacije iz Mac App Storea, drugu opciju koja dopušta i poznate razvojne programere, te zadnju opciju koja omogućava instaliranje svih aplikacija. Korisnik može mijenjati svoj odabir u postavkama sustava, pod dijelom Sigurnost i Privatnost.



Slika 3.2 Odabir postavki GateKeeper mehanizma [7]

3.1.3 Runtime Protection

OS X primjenjuje brojne hardverske i softverske tehnike za zaštitu operacijskog sustava i aplikacija. Ugrađena direktno u procesor, XD („execute disable“) funkcionalnost pruža zaštitni zid između memorije korištene za podatke i memorije korištene za izvršne instrukcije. Ovo pruža zaštitu od zlođudnih aplikacija koje pokušavaju prevariti Mac da podatke smatra istovjetnima programu, te na taj način kompromitirajući sustav. Adress Space Layout Randomization (ASLR) mijenja lokacije u memoriji gdje se spremaju različiti dijelovi aplikacije. Na ovaj način napadaču je teško napraviti štetu koja se događa pronalaskom i promjenom dijelova aplikacije, u namjeri da ona učini nešto van svoje prvotne namjene. OS X donosi ASLR u memoriju korištenu od strane kernela u jezgri operacijskoj sustava, tako da navedena obrana djeluje na svim razinama OS-a. Sve navedene ugrađene tehnologije pridonose slojevitoj obrani protiv zlođudnih aplikacija. [8]

3.1.4 Mandatory Acess Controls

OS X koristi mehanizam za kontrolu pristupa pod nazivom „mandatory access controls“. Iako mehanizam nije vidljiv krajnjem korisniku, on je ugrađen u operativni sustav i to su pravila koja ne mogu biti nadvladana. Ova pravila postavljaju sigurnosne restrikcije kreirane od strane

razvojnog programera. Ovakav pristup je drugačiji u odnosu na diskretnu kontrolu pristupa koja dopušta korisniku promjenu sigurnosnih pravila prema njegovom odabiru.

Iako ovaj mehanizam nije vidljiv korisniku, ovo je važna tehnologija koja omogućuje rad nekoliko funkcionalnosti, uključujući sandboxing, roditeljsku zaštitu i kontrolirane povlastice. Integriran je sa exec sistemskim servisom za sprječavanje izvršavanja neovlaštenih aplikacija. Ovo je baza za kontrolu aplikacija kod roditeljske zaštite i kontrolu povlastica kod server verzije. Kod sandboxa, mandatory access controls izvode restrikciju pristupa sistemskim resursima, određenu prema posebnom sandbox profilu. U ovom slučaju root korisnik također može imati veoma limitiran pristup sistemskim resursima. [9]

3.2 KORISNIČKE SIGURNOSNE ZNAČAJKE

3.2.1 FileVault 2

FileVault osigurava podatke kroz enkripciju cijelog diska te su podaci zaštićeni od neovlaštenog korištenja. Zaštita podataka je osigurana korištenjem XTS-AES 128 enkripcije, koja je brza i neprimjetna. Omogućuje enkripciju prijenosnog diska za lakšu izradu sigurnosne kopije pute TimeMachine funkcionalnosti. Korištenjem instantnog brisanja brišu se enkripcijski ključevi s diska, što podatke čini nepristupačnima. Samo korisnici kojima je omogućena mogućnost otključavanja diska, mogu pokrenuti ili otključati disk pod enkripcijom.

FileVault surađuje s funkcionalnosti OS X Recovery, posebnom particijom na disku koja omogućava korištenje Disk Utilitiy aplikacije na disku s kojim imamo problema. Ovo omogućava vraćanje starog stanja sustava ili ponovnu instalaciju OS X sustava putem Interneta, povratak sigurnosne kopije napravljene TimeMachine funkcionalnošću i korištenje Safari preglednika. Računalo se pokreće direktno s Recovery particije, te omogućuje prijavu na korisnički račun koji ima pristup pokretanju sustava.

3.2.2 Keychain

Keychain je sustav za upravljanje korisničkim lozinkama. Može spremiti lozinke za aplikacije, servere, web stranice, povjerljive podatke poput broja kreditne kartice ili PIN brojeva. Datoteke s lozinkama spremaju se na više lokacija —/System/Library/Keychains, /Library/Keychains, i userfolder/Library/Keychains. Uvijek postoji više keychainsa, sistemski keychain i više korisničkih keychainsa. Keychain Acess je aplikacija koja omogućava korisniku pregled i izmjenu postojećih lozinki, certifikata, web stranica, web formi i ostalih povjerljivih podataka. Moguće je zaključavanje, otključavanje i pregled lozinki spremljenih u sustavu, koje su

povezane sa glavnom korisničkom lozinkom., te pregled root certifikata, ključeva i sigurnosnih bilješki.

3.2.3 Kontrola korisničkih računa

Roditeljska zaštita pruža administratorima alate za primjenu određenog nivoa restrikcija za korisnike računala. Administrator računala može koristiti funkcionalnost Simple Finder za pokretanje seta aplikacija ili može kreirati listu web stranica koje korisnici mogu pokrenuti. Ako napadač ima fizički pristup računalu i njegovim ulaznim priključcima može zaobići ograničenja korištenjem zloćudnog softvera. Sigurnost se može postići onemogućavanjem ulaznih sučelja. Ovo je vrlo jednostavna administracija korištenja računala putem grafičkog sučelja, koja lako omogućava restrikciju pristupa aplikacijama ili pojedinim web stranicama koje sadrže zloćudni softver.

3.2.4 Vatrozid

Vatrozid ili firewall kod OS X sustava je aplikacija koja ima namjenu blokiranja neželjenog mrežnog prometa. Ovakav pristup vatrozidu putem aplikacije omogućuje lakše postavljanje vatrozida za prosječnog korisnika. Omogućava blokiranje nadolazećih veza na bazi aplikacije, u odnosu na bazi korištenog priključka.

Korisnici mogu ograničiti primjenu vatrozida na važne mrežne servise ili mogu dopustiti ili blokirati individualno pristup odabranim aplikacijama. Aplikacijski vatrozid koristi potpisivanje aplikacija za utvrđivanje njihova identiteta. Ako aplikacija nije sigurna, korisnik dobiva obavijest za potvrdu identiteta aplikacije. Jednom kad aplikacija bude odobrena, omogućen joj je pristup bilo kojem priključku koji zatraži. Postoji mogućnost da sav potpisan softver automatski ima omogućenu dolaznu vezu.

Za napredne korisnike dostupan je IPFW vatrozid. Pošto IPFW manipulira paketima na mrežnom sloju u odnosu na aplikacijski vatrozid, pravila IPFW vatrozida imaju veću važnost.

4 TESTIRANJE SIGURNOSTI

Macintosh računala i OS X sustav dulji niz godina izgrađuju reputaciju o svojoj sigurnosti. Prema mišljenju sigurnosnih stručnjaka stanje je drugačije. Smatraju da je OS X imao određene sigurnosne propuste čija je važnost umanjena, jedino zbog razloga jer nije došlo do njihove zlouporabe. Ovo podiže svijest o važnosti testiranja sigurnosti OS X sustava radi zašite od mogućih sigurnosnih propusta.

Pojam ranjivosti u kontekstu IT sustava se može definirati kao potencijalna slabost sistema ili infrastrukture, koja u slučaju iskorištavanja može dovesti do napada na sustav. Primjer ranjivosti je slaba lozinka, koja može biti otkrivena napadom uz korištenje rječnika te može doći do neovlaštenog korištenja računala.

Procjena ranjivosti koristi podatke o stvarnim ranjivostima koje mogu biti korištene protiv određenog softvera, u cilju utvrđivanja potencijalnih rizika za Mac računala i OS X sustav. Može otkriti na primjer da na nekom priključku koji želimo otvoriti za aplikaciju, potencijalno postoji rizik od iskorištavanja propusta. Otkrivanjem ovakvih ranjivosti možemo naći rješenje, te nadogradnjom sustava ili softvera otkloniti sigurnosne propuste. Zbog Internet pristupa nemamo mogućnost zatvoriti sva mrežne sučelja, pa procjena ranjivosti pomaže u otkrivanju i rješavanju određenih područja slabosti sustava.

Procjena ranjivosti (VA – eng. Vulnerability assessment) i testiranje ranjivosti (PT – eng. Penetration testing) su najviše korišteni tipovi procjene sigurnosti. Procjenu ranjivosti provodimo korištenjem programa Nessus, koji je dizajniran za otkrivanje ranjivosti i generiranje obavijesti o stanju sustava bez mogućnosti testiranja pronađenih ranjivosti i propusta. Za korak dalje i implementaciju određenih napada na pronađene propuste korišten je program Metasploit. Ovo je jedini način na koji možemo sa sigurnošću potvrditi koliki je rizik za naše Mac računalo. Potrebno je napomenuti da ovi alati pružaju dobre rezultate ako se ispravno koriste. Pogrešna konfiguracija može dovesti do pogrešnih rezultata koji mogu, ali ne moraju pokazati prave ranjivosti sustava.

Korištenjem ovih alata kroz određene periode, organizacija može na vrijeme otkriti ranjivosti svoje informatičke infrastrukture. Svijest o određenim ranjivostima na vrijeme, može organizaciji pomoći u ispravku propusta, te na taj način unaprijed umanjiti rizik od iskorištavanja istih. Neki od rizika u slučaju iskorištavanja propusta uključuju:

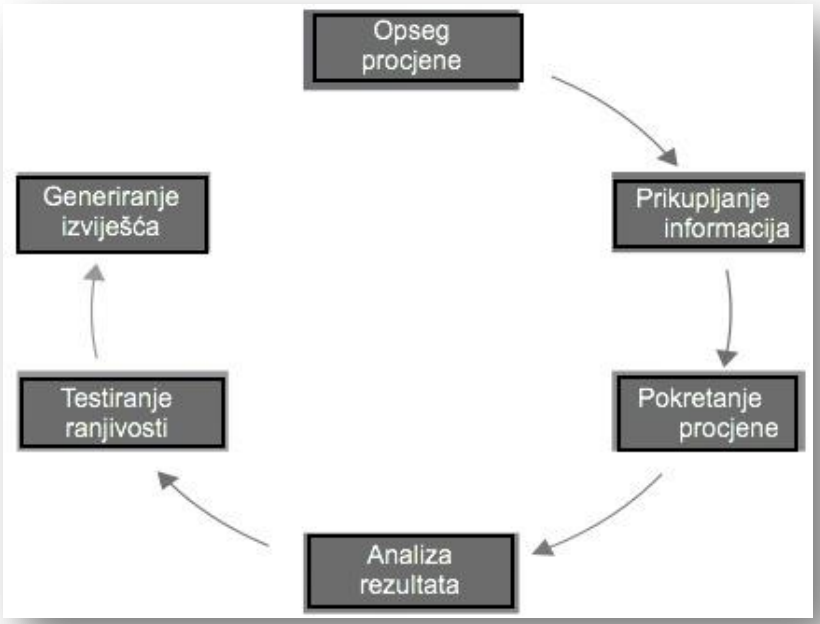
- Financijska šteta
- Reputacija organizacije

- Krađa podataka
- Kompromitacija provjerljivosti
- Kompromitacija dostupnosti

4.1 FAZE U PROCJENI I TESTIRANJU RANJIVOSTI

Preporučljivo je da se procjena i testiranje ranjivosti provode na temelju potreba i ciljeva organizacije. Faze provedbe u organizaciji uključuju:

- Opseg procjene
- Prikupljanje informacija
- Procjena ranjivosti
- Analiza rezultata
- Testiranje ranjivosti
- Generiranje izvješća



Slika 4.1 Prikaz faza procjene i testiranja ranjivosti [11]

4.1.1 Faza 1: Opseg procjene

Određivanje opsega procjene sustava je prvi korak u bilo kojoj sigurnosnoj provjeri. Prvi korak određuje infrastrukturu na kojoj vršimo provjeru, na primjer serveri, mrežni uređaji, baze ili aplikacije. Ovo se određuje prema sigurnosnom cilju organizacije. Potrebno je dogovoriti ukupno trajanje skeniranja sustava i tipovi napada koji su dopušteni prilikom testiranja. U ovoj fazi dolazi do planiranja i pripreme za testiranje sustava, određivanje tima, datuma i vremena provođenja procjene i testiranja.

Bitna stvar kod testiranja sigurnosti je pismeni dogovor između tvrtke koja provodi testiranje, te tvrtke koja je zatražila sigurnosnu provjeru infrastrukture. Potrebno je odrediti broj elemenata sustava nad kojima se provodi testiranje, uz određivanje metodologije procjene koja je u skladu s poslovnim ciljevima organizacije. Organizacija bi trebala odrediti tipove napada na infrastrukturu koju želi testirati.

4.1.2 Faza 2: Prikupljanje informacija

Prikupljanje informacije je najvažnija faza u procjeni i testiranju ranjivosti infrastrukture. Uključuje pronalažene informacija o ciljanom sustavu koristeći tehničke i ostale metode kao pretraživanje Interneta. Ovo je ključan korak jer pomaže stvoriti sliku ciljanje infrastrukture i njezinih resursa. Pošto je procjena ranjivosti obično vremenski ograničena, informacije prikupljene tijekom ove faze pomažu usmjeriti testiranje u pravom smjeru, te na korištenje ispravnog pristupa i alata.

Nakon prikupljanja informacija slijedi tehnički dio mapiranja ciljane mreže koristeći alate kao ping i Telnet, uz alat za skeniranje priključaka NMAP. Korištenje ovih alata omogućava pronalaženje domaćina, otvorenih servisa, operativnih sustava, te ostalih informacija. Informacije prikupljene kroz mrežno mapiranje dodatno potvrđuju informacije prikupljene kroz pasivne metode o ciljanoj infrastrukturi, što je veoma bitno kod konfiguriranja alata za procjenu ranjivosti. Ovo osigurava da skeniranje infrastrukture bude ispravno obavljeno.

4.1.3 Fraza 3: Procjena ranjivosti

U ovoj fazi dolazimo do provođenja procjene ranjivosti ciljane infrastrukture. Ovo provodimo korištenjem alata poput programa Nessus. Prije same procjene, alat mora biti optimalno konfiguriran prema prikupljenim informacijama u prijašnjim fazama. Potrebno provjeriti da li su postavljane iznimke u vatrozidu sustava, tako da alat može provesti skeniranje infrastrukture. Alati provode pretraživanja protokola TCP, UDP i ICMP s ciljem pronalaska otvorenih priključaka i servisa koji su pokrenuti na ciljanom uređaju, te ih uspoređuju s poznatim

ranjivostima iz svoje baze, za potvrdu pronalaska određenih ranjivosti infrastrukture. Rezultat ove faze pruža sveobuhvatan pogled na ranjivosti koje postoje unutar ciljanje infrastrukture, koje u slučaju zlouporabe mogu dovesti do kompromitiranja sustava.

4.1.4 Faza 4: Analiza rezultata

Kao rezultat faze procjene ranjivosti dobivamo listu ranjivosti ciljane infrastrukture. Ključna aktivnost analize liste je brisanje ranjivosti koje su lažno pozitivne, zapravo nisu ranjivosti infrastrukture. Većina alata je sklona prijavljivanju određenih lažno pozitivnih rezultata, te je potrebno obaviti analizu korištenjem metoda kao što je stvaranje veza između ranjivosti i prethodno prikupljenih informacija iz prijašnjih analiza, uz provjeru da li zbilja dobivamo pristup sustavu iskorištavanjem pronađenih ranjivosti. Alati za procjenu ranjivosti daju ocjenu rizika pronađenih ranjivosti, ovisno o važnosti elementa infrastrukture i učinku ranjivosti.

4.1.5 Faza 5: Testiranje ranjivosti

Za dokazivanje pronađenih ranjivosti u svrhu prikaza štete koja može nastati u slučaju kompromitiranja sustava, potrebno je demonstrirati napad u kontroliranom okružju bez štete na infrastrukturi, ako je potrebno. Testiranje ranjivosti je sljedeći korak koji ima za cilj iskoristiti propuste pronađene u prethodnim fazama. Testiranje ranjivosti može se podijeliti u faze prije testiranja, testiranje i poslije testiranja. Aktivnosti u fazi prije testiranja opisane su fazama 1-4.

Nakon što je ranjivost iskorištena za dobivanje pristupa sustavu, napadač bi trebao imati za cilj dobivanje dodatnih informacija prisluškivanjem prometa, mapinjem unutarnje mreže te dobivanje maksimalne razine pristupa sustavu. Ovime dobivamo mogućnost za pokretanjem dodatnih napada na mrežu, u cilju šireg kompromitiranja sustava. Faza poslije testiranja uključuje brisanje tragova provođenjem aktivnosti poput brisanja zabilješki i onemogućavanjem antivirusne zaštite.

4.1.6 Faza 6: Generiranje izvješća

Nakon provođenja testiranja, zadnji korak uključuje izradu izvješća koji sadrži određene korake:

- Kratak uvod o provođenju procjene
- Opis opsega procjene
- Sažetak vođenja procesa procjene
- Pregled pronađenih ranjivosti uz procjenu rizika

- Detalji o pronađenim ranjivostima i mogućem učinku na sustav uz preporuke o ispravljanja propusta

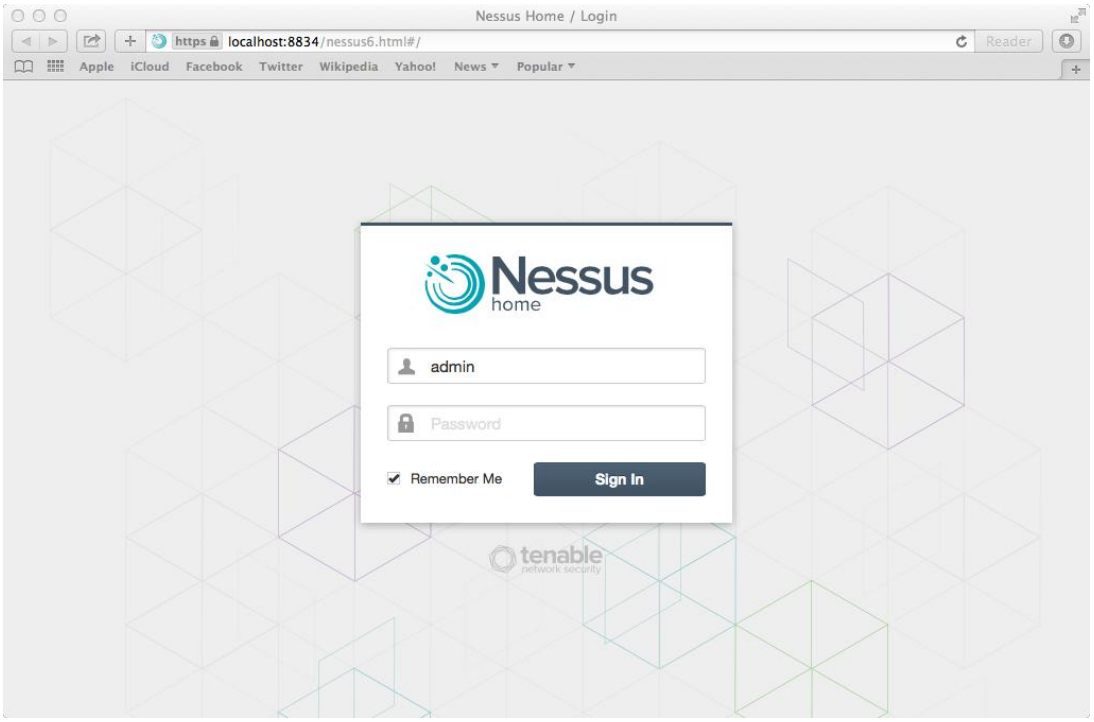
4.2 PROCJENA RANJIVOSTI SUSTAVA KORIŠTENJEM PROGRAMA NESSUS

Procjena ranjivosti sustava ili jednostavnije pronalaženje ranjivosti testirane infrastrukture, ključna je aktivnost koja se provodi korištenjem alata poput programa Nessus. Prilikom korištenja alata za procjenu ranjivosti bitna je ispravna konfiguracija parametara skeniranja, te efikasnost procjene, imajući u vidu infrastrukturu na kojoj radimo procjenu. Ovo će rezultirati efikasnom procjenom ranjivosti uz optimizirano vrijeme trajanja skeniranja.

Konfiguracija procjene ranjivosti uključuje dva glavna koraka, konfiguriranje strategije i pokretanje procjene korištenjem strategije. Preporučljivo je imati direktnu konekciju Nessus programa sa ciljanim sustavom za bolje rezultate, ovo znači da je potrebno isključiti vatrozid ili neki drugi uređaj koji može blokirati promet između Nessusa i ciljanog sustava.

4.2.1 Procjena ranjivosti OS X sustava

Nessus ima mogućnost kreiranja korisničkih računa, funkcionalnost koja je korisna u većim tvrtkama. Ova funkcionalnost omogućava administratoru kreiranje korisnika s različitim razinama pristupa za provedbu procjene ranjivosti sustava.



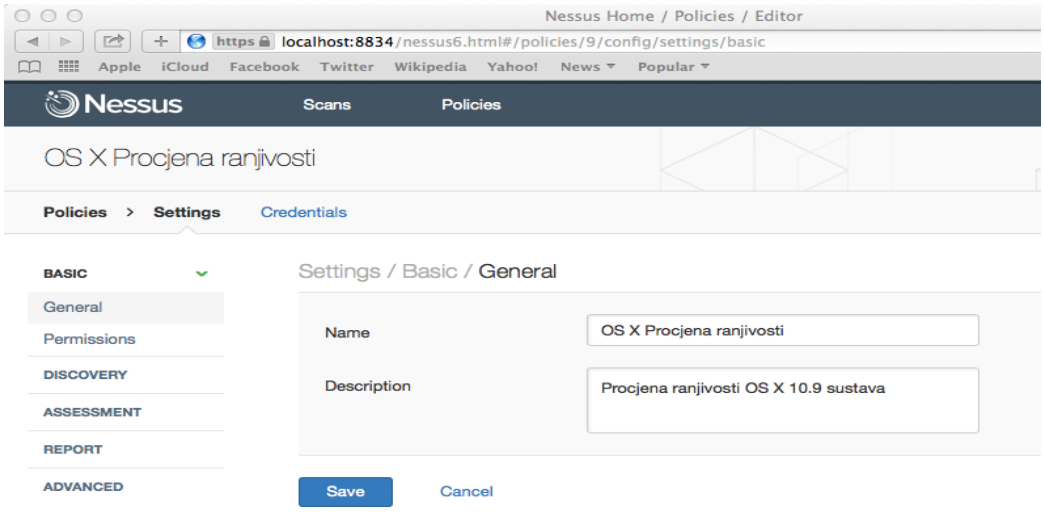
Slika 4.2 Pristup Nessus programu putem web sučelja

Nessus program se može preuzeti na stranicama proizvođača i besplatan je za kućnu uporabu. Verzija programa se bira prema sustavu na kojem instaliramo program, odnosno s kojeg

provodimo procjenu ranjivosti, a ne prema ciljanom sustavu. U našem slučaju preuzimamo verziju 6.0 za OS X sustav. Nakon preuzimanja programa slijedi instalacija, zatim pokretanje programa u web okružju te kreiranje administratorskog računa. Nakon pristupanja programu putem administratorskog računa, kreiramo strategiju skeniranja. Ako je potrebno možemo promijeniti postavke programa, isključiti određene dodatke, kreirati korisnika, postaviti proxy postavke i ostalo, ali za osnovnu procjenu ranjivosti ostavljamo početne postavke. Nessus pruža mogućnost prilagođavanja strategija procjene prilagođene organizacijskoj strategiji. Pruža fleksibilnost prilagođavanja strategije temeljenu na našim potrebama prije pokretanja procjene.

Glavni parametri koji mogu biti konfigurirani prilikom kreiranja strategije su:

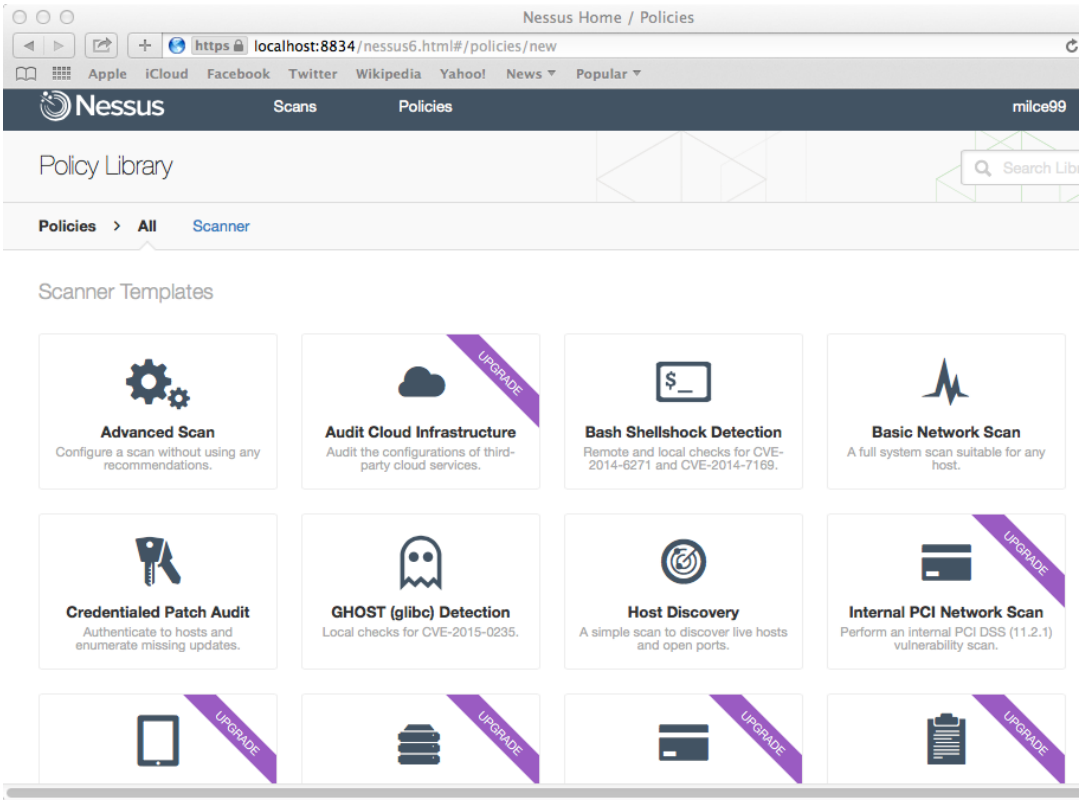
- Ime strategije
- Tip skeniranja priključaka
- Performanse procjene u vidu maksimalnog broja provjera u istom trenutku, ujedno i vrijeme trajanja procjene
- Opcija unosa korisničkih podataka sustava nad kojim se provodi procjena ranjivosti
- Opcija odabira najprikladnijih dodataka
- Dodatne postavke za posebne provjere



Slika 4.3 Kreiranje strategije za procjenu ranjivosti sustava

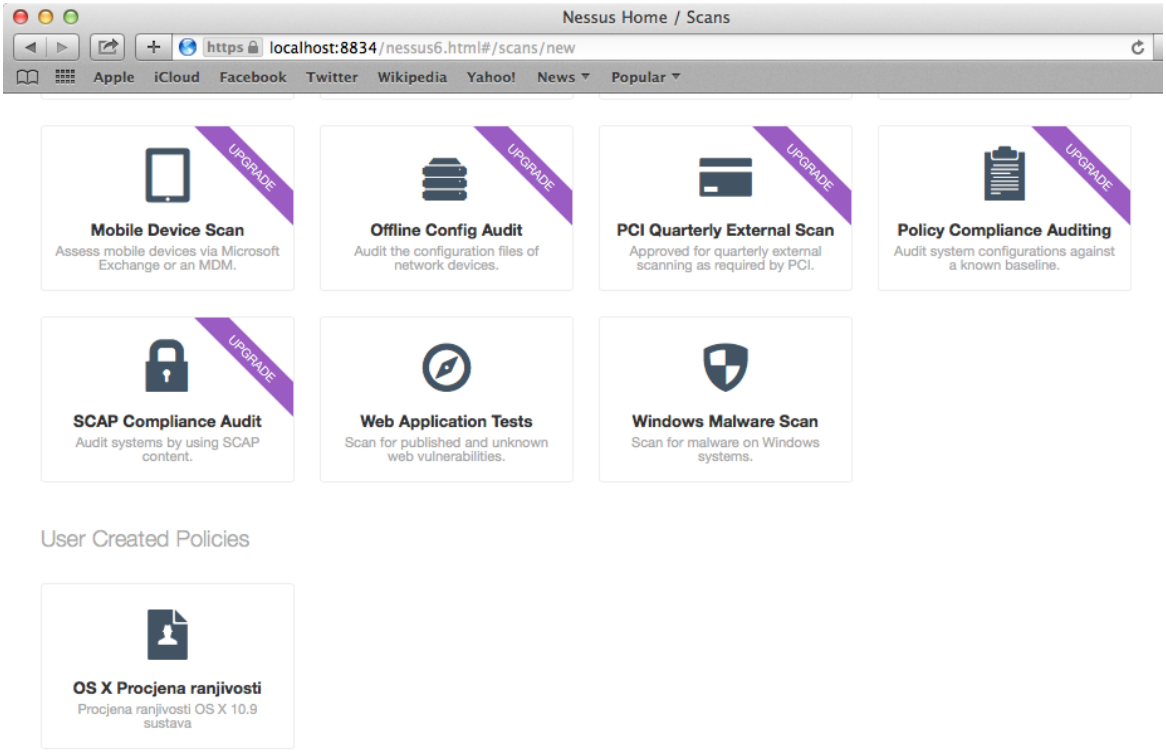
Nessus pruža mogućnost uvoza vlastitih strategija, izvoz, spremanje i brisanje postojećih strategija. Naravno postoji mogućnost korištenja predefiniranih strategija prilagođenih za različite procjene, ali u našem slučaju kreiramo vlastitu strategiju. Strategiju kreiramo odabirom

Policy taba, te odabiremo osnovnu mrežnu procjenu koja omogućava procjenu ranjivosti cijelog sustava. Osnovne postavke ne mijenjamo, dajemo ime strategije i detaljni opis, prikazano na slici 4.3.

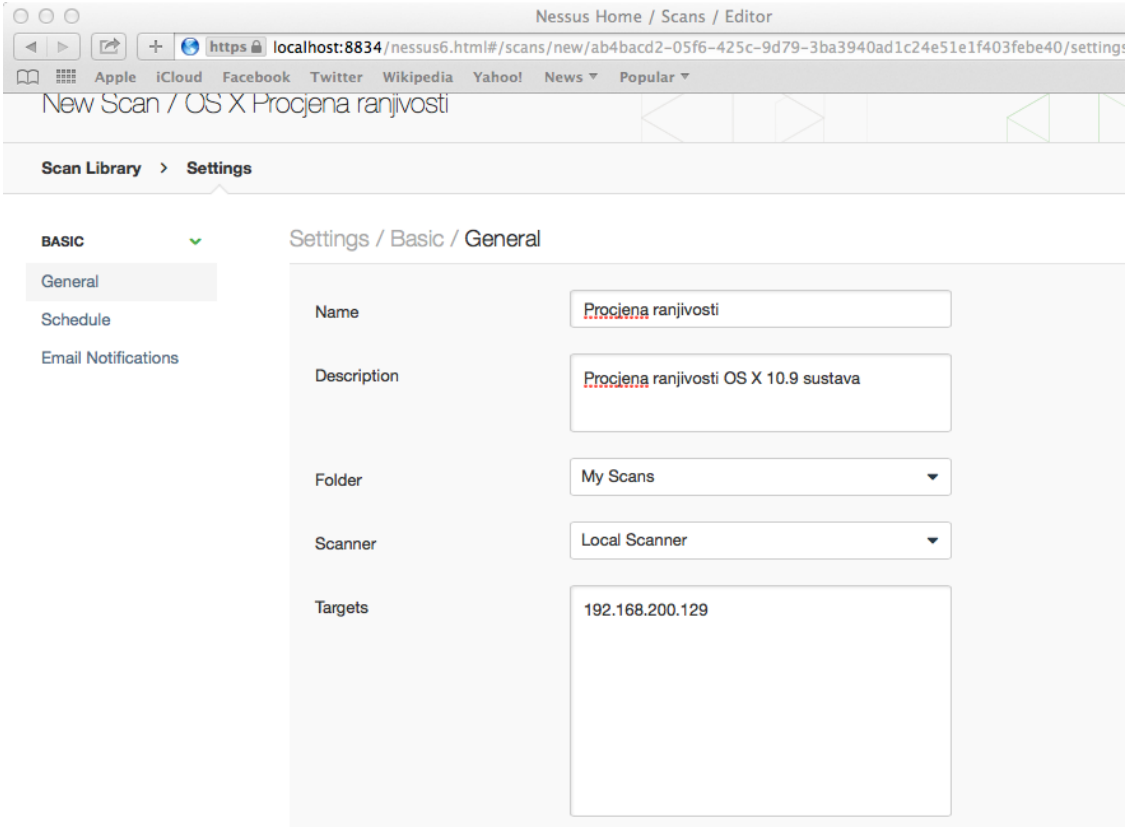


Slika 4.4 Odabir načina procjene ranjivosti prilikom kreiranje strategije

Kreiranjem strategije spremni smo za pokretanje procjene sustava u svrhu pronalaska ranjivosti. Kreiramo novu procjenu ranjivosti sustava odabirom kreirane strategije, vidljiva je već prije kreirana strategija na slici 4.5. Pod glavnim postavkama stavljamo naziv procjene, vrijeme pokretanja, odabir strategije i IP adrese sustava nad kojima izvršavamo procjenu ranjivosti. Postoji i mogućnost uploada datoteke koja sadrži listu IP adresa sustava. Moguće je navesti e-mail adrese na koje se prosljeđuju rezultati procjene ranjivosti. Trajanje procjene ovisi o sustavu nad kojim provodimo procjenu. Izvršenjem procjene dostupni su nam rezultati i detaljan opis svake ranjivosti.



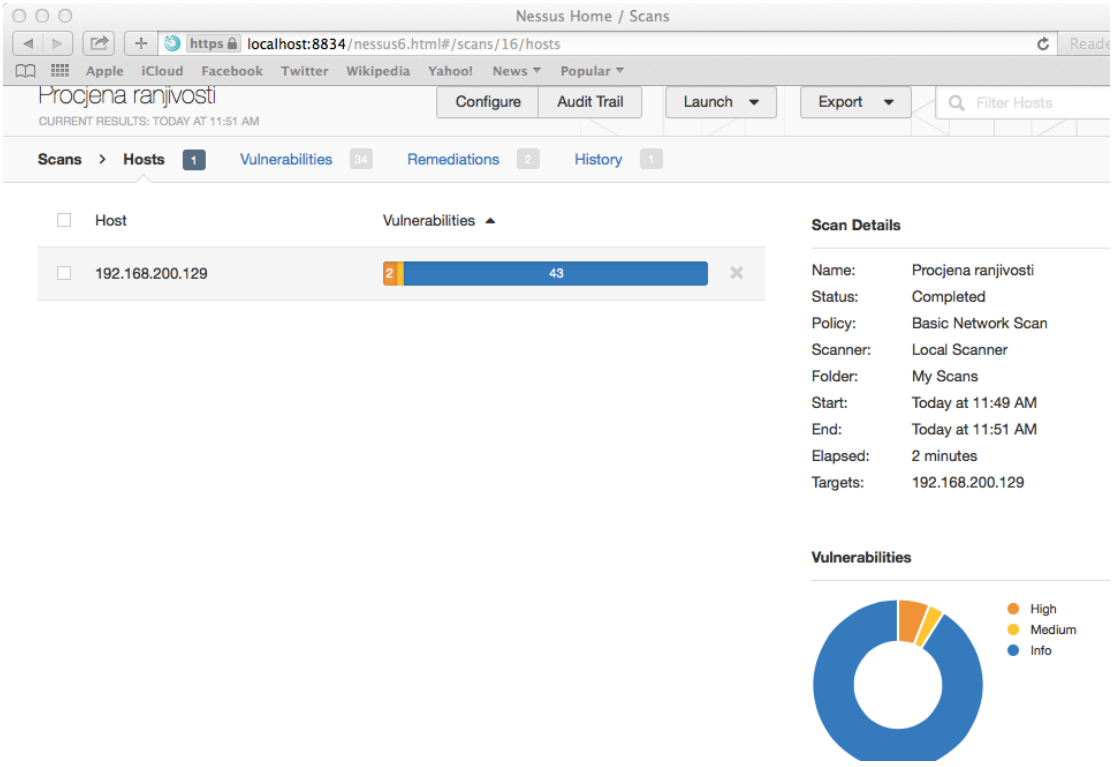
Slika 4.5 Odabir strategije prilikom kreiranja nove procjene ranjivosti sustava



Slika 4.6 Glavne postavke procjene ranjivosti sustava

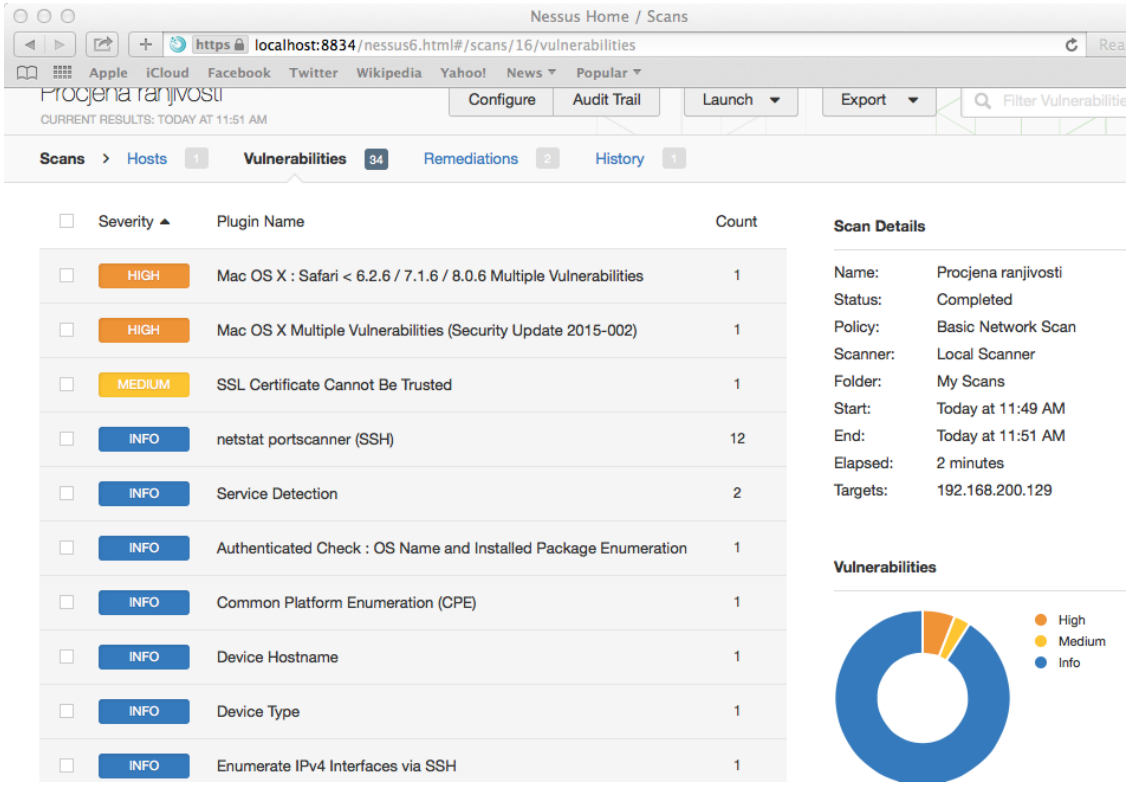
4.2.2 Analiza rezultata procjene ranjivosti

Dobivene rezultate procjene potrebno je analizirati, izbaciti lažno pozitivne rezultate te učiniti potrebne promjene za poboljšanje sigurnosti sustava. Ranjivosti su podijeljene na srednje, visoke i kritične ranjivosti sustava, dodatno prikazane tortnim dijagramom kao što je vidljivo na slici 4.7. Pod detaljnim pregledom rezultata dostupne su nam informacije o skeniranom domaćinu koji prikazuje IP adresu, te broj pronađenih ranjivosti prema prethodnoj podjeli. Kod naše procjene 10.9 verzije sustava pronađene su 2 važne ranjivosti, 1 srednje važna i 43 preporuke za poboljšanje sigurnosti.

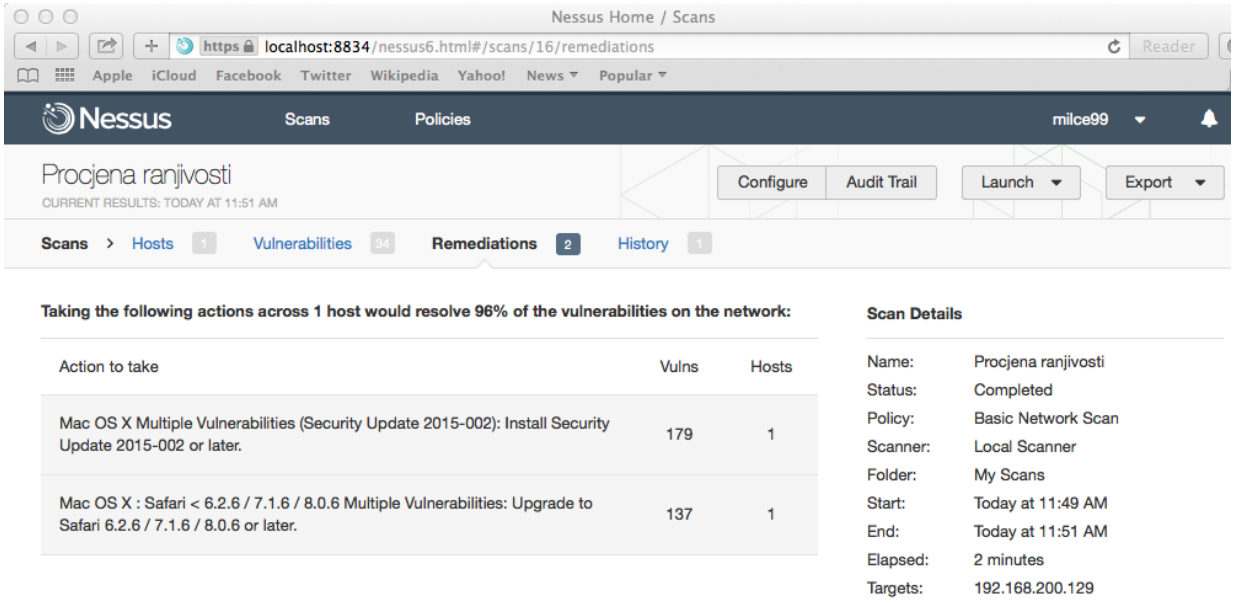


Slika 4.7 Osnovni prikaz rezultata procjene ranjivosti sustava

Pod dijelom Vulnerabilities prikazana nam je lista ranjivosti uz njihov broj i pojedinačnu procjenu rizika za sustav. Odabirom ranjivosti dobivamo detaljan pregled koji uključuje opis, rješenje, poveznice na web rješenja, informacije o dodacima, procjenu rizika i ostalo. Remediations dio sadrži akcije koje možemo poduzeti da smanjimo broj ranjivosti sustava. Dobivamo detaljan opis akcije, broj ranjivosti koje bi bile riješene i na kolikom broju sustava. U našem slučaju poduzimanjem dvije akcije riješili bi se 96 % pronađenih ranjivosti našeg OS X sustava. Prva preporučena akcija je preuzimanje i instaliranje Sigurnosne nadogradnje 2015-002 koja bi riješila 179 ranjivosti, dok druga akcija uključuje nadogradnju Safari preglednika na najnoviju verziju, ovime rješavamo 137 ranjivosti sustava. Ove preporuke prikazane su na slici 4.9.



Slika 4.8 Prikaz ranjivosti u obliku liste s detaljima



Slika 4.9 Preporučene akcije za smanjenje broja ranjivosti OS X sustava

4.3 TESTIRANJE RANJIVOSTI KORIŠTENJEM PROGRAMA METASPLOIT

Testiranje ranjivosti ima dodatan korak nad procjenom ranjivosti, iskorištavanje pronađenih propusta. Testiranje ranjivosti je nametljiv test, prvi korak je procjena ranjivosti za pronalaženje propusta, a zatim pokušaj ulaska u sustav iskorištavanjem pronađenih ranjivosti.

Testiranje ranjivosti je napad na računalni sustav s namjerom pronalaženja sigurnosnih ranjivosti, ovjere sigurnosti sustava i pronalaženja pristupa sustavu iskorištavanjem pronađenih ranjivosti. Testiranje ranjivosti ima za cilj poboljšanje sigurnosti sustava određene organizacije. Uspjeh u testiranju sigurnosti uvelike ovisi o korištenim alatima i tehnikama. Tu dolazimo do jednog od najefektivnijih alata za testiranje ranjivosti Metasploit-a. U fazi testiranja ranjivosti prema ciljanom sustavu šaljemo eksploite, koji ciljaju prethodno pronađene ranjivosti sustava s ciljem dobivanja pristupa resursima sustava.

4.3.1 Priprema alata

Za testiranje ranjivosti koristimo Kali Linux OS koji je namijenjen za testiranja sigurnosti, te ima instaliran alat Metasploit. Kali Linux radi jednostavnosti koristimo u virtualnom okružju. Nakon potrebne instalacije sustava Kali Linux i od prije provedene procjene ranjivosti spremni smo za izvođenje testiranja ranjivosti korištenjem alata Metasploit.

Bez obzira na sučelje Metasploita koje koristimo, grafičko ili komandno, proces testiranja ranjivosti provodimo prema poznatoj proceduri:

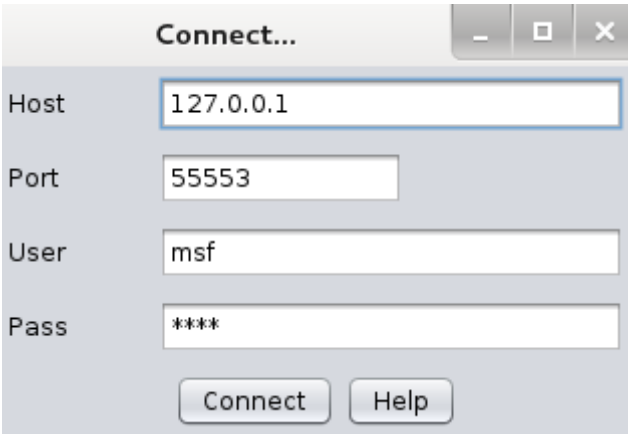
- Odabir eksploita – potrebno je odabrati ekploit koji je dizajniran za ciljani operativni sustav, softver i priključke. Metasploit dijeli eksploite u grupe prema operacijskom sustavu i pruža mogućnost pretrage baze eksploita.
- Odabir cilja – cilj se odnosi na specifični servis nad kojim se izvodi napad.
- Odabir korisnog sadržaja – odabir programskog koda koji izvodi napad.
- Postavke – namještamo postavke odabranog ekploita ili korisnog sadržaja. U većini slučajeva koristimo početne postavke, ali u pojedinim slučajevima potrebno je ručno namjestiti postavke.
- Pokretanje eksploita – nakon namještanja opcija pokretanje eksploita je jednostavna radnja. Ako pokretanje eksploita bude uspješno, omogućeno je upravljanje napadnutim sustavom.

4.3.2 Armitage

Armitage je alat s grafičkim sučeljem koji podiže korištenje Metasploit okružja na novu razinu. Inteligentan alat za Metasploit koji vizualizira ciljani sustav, daje preporuke eksploita i prikazuje napredne funkcije za korištenje nakon iskorištavanja ranjivosti i dobivanja pristupa sustavu. Sadrži funkcionalnosti za otkrivanje, pristup i fazu poslije pristupa sustavu. Moguće je pokretanje skeniranja i uvoz podataka iz mnogih sigurnosnih alata. Omogućuje vizualizaciju trenutno ciljanih sustava, te na taj način omogućuje prepoznavanje domaćina i lakše praćenje trenutno pokrenutih testiranja. Armitage daje preporuke eksploita koji se mogu primijeniti, te mogućnost aktivnih provjera s ciljem određivanja eksploita koji funkcioniraju. Ako navedene opcije ne uspiju, postoji opcija Hail Mary koja omogućuje pametno automatsko korištenje eksploita na ciljanom sustavu.

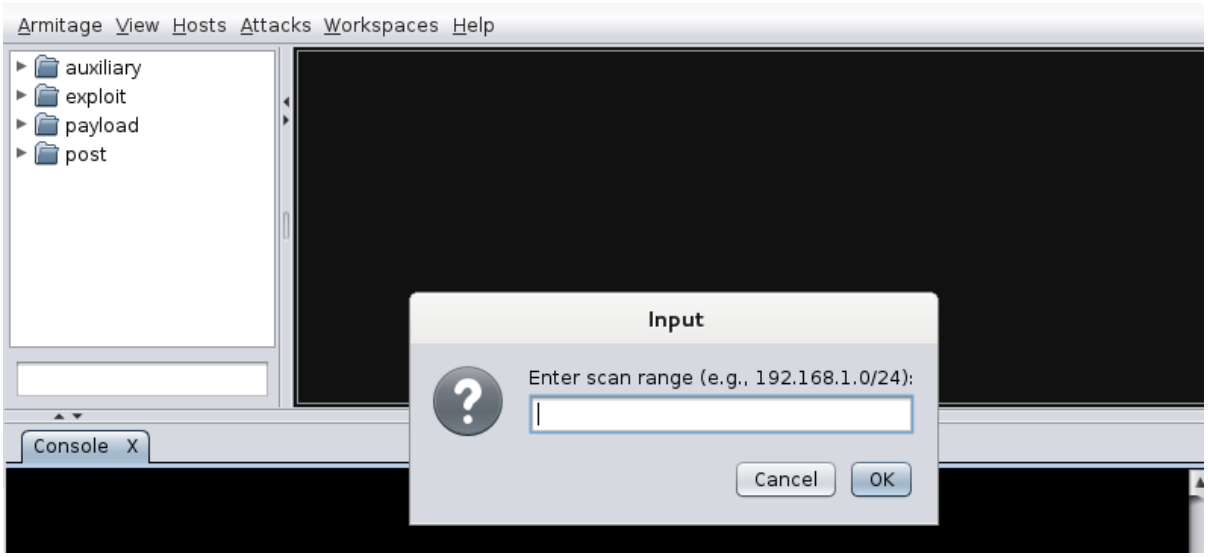
Nakon dobivanja pristupa sustavu pruža se mogućnost korištenja raznih ugrađenih alata. U samo par odabira moguća je eskalacija privilegija, pregled datotečnog sustava, korištenje komandi i ostalo. Korištenjem Armitage alata olakšavamo proces testiranja ranjivosti korištenjem njegovih mnogobrojnih funkcionalnosti.

Za prvi korak pokrećemo alat Armitage putem naredbe ili pronalaskom programa pod aplikacijama. Ostavljamo početne postavke i pokrećemo konekciju, alat nakon toga automatski pokreće Metasploit program za testiranje ranjivosti. Armitage funkcionira tako da šalje RPC pozive prema Metasploit programu.



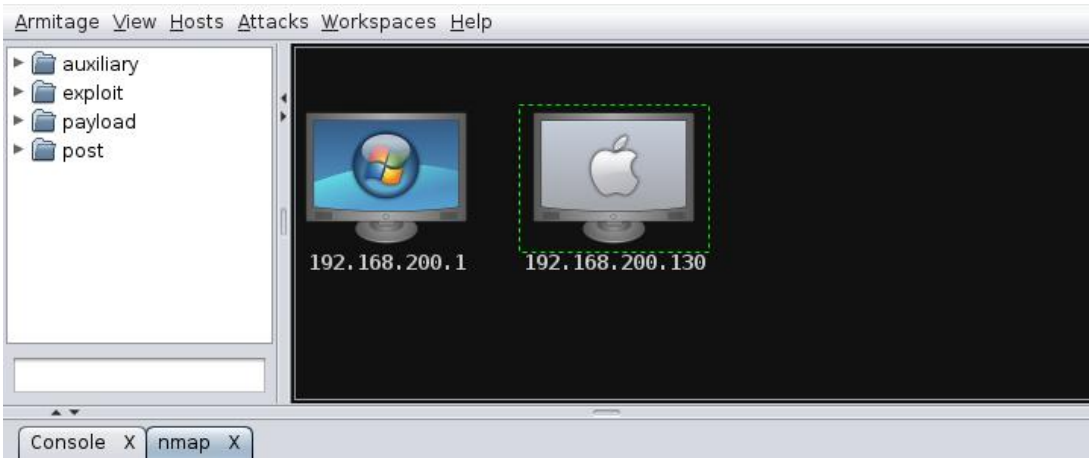
Slika 4.10 Pokretanje Armitage alata

Nakon pokretanja alata odabiremo Nmap skeniranje mreže koje nam omogućuje pronalazak uređaja na mreži, njihove IP adrese i operativni sustav. Odmah nakon pokretanja Nmap alata unosimo raspon IP adresa nad kojima izvodimo pretragu. Rezultati skeniranja i pronađeni uređaji prikazani su grafički u sučelju alata.



Slika 4.11 Pokretanje Nmap alata

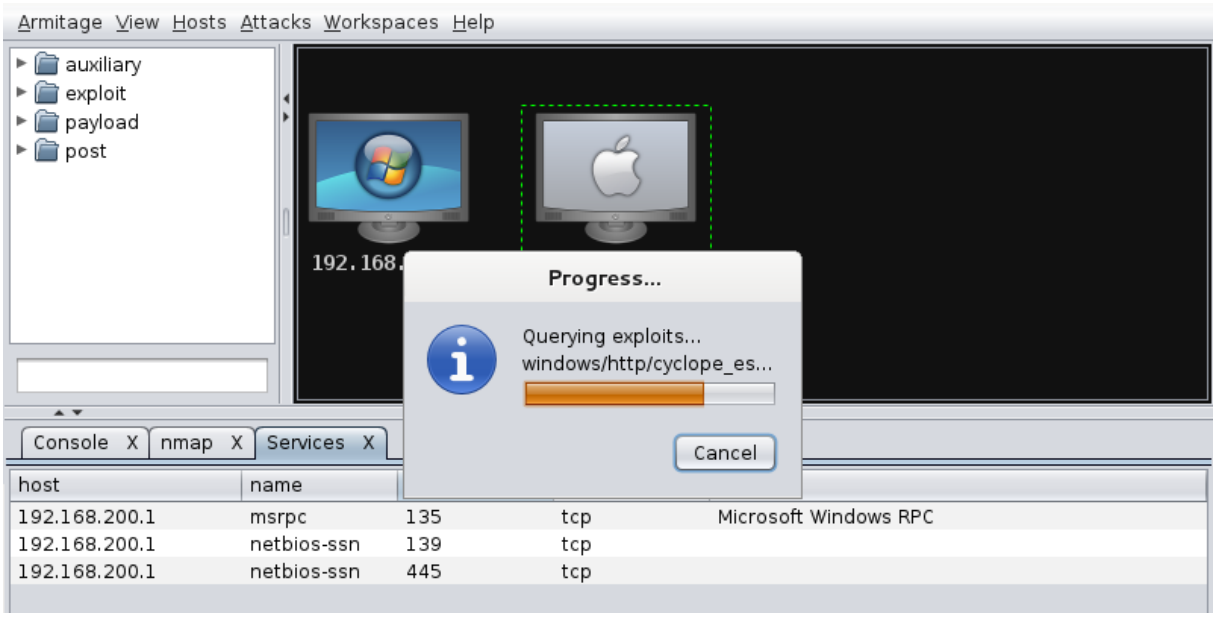
Nakon završetka Nmap skeniranja dobivamo prikaz dostupnih domaćina na mreži i grafički prikaz njihovih operativnih sustava. U našem slučaju dostupna su dva domaćina, od koji jedan koristi Windows a drugi koristi OS X nad kojim želimo provesti testiranje ranjivosti.



Slika 4.12 Prikaz rezultata skeniranja i pronađenih domaćina

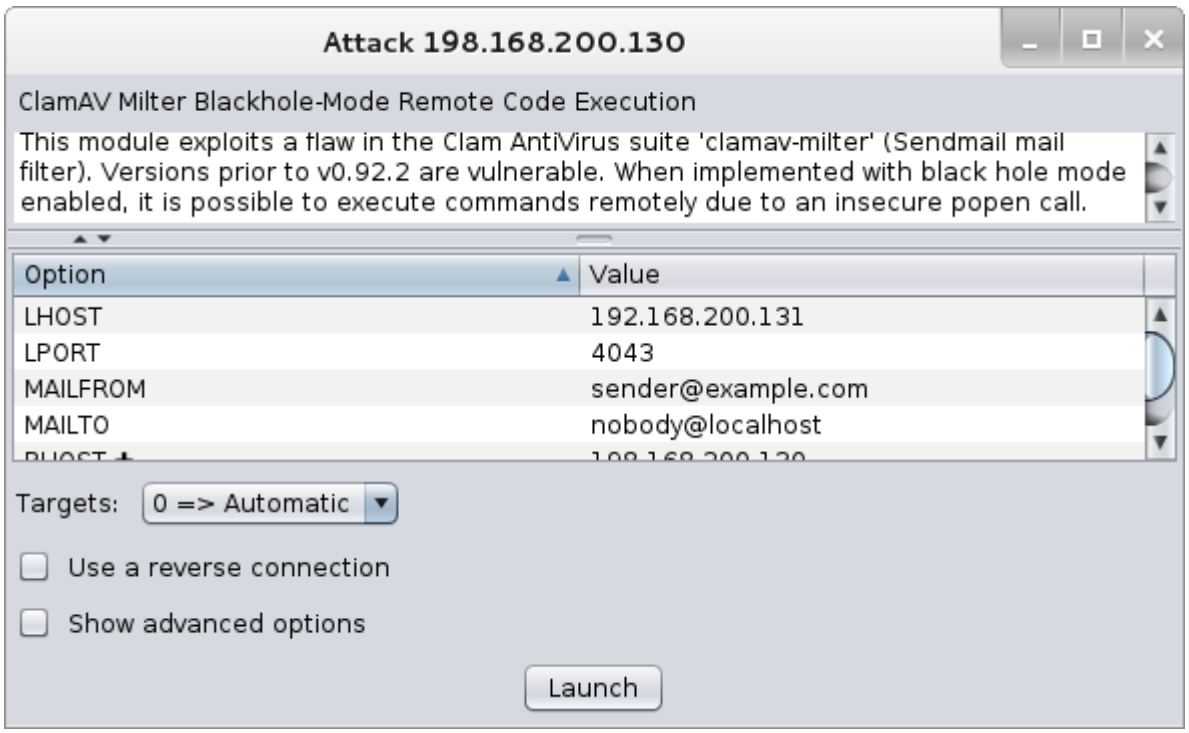
Armitage kreira novi tab za svaku novu radnju što omogućava lakšu promjenu ciljanog sustava te lakše prikupljanje informacija. Dostupno nam je i komandno Metasploit sučelje ako su potrebne napredne radnje koje nisu dostupne u Armitage alatu.

Nakon pronalaska dostupnih domaćina, sljedeći korak je automatsko pronalaženje poznatih ranjivosti OS X sustava nad kojim provodimo testiranje. Armitage prikazuje dostupne eksploite na temelju informacija o otvorenim priključcima i pronađenim ranjivostima sustava. Za automatsko pronalaženje eksploita koristimo Attacks opciju dostupnu unutar sučelja Armitage alata.



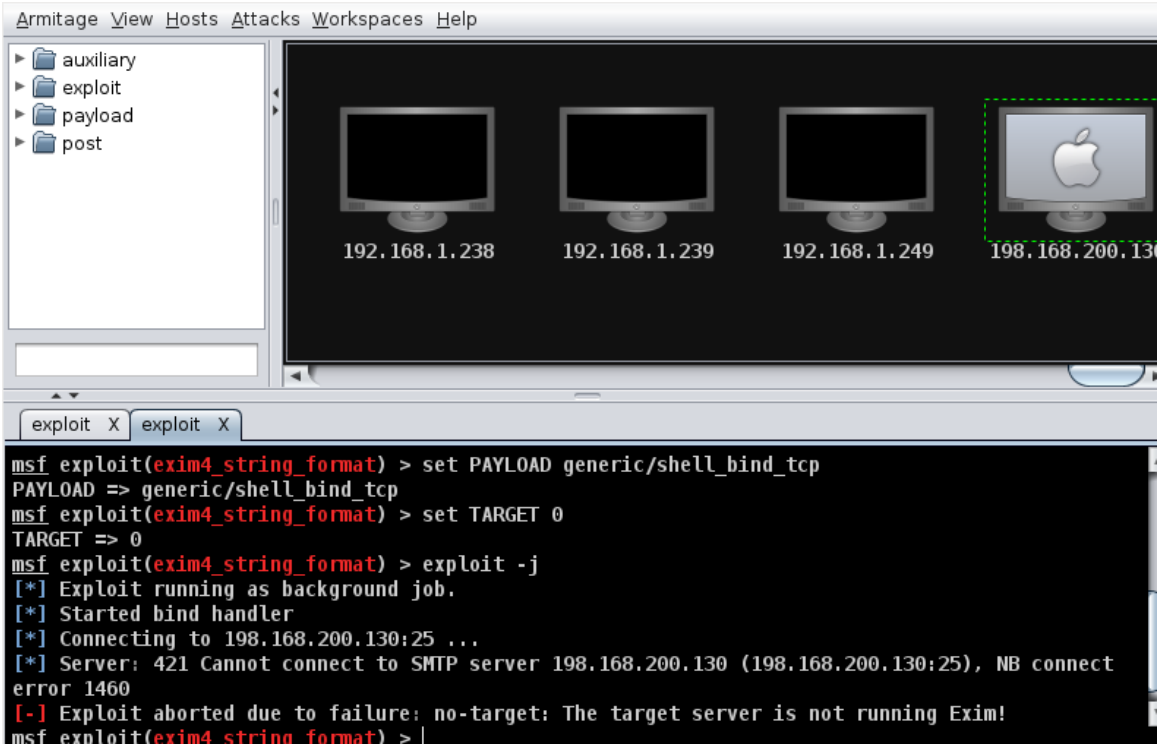
Slika 4.13 Pronalazak dostupnih eksploita za ciljani sustav

Nakon pronalaska eksploita desnim klikom na domaćina dostupna nam je dodatna opcija Attack, koja pruža odabir napada koji su pronađeni od strane Armitage alata. U slučaju OS X sustava pronađena su dva eksploita koja mogu biti korištena za testiranje ranjivosti sustava. Pokretanje odabranog ekploita otvara mogućnost podešavanja dodatnih opcija prije izvršavanja. Odabirom naredbe launch pokrećemo testiranje te nam rezultat ubrzo dostupan.



Slika 4.14 Pokretanje pronađenog eksploita za testirani OS X sustav

Kod provedenog testiranja OS X sustava pronađena su dva eksploita koja nisu rezultirala uspješnim iskorištavanjem ranjivosti. Prikaz neuspješnog iskorištenja ranjivosti korištenjem pronađenog eksploita za OS X prikazano je na slici 4.15.



Slika 4.15 Prikaz procesa korištenja eksploita na OS X sustavu

U slučaju uspješnog korištenja eksploita dolazi do iskorištavanja ranjivosti sustava, te dobivamo mogućnost korištenja Meterpreter opcije unutar Armitage sučelja. Ova opcija omogućava ubacivanje korisnog sadržaja koji izvodi određene naredbe u svrhu upravljanja operativnim sustavom.

Nakon provedenog testiranja OS X sustava korištenjem Armitage i Metasploita alata možemo doći do zaključka da su sigurnosni mehanizmi OS X sustava dobro implementirani. Unatoč pronađenim ranjivostima i korištenjem alata Metasploit, pri testiranju ranjivosti nije došlo do uspješnog iskorištavanja ranjivosti i u konačnici zadobivanju pristupa OS X sustavu.

5 OPIS PROGRAMA

Prilikom skeniranja računala na ranjivosti putem mreže koje mogu iskoristiti otvorene priključke, koristio sam poznat alat dostupan za OS X: Nessus. Dok sam za testiranje i potvrdu pronađenih ranjivosti koristio alat Metasploit. Radi se o poznatim alatima za skeniranje i testiranje ranjivosti sustava. U ovom poglavlju objašnjen je njihov način funkcioniranja, mogućnosti i primjena.

5.1 NESSUS

Trenutno program koji je u svijetu prepoznat kao najbolji na području alata za pronalaženje mrežnih ranjivosti, izdan od tvrtke Tenable Network Security. Prva verzija izdana je 1998 godine od strane Renaulda Deraisona, te je ovaj alat jedan od najpopularnijih alata za procjenu ranjivosti u zadnjih 15 godina. Prethodne verzije programa do 2005 godine i verzije 3 bile su otvorenog koda, a nakon toga dostupne su besplatno jedino za osobnu uporabu. Program je dostupan za OS X, Windows i Linux platformu i sadrži grafičko sučelje. [10]

Kroz godine Nessus se razvio od osnovnog alata za skeniranje sustava u alat koji uključuje funkcionalnosti za reviziju konfiguracija, dodataka, kontrolnih sustava i mobilnih uređaja. Poznat je po lakoći korištenja i fleksibilnosti alata za procjenu ranjivosti sustava.

Ključna infrastruktura koja prolazi kroz procjenu ranjivosti uključuje:

- Mrežne uređaje: Juniper, Cisco, vatrozid, pisači
- Virtualni domaćini: VMware ESX, ESXi, vSphere, vCenter
- Operativni sustavi: Windows, Mac, Linux, Solaris, BSD, Cisco iOS, IMB iSeries
- Baze podataka: Oracle, MS SQL Server, MySQL, DB2, PostgreSQL
- Web aplikacije: web serveri, web servisi

Nessus pruža fleksibilnost planiranih procjena ranjivosti ciljanih domaćina. Moguće je konfigurirati raspored i vrijeme procjene uz određivanje metode. Nessus će automatski inicijalizirati procjenu u definirano vrijeme i poslati e-mailom rezultate na unaprijed definirane e-mail adrese.

Za osiguravanje opsežne procjene sigurnosti, Nessus pruža veliki izbor dodataka, koji su posebno grupirani za određenu sigurnosnu procjenu. Grupiranje pruža korištenje velikog broja dodataka specifičnih za pojedinu infrastruktura. Veće grupe dodataka uključuju Windows, Linux, Cisco, Solaris i baze podataka. Nessus pruža prikaz rezultata u različitim formatima,

poput HTML, PDF, CSV. Ovo omogućuje lakše korištenje rezultata u drugim alatima za analizu. [11]

5.2 METASPLOIT

Metasploit je trenutno najpoznatija riječ u području informacijske sigurnosti i testiranja ranjivosti. Ovaj alat je totalno izmijenio način na koji se provode sigurnosne provjere sustava. Razlog zašto je Metasploit popularan je broj različitih testova koji se mogu provesti u sklopu testiranja ranjivosti sustava, s ciljem poboljšanja sigurnosti. Metasploit je dostupan za sve veće operacijske sustave, te je proces izvođenja testiranja skoro identičan na svima.

Kada je potrebno provesti testiranje velikog broja umreženih sustava koristi se okosnica za testiranje ranjivosti. Automatizacijom procesa testiranja dolazi do brže provedbe te se pruža bolja efikasnost i lakša kontrola nad aktivnostima tijekom testiranja ranjivosti. Korištenjem okosnice za testiranje ranjivosti automatizira se generiranje i spremanje rezultata za lakšu analizu. Okosnica alata Metasploit je platforma otvorenog koda koja pomaže u stvaranju realnih testiranja ranjivosti uz mnoge ostale funkcionalnosti. Zadnje stabilne verzije okosnice su pisane programskim jezikom Ruby. Ova okosnica ima najveću bazu testiranih eksploita i do danas je jedan od najkompleksnijih projekata izrađen programskim jezikom Ruby.

Potrebno je dodatno objasniti pojmove vezane uz testiranje sigurnosti:

- Eksploit (eng. Exploit) – programski kod koji omogućava napadaču ulaz u sustav iskorištavanjem pronađenih ranjivosti. Svaka ranjavost ima svoj odgovarajući eksploit. Metasploit ima preko 700 testiranih eksploita.
- Ranjivost sustava – to je propust koji omogućava napadaču ulaz u sustav. Ovaj propust može postojati u operacijskom sustavu, aplikacijskom softveru te čak u mrežnim protokolima.
- Korisni sadržaj (eng. Payload) – Programski kod koji izvodi napad. Pokreće se u sustavu nakon korištenja eksploita. Koriste se za stvaranje konekcije između napadača i napadnutog sustava. Metasploit ima preko 250 vrsta ovog koda.
- Moduli – Moduli su mali dijelovi koji izgrađuju sustav. Svaki modul izvodi određenu operaciju, dok je cijeli sustav izrađen kombiniranjem više modula koji funkcioniraju kao cjelina. Najveća prednost ovakve arhitekture je lakoća kojom razvojni programeri mogu integrirati nove ekploite i alate u okosnicu Metasploita.

Metasploit koristi različite baze podataka koje su ključne za ispravno funkcioniranje okosnice programa. Ove baze su kolekcije unaprijed definiranih zadataka, operacija i funkcija koje mogu biti korištene od strane različitih modula okosnice programa. Temeljni dio okosnice je baza Ruby Extention (Rex). Neke od komponenti Rex baze uključuju: implementacije protokola klijent server, podsustav zapisnika, klase za implementaciju eksploita i ostale korisne klase. Rex baza je dizajnirana da nema dodatnih poveznica, osim onih koje dolaze zadanom instalacijom programskog jezika Ruby. [12]

Zatim imamo MSF Core bazu koja proširuje Rex bazu. MSF Core je odgovorna za implementaciju svih potrebnih sučelja koja se koriste za interakciju s eksploit modulima, dodacima i sesijama. Ova baza se proširuje bazom okosnice koja je dizajnirana za pružanje jednostavnih rutina za rukovanje s jezgrom okosnice programa, kao i za pružanje korisnih klasa za rukovanje s različitim aspektima okosnice programa. Baza okosnice proširuje se korisničkim sučeljem (UI) koje puža podršku za različite tipove korisničkog sučelja, poput komandne konzole ili web sučelja. [12]

Testiranje ranjivosti uključuje kompletnu analizu sustava implementiranjem stvarnih testova sigurnosti. Razlog koji testiranje ranjivosti čini važnim aspektom sigurnosti je taj da pomaže identificirati prijetnje i ranjivosti s perspektive hakera. Pronađene ranjivosti mogu biti testirane u realnom vremenu u cilju procjene šteta koja bi nastala iskorištavanjem propusta. Ovime se omogućuje izrada zakrpe ranjivosti u svrhu zaštite sustava od vanjskih napada i smanjenja rizika.

Najveći utjecaj na izvedivost testiranja ranjivosti imaju znanje i informacije o ciljanom sustavu. Black box testiranje je naziv za testiranje ranjivosti bez poznavanja prethodnih informacija o sustavu. Testiranje mora početi od prvog koraka izrade plana i sakupljanja informacija o ciljanom sustava, da bi moglo doći do implementacije napada na isti. U slučaju White box testiranja poznata je većina informacija o sustavu i testiranje mora potvrditi postojanje pronađenih ranjivosti. Razlog zašto testiranje ranjivosti može potrajati više dana ili mjeseci je u tome jer se bazira na testiranju i ispravljanju pogrešaka.

6 METODIČKI DIO

U metodičkom dijelu diplomskog rada dotičem se nastavnog programa srednje strukovne škole povezanog sa sadržajem diplomskog rada, te će biti priložena priprema za izvođenje nastave za pripadnu razinu kvalifikacije u skladu s HKO (Hrvatski kvalifikacijski okvir).

Provedena je analiza plana i programa usporedno s Hrvatskim kvalifikacijskim okvirom. U središtu su HKO-a ishodi učenja - dakle, kompetencije koje je osoba stekla učenjem i dokazala nakon postupka učenja. Svakoj kvalifikaciji stečenoj u Republici Hrvatskoj mjesto je određeno prema razini koju imaju skupovi ishoda učenja koji pripadaju toj kvalifikaciji. Smještanje kvalifikacija na određenu razinu omogućuje da se kvalifikacije mogu uspoređivati i povezivati. Pitanje je hoće li učenici usvojiti određenu količinu kompetencija predviđenu za ovu razinu obrazovanja i na kraju obavljati predviđene poslove.

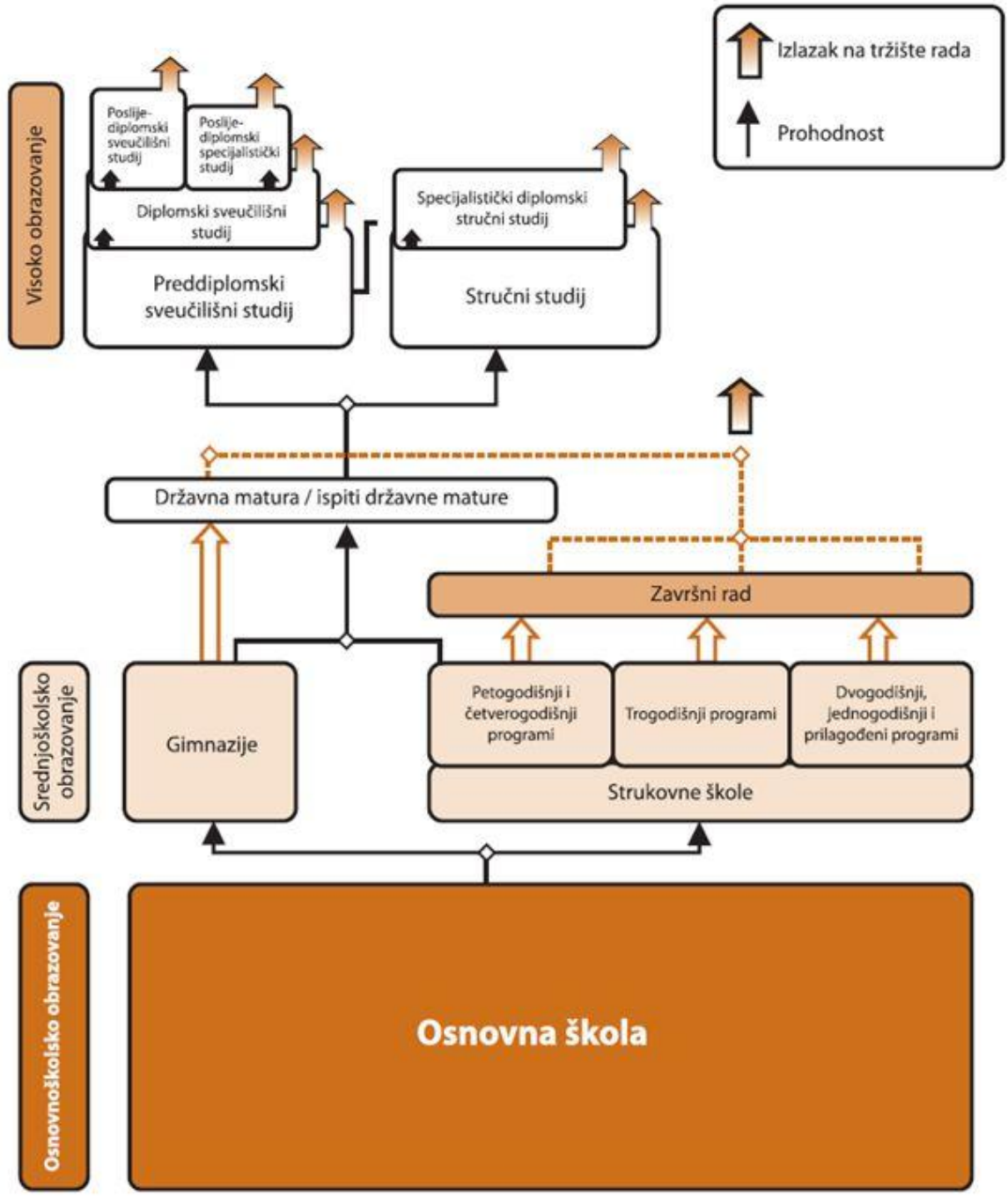
6.1 ANALIZA PROGRAMA SREDNJE STRUKOVNE ŠKOLE

Sustav obrazovanja u Republici Hrvatskoj sastoji se od:

- predškolskog odgoja i obrazovanja
- osnovnog obrazovanja
- srednjeg obrazovanja
- visokog obrazovanja
- obrazovanja odraslih

Ovisno o vrsti nastavnog plana i programa koji provode, srednje škole dijele se na gimnazije, strukovne škole i umjetničke škole. U gimnazijama se izvodi općeobrazovni nastavni plan i program u četverogodišnjem trajanju, a obrazovanje završava obveznim polaganjem državne mature. U strukovnim i umjetničkim školama (glazbenim, plesnim, likovnim) izvodi se nastavni plan i program/kurikulum u trajanju do pet godina, a završetkom obrazovanja učenik stječe strukovnu kvalifikaciju/zanimanje. Obrazovanje završava izradbom i obranom završnog rada, a ukoliko učenik želi nastaviti obrazovanje na visokoškolskoj instituciji, obvezan je polagati ispite državne mature. [13]

Dakle, nakon srednje strukovne škole, učenici su osposobljeni za određeno zanimanje i mogu se zaposliti u struci. Sljedeća shema prikazuje odgojno-obrazovni sustav u Republici Hrvatskoj prema razinama obrazovanja, dužini trajanja, načinu završetka obrazovanja, kao i mogućnosti zapošljavanja ili nastavka daljnjeg školovanja, vidljivo na slici 6.1.



Slika 6.1 Shema odgojno-obrazovnog sustava u Republici Hrvatskoj [13]

Srednja strukovna škole prema ranije navedenom Hrvatskom kvalifikacijskom okviru spada u četvrtu razinu obrazovanja. Znanja koja na ovoj razini učenici usvajaju tijekom nastavnog procesa su činjenična i teorijska. Vještine koje se usvajaju su uglavnom spoznajne i socijalne. Komunikacija i suradnja u skupini su jedna od bitnih vještina za rad. Ako gledamo kompetencije u užem smislu, učenici će razviti samostalnost u radu rješavanje domaćih zadaća i zadanih programa kao i odgovornost.

Definiran je spektar ishoda učenja prema razinama. Razine se razlikuju po složenosti i opsegu. Niže razine su uključene u višoj razini te ih nije potrebno ponavljati, nego se podrazumijevaju. Mjerljivi pokazatelji razina učenja su prikazani složenošću ovih kompetencija: znanja (činjenična, teorijska), vještine (spoznajne, psihomotoričke, socijalne), te pripadajuća samostalnost i odgovornost.

U odabranom nastavnom planu i programu srednje Obrtničke i tehničke škole Ogulin za zanimanje Tehničar za računalstvo predviđen je nastavni sat o Operativnom sustavu. Smatram da bi bilo potrebno upoznati učenike s OS X sustavom i njegovim značajkama, pošto je OS X nakon Windowsa najviše korišten operativni sustav za osobna računala. Uvođenjem teme „Operativni sustav – OS X“ učenici bi dobili novi pogled na operativni sustav uz pregled glavnih funkcionalnosti OS X sustava, što uključuje njegove sigurnosne mehanizme.

6.2 PRIPREMA ZA IZVOĐENJE NASTAVE U SKLADU S HKO

SVEUČILIŠTE U RIJECI

FILOZOFSKI FAKULTET RIJEKA

ODSJEK ZA POLITEHNIKU

Ime i prezime: **Ivan Stipetić**

P R I P R E M A

Z A I Z V O Đ E NJ E N A S T A V E

Škola: **Obrtnička i tehnička škola Ogulin**

Mjesto: **Ogulin**

Razred: **I.**

Nastavni predmet: **Računalstvo**

Kompleks: **Software**

Metodička (nastavna) jedinica: **Operativni sustav – OS X**

Trajanje nastavnog sata: 1 školski sat (45 minuta)

S A D R Ž A J N I P L A N

Podjela kompleksa na teme (vježbe, operacije)

Redni Broj	Naziv tema u kompleksu	Broj sati	
		teorija	vježbe
1.	Uloga operativnog sustava	1	
2.	Operativni sustav – Windows	1	
3.	Operativni sustav – OS X	1	
4.	Osnovne naredbe operativnog sustava	1	1

Karakter teme (vježbe, operacije) – metodičke jedinice

Informativni karakter – obrada sadržaja je u svrsi općeg obrazovanja o Operativnom sustavu – OS X kako bi se učenici upoznali sa sigurnosnim mehanizmima OS X sustava.

PLAN VOĐENJA ORGANIZACIJE NASTAVNIH PROCESA

Cilj (svrha) obrade metodičke jedinice:

Upoznati učenike sa UNIX arhitekturom te ukazati na sigurnosne mehanizme sustava potrebne za obranu od raznih prijetnji.

Zadatci koje treba ostvariti da bi se cilj postigao:

OBRAZOVNI:

- definirati operativni sustav
- nabrojati slojeve arhitekture sustava
- navesti sigurnosne mehanizme OS X sustava
- objasniti postupak funkcioniranja sandbox sigurnosnog mehanizma

FUNKCIONALNI:

- izraziti strategiju sandbox sigurnosnog mehanizma
- opisati način funkcioniranja sigurnosnog mehanizma potpisivanje programskog koda
- objasniti način primjene Adress Space Layout Randomization funkcionalnosti

ODGOJNI:

- uvidjeti važnost sigurnosti sustava
- razvijanje svijesti o sigurnosti sustava

Organizacija nastavnog rada – artikulacija metodičke jedinice:

Dio sata	Faze rada i sadržaj	Metodičko oblikovanje	Vrijeme (min)
UVODNI DIO	- materijalno tehnička priprema - kronološko ponavljanje sadržaja – operativni sustav - uvođenje u temu (motivacija)	- dijalog s učenicima o operacijskom sustavu - predavanje o povijesnom razvoju operativnog sustava OS X	**10**
GLAVNI DIO	- Arhitektura sustava - Osnove sigurnosti - Potpisivanje programskog koda - Sandboxing - Runtime Protection - Mandatory Acess Controls	- popularno predavanje o arhitekturi sustava - dijalog s učenicima o sigurnosti računala - predavanje o potpisivanju programskog koda - predavanje o Sandboxing-u - predavanje o Runtime Protection - predavanje o Mandatory Acess Controls	**25**
ZAVRŠNI DIO	- zadavanje domaće zadaće - ponavljanje i zaključivanje teme	- ponavljanje kroz dijalog s učenicima o najvažnijim obrađenim sadržajima	**10**

Potrebna nastavna sredstva, pomagala i ostali materijalni uvjeti rada:

- Nastavna pomagala:

- računalo
- LCD projektor
- ploča

- Nastavna sredstva:

- listići s domaćom zadaćom

Korelativne veze metodičke jedinice s ostalim predmetima i područjima:

1. Engleski jezik (nazivi)
2. Povijest (povijesni razvoj)

Metodički oblici koji će se primjenjivati tijekom rada:

- **Uvodni dio**

  - dijalog s učenicima o operativnom sustavu kroz koji učenici iznose svoje znanje
  - popularno predavanje o povijesnom razvoju operativnog sustava tvrtke Apple

- **Glavni dio**

  - popularno predavanje o arhitekturi sustava
  - dijalog s učenicima o sigurnosti računala uz pomoć PowerPoint prezentacije na kojoj su prikazane slike
  - predavanje o potpisivanju programskog koda
  - predavanje o Sandboxing-u
  - predavanje o Runtime Protection-u
  - predavanje o Mandatory Acess Controls

- **Završni dio**

  - letimično provjeravanje obrađenog gradiva u neformalnom dijalogu s učenicima

Izvori za pripremanje nastavnika:

1. Jonathan Levine: Mac OS X and iOS Internals, To the Apple's Core, John Wiley & Sons, Inc., 2013
2. Joe Kissell: Mac Security Bible, Wiley Publishing, Inc; 2010

Izvori za pripremanje učenika:

1. Saša i Slavica Prudkov: Ukrotite Leoparda Mac OS X 10.5, KOMPJUTER BIBLIOTEKA, 2008

TIJEK IZVOĐENJA NASTAVE – NASTAVNI RAD

UVODNI DIO

- Materijalno tehnička priprema

Na početku sata potrebno je pripremiti sva nastavna sredstva i pomagala. Nastavnik priprema računalo te uključuje projektor na kojem će biti prikazana PowerPoint prezentacija, dok učenici brišu ploču ukoliko nije obrisana.

- Kronološko ponavljanje sadržaja – operativni sustav

S obzirom da se učenici kroz svoje školovanje susreću s pojmom operativni sustav, pokrećem dijalog kako bi ih uputio prema temi današnjeg predavanja. Motivacija učenika za nastavni sat se postiže pitanjima, pomoću kojih učenici sudjeluju u raspravi:

- što je operativni sustav?
- koje operativne sustave poznajete?
- na kojim operativnim sustavima ste radili?

- Uvođenje u temu (najava)

Kroz kratko predavanje naglasiti da je u današnjem svijetu mrežno povezanog računalstva sigurnost vrlo bitan aspekt razvoja softvera. Kako bi tvrtka Apple razvila što bolji operativni sustav napravila je niz promjena. Kroz kratak povijesni razvoj prikazati kako se od verzije NeXTSTEP došlo do OS X sustava.

Naziv Mac OS Classic odnosi se na verzije Mac OS-a prije pojavljivanja OS X sustava. Operativni sustav nije bio za pohvalu, jedina posebnost ovog operativnog sustava je njegovo grafičko korisničko sučelje ili GUI (eng. Graphical User Interface). Upravljanje memorijom je bilo loše izvedeno, a multitasking je bio kooperativan, što se po današnjim standardima smatra primitivnim. Iako primitivan ovaj sustav unio je temelje nekih značajki modernog OS X sustava, kao što je Finder GUI, te podrška za sistemske pozive (forks) u prvoj generaciji HFS datotečnog sustava. Ove značajke su bitne za rad modernog OS X sustava.

NeXTSTEP je naziv za objektno orijentirani operativni sustav s podrškom za multitasking, razvijen od strane tvrtke NeXT Computer za njihova računala. NeXTSTEP je donio velike promjene kao što su:

- Bazira se na Mach mikrokernelu. Novost je bila u samom konceptu mikrokernela koji se rijetko implementira i danas.
- Programski jezik korišten pri razvoju je Objective-C, koji je u odnosu na C++ više objektno orijentiran jezik.
- Upravljački programi su mogli sadržavati ostale upravljačke programe, te na taj način proširujući njihovu funkcionalnost.
- Aplikacije i programske biblioteke su bile distribuirane u nezavisnim paketima. Paketi su imali unaprijed određen datotečni sustav, koji je bio korišten za pakiranje softvera zajedno sa povezanim datotekama, te je instaliranje i brisanje aplikacija bilo jednostavno kao micanje obične mape.
- PostScript je bio dosta korišten, uključujući funkciju display postscript koja je omogućavala renderiranje slika kao postscript. Ovo je omogućavalo ispis u formatu 1:1, za razliku od ostalih operativnih sustava koji su morali konvertirati u format pogodan za ispis.

NeXTSTEP sustav unatoč mogućnostima koje je donio nije stekao veliku popularnost, te se danas ne koristi. Tvrtka Apple je 1997 godine kupila tvrtku NeXT Computer, te je zajedno uz kupnju sustava NeXTSTEP ponovno zaposlila vizionara Steve Jobsa. Nasljedstvo NeXTSTEP operativnog sustava nalazi se u današnjem OS X.

Kao rezultat kupnje NeXT-a, Apple je dobio pristup novim tehnologijama poput Mach mikrokernela, programskog jezika Objective-C te ostalim dijelovima NeXTSTEP arhitekture. Nakon preuzimanja prestaje razvoj NeXTSTEP sustava, ali su glavne tehnologije korištene u razvoju OS X. Zapravo OS X možemo nazvati spojem Mac OS Classica i NeXTSTEP-a, većim dijelom potonjeg. Tranzicija Mac OS bila je postupna, uz razvojnu inačicu nazvanu Rhapsody koja nije javno objavljena. Međutim ta razvojna inačica je kroz konstantan razvoj postala prva verzija Max OS X, a njezin kernel je postao osnova za današnji Darwin.

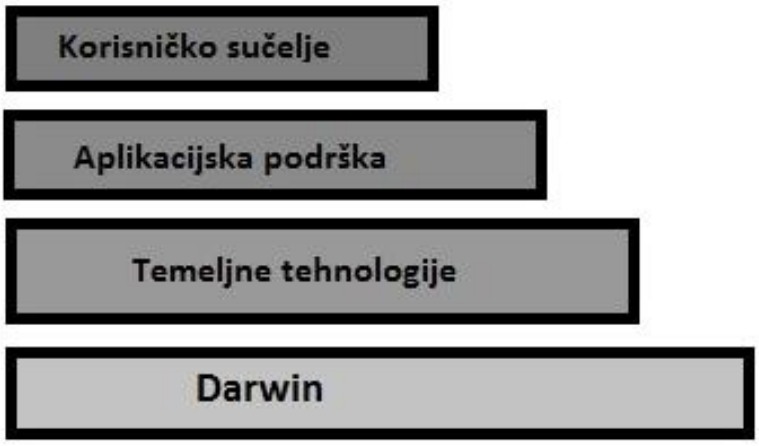
Postoje određene razlike između termina OS X i Darwin, te veze između ova dva termina. Naziv OS X predstavlja ime za cijeli operativni sustav, dok je Darwin samo jedna od mnogih komponenti od kojih se sastoji.

GLAVNI DIO

- Arhitektura sustava

Učenicima objašnjavam arhitekturu sustava. U odnosu na prethodnika OS 9, OS X je potpuno redizajniran, s ciljem da postane jedan od najinovativnijih operativnih sustava. Posebno s novim funkcionalnostima koje donosi u korisničkom sučelju (GUI) i aplikacijskom programskom sučelju (API), koje brzo bivaju prenesene na Windows i Linux platformu.

Nastavnik na ploču zapisuje naslov te učenicima pojašnjava da sve što zapiše na ploču, potrebno je prepisati u bilježnicu. Nakon toga nastavnik na ploču crta dijagram arhitekture sustava te ga učenici precrtavaju u svoje bilježnice:



Slika 1 Dijagram arhitekture OS X operativnog sustava

Nakon crtanja, nastavnik ukratko objašnjava slojeve:

- Sloj korisničkog sučelja: uključuje komponente Aqua, DashBoard, Spotlight i funkcionalnosti pristupačnosti.
- Sloj aplikacijske podrške: uključuje komponente Cocoa, Carbon i Java.
- Sloj temeljnih tehnologija: naziva se još sloj medija i grafike. Sadrži tehnologije Open GL i QuickTime.
- Darwin: jezgra operacijskog sustava — sadrži kernel i UNIX ljusku.

- Osnove sigurnosti

Kroz kratak uvod upoznajem učenike sa osnovom sigurnosti OS X sustava. Apple već dulje reklamira OS X kao sustav gdje su virusi i maliciozan softver rijetka pojava. Ali razlog takvoj situaciji je u prevlasti Windows sustava na stolnim i prijenosnim računalima. Jednostavno objašnjeno, sa stajališta programera malicioznog softvera, želimo li svoje vrijeme i trud uložiti u maliciozan softver koji može napasti 90% računala u svijetu ili samo 5%. S rastom udjela OS X sustava ovo se polako mijenja, te se u novije vrijeme pojavljuju opasniji virusi**.**

U stvarnosti sigurnost OS X i iOS sustava je dosta naprednija od konkurenata. Kontrola korisničkih računa (UAC) koju nalazimo u Windows sustavu prisutna je dosta dugo u OS X sustavu. Određene promjene po pitanju sigurnosti su uvedene s Leopard verzijom, uz uvođenje novih i unapređenje postojećih sigurnosnih značajki sa svakom novom verzijom.

OS X je dizajniran da pruži obranu od raznih sigurnosnih prijetnji kroz obrambene sisteme i pristupe, koji imaju zadaću da identificiraju potencijalne prijetnje i proaktivno štite sustav od tih istih prijetnji.

Navesti ćemo sigurnosne mehanizme za zaštitu povjerljivosti korisničkih i poslovnih podataka. Zapisujem na ploču svaki sigurnosni mehanizam uz objašnjavanje njegovog funkcioniranja i važnosti.

- Potpisivanje programskog koda

Prije nego što se može potvrditi sigurnost određenog softvera, potrebno je potvrditi sigurnost izvora korištenjem certifikata. Softver lako može biti zloćudan ako je preuzet s nepoznate stranice na Internetu. Rizik se lako može umanjiti tako da potvrdimo sigurnost izvora, dodatno kroz potvrdu da softver nije izmijenjen prilikom preuzimanja.

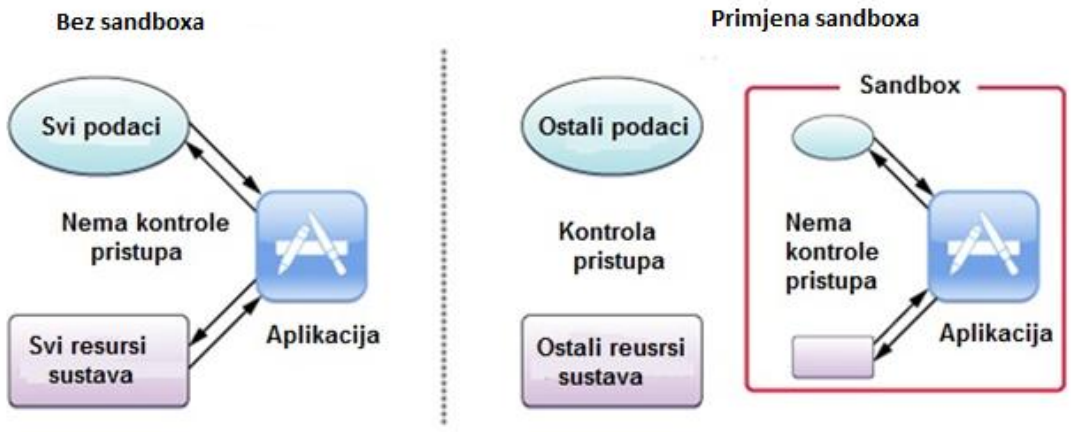
Apple potiče razvojne programere na potpisivanje programskog koda softvera za lakše utvrđivanje njihove identiteta. Jedna od bitnih stvari koda potpisivanja programskog koda je ta, da javni ključ mora biti poznat odobravatelju koda.

Iako potpisane aplikacije mogu sadržavati zloćudan kod, one krše uvjete korištenja te bi ubrzo bile maknute iz Mac App Storea, uz zabranu za razvojnog programera. Ovo je jedan od razloga zašto nalazimo tako mali broj zloćudnih aplikacija u Mac App Storeu.

- Sandboxing

Na početku smatrana zanimljivom funkcionalnosti, kompartmentalizacija ili sandboxing postaje integralan dio OS X i iOS sustava. Ideja je jednostavna, ali je ona važan princip za sigurnost aplikacija. Neprovjerene aplikacije moraju biti pokrenute u posebnom odjeljku, poput karantene u kojoj su sve operacije podložne restrikcijama.

Uz pomoć prezentacije prikazujem učenicima slikovit prikaz sandbox mehanizma u svrhu boljeg razumijevanja.



Slika 2 Primjena sandbox sigurnosnog mehanizma

Strategija sandbox funkcionalnosti:

- Razvojnom programeru omogućava opis interakcije koju aplikacija ima sa sustavom. Sustav zatim dodjeljuje aplikaciji prava da izvrši svoj zadatak i ništa više.
- Korisniku daje pravo da omogući dodatne pristupe alokacijama kroz poznate interakcije i korisničko sučelje

Prednost ovako čvrstog sandboxa je u tome da korisnik može pokrenuti nesigurnu aplikaciju u sandboxu, bez straha da će zlćudni softver učiniti neku štetu podacima ili samom sustavu. Sandbox mehanizam jedan je od boljih sigurnosnih mehanizama u operativnim sustavima, ali to ne podrazumijeva savršenstvo.

- Runtime Protection

OS X primjenjuje brojne hardverske i softverske tehnike za zaštitu operacijskog sustava i aplikacija. Ugrađena direktno u procesor, XD („execute disable“) funkcionalnost pruža zaštitni zid između memorije korištene za podatke i memorije korištene za izvršne instrukcije.

Ovo pruža zaštitu od zloćudnih aplikacija koje pokušavaju prevariti Mac da podatke smatra istovjetnima programu, te na taj način kompromitirajući sustav.

Adress Space Layout Randomization (ASLR) mijenja lokacije u memoriji gdje se spremaju različiti dijelovi aplikacije. Na ovaj način napadaču je teško napraviti štetu koja se događa pronalaskom i promjenom dijelova aplikacije, u namjeri da ona učini nešto van svoje prvotne namjene. Ova obrana djeluje na svim razinama sustava.

- Mandatory Acess Controls

OS X koristi mehanizam za kontrolu pristupa pod nazivom „mandatory access controls“. Iako mehanizam nije vidljiv krajnjem korisniku, on je ugrađen u operativni sustav i to su pravila koja ne mogu biti nadvladana.

Ova pravila postavljaju sigurnosne restrikcije kreirane od strane razvojnog programera. Ovakav pristup je drugačiji u odnosu na diskretnu kontrolu pristupa koja dopušta korisniku promjenu sigurnosnih pravila prema njegovom odabiru.

Iako ovaj mehanizam nije vidljiv korisniku, ovo je važna tehnologija koja omogućuje rad nekoliko funkcionalnosti, uključujući sandboxing, roditeljsku zaštitu i kontrolirane povlastice. Kod sandboxa, mandatory access controls izvode restrikciju pristupa sistemskim resursima, određenu prema posebnom sandbox profilu.

ZAVRŠNI DIO

- zadavanje domaće zadaće

Kako bi učenici kod kuće ponovili što su naučili u školi, zadajem im domaću zadaću. Zadatak je preuzeti CARNET-ov dokument na temu „Sigurnost Mac OS operacijskog sustava“ i pročitati prva četiri poglavlja, te izdvojiti glavne stvari u natuknicama. Dokument je dostupan na poveznici: http://bit.ly/1SjXD5s. Nakon pojašnjenja zadatka dijelim učenicima listiće sa zadatkom te pitam učenike ima li pitanja u vezi zadaće.

- ponavljanje i zaključivanje teme

Za letimično provjeravanje sadržaja postavljam pitanja iz gradiva koje smo upravo obradili te na temelju podignutih ruku učenika koji žele odgovoriti provjeravam obrađeno gradivo. Provjeru provodim postavljanjem slijedećih pitanja:

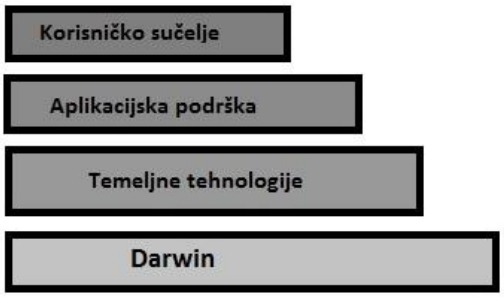
1. Od čega se sastoji arhitektura sustava?
2. Za koje sigurnosne mehanizme ste čuli?
3. Objasnite sandbox sigurnosni mehanizam?
4. Navedite prednost sandbox sigurnosnog mehanizma?
5. Čemu služi Adress Space Layout Randomization funkcionalnost (ASLR)?
6. Pod koji mehanizam spada Adress Space Layout Randomization (ASLR) funkcionalnost ?
7. Pojasnite važnost sigurnosnog mehanizma potpisivanja programskog koda?

Nakon obavljenog letimičnog provjeravanja, učenicima koji su točno odgovorili na dva ili više postavljenih pitanja dajem ocjenu izvrstan iz zalaganja. U slučaju da u razredu nema učenika koji žele odgovoriti na pitanja, nasumično odabirem učenike.

Izgled ploče

Operativni sustav – OS X

Arhitektura sustava:



Sigurnosni mehanizmi:

- Potpisivanje programskog koda
- Sandboxing
- Runtime protection
- Mandatory Acess Controls

Prilog 1. RADNI LISTIĆ1 (domaća zadaća)

DOMAĆA ZADAĆA

ZADATAK:

1. Preuzeti CARNET-ov dokument na temu „Sigurnost Mac OS operacijskog sustava“ i pročitati prva četiri poglavlja, te izdvojiti glavne stvari u natuknicama.

   Dokument je dostupan na poveznici: http://bit.ly/1SjXD5s

6.3 GODIŠNJI OPERATIVNI PLAN I PROGRAM U TEHNIČKIM STRUKOVNIM ŠKOLAMA

OPĆI OSVRT NA PROGRAM NASTAVNOG PLANA

1. CILJEVI I ZADAĆE

Program predmeta računalstvo za srednje elektrotehničke škole izrađen je tako da učenika osposobi za uporabu računala. Težište programa stavljeno je na upoznavanje mogućnosti računala i njegovu učinkovitu uporabu s pomoću aplikacijskih programa u prvom razredu, a u drugom i trećem razredu s pomoću viših programskih jezika. Cilj obrazovanja iz područja računalstva u prvom razredu jest stjecanje osnovnih znanja i vještina uporabe računala do razine rješavanja jednostavnih problema u raznim problemskim situacijama uz uporabu aplikacijskih programa.

Znanje stečeno u ovom predmetu učenici će primjenjivati pri rješavanju praktičnih zadataka u okviru drugih predmeta, naročito u predmetima struke. Primjene trebaju odgovarati stupnju stečenog znanja tijekom školovanja.

2. ORGANIZACIJA NASTAVE

Nastava ovog predmeta izvodi se putem predavanja i vježbi. Teorijsku nastavu (predavanja, ponavljanje) treba izvoditi u namjenskoj učionici. Laboratorijske vježbe izvode se u laboratoriju koji je opremljen prema napucima iz materijalnih uvjeta rada. U nastavi ovog predmeta treba, uz objašnjenje, što više koristiti primjere praktičnih izvedbi putem demonstracijskih metoda rada i samostalnog rada učenika u laboratoriju. Laboratorijski rad učenika i ostali oblici nastave se upotpunjuju i čine jedinstvenu cjelinu. To zahtijeva da nastavu u laboratoriju izvodi isti nastavnik koji izvodi ostale oblike nastave ovog predmeta. Nastava se izvodi prema izvedbenom nastavnom programom, podijeljenim u tematske cjeline koje se obrađuju po tjednima nastave.

3. OBVEZE UČENIKA

Redovit dolazak na sve oblike nastave. Izostanak s vježbi mora se nadoknaditi, jer nastavnik ocjenjuje vježbe učenika. Učenik za izvođenje vježbe treba biti pripremljen putem nastave ili samostalnim radom na temelju razrađenih zadataka za vježbe. Obaveza učenika je imati potreban pribor i udžbenik za sudjelovanje u nastavi.

4. MATERIJALNI UVJETI

Za ostvarivanje zadataka predmeta računalstvo potrebno je osigurati:

- specijaliziranu učionicu s računalima
- kabinet za nastavnika.

Specijalizirana učionica za nastavu računalstva, potrebna je da bi se u njoj izvodila cjelokupna nastava i individualni praktični rad učenika. Učionica mora sadržavati po jedno radno mjesto za svakog učenika.

Oprema radnog mjesta uključuje:

- računalo prema standardima i kriterijima za opremanje škola računalnom opremom
- stol za računalo i prostorom za priručnu dokumentaciju i pisanje i odlaganje medija te potrebnom električnom instalacijom
- anatomski oblikovano sjedalo za učenika

Radno mjesto nastavnika u učionici treba biti opremljeno računalom i LCD projektorom. Prilikom uporabe projektora, nastavnik mora imati mogućnost zamračenja prostorije.

Sva računala u učionici, po mogućnosti, trebaju biti povezana u mrežu. Učionica treba biti opremljena jednim laserskim pisačem i jednim skenerom. Učionica mora imati kompletnu električnu instalaciju s posebnom zaštitnom sklopkom. Osvjetljenje u učionici mora biti izvedeno tako da se ne reflektira od monitora.

Nastavna sredstva za izvođenje nastave računalstva obuhvaćaju i licencirane sistemske i programske pakete.

Prilog 2. Operativni godišnji plan i program

Redni broj sata	Naziv nastavne cjeline i nastavne jedinice	Cilj za nastavnu cjelinu (zadaće za učenike)	Broj sati nastave		Nastavne metode i metodički oblici rada	Korelacijske veze s drugim nastavnim predmetima	Nastavna sredstva i pomagala	Mjesto izvođenja nastavnog sata	Broj radnog tjedna (rok realizacije)	Napomena
			T	V						
0	1	2	3	4	5	6	7	8	9	10
1.	Upoznavanje s nastavnim planom i programom	- predstaviti gradivo i upozoriti na dužnosti i obveze za postizanje uspjeha	1		Nastavne metode: usmeno izlaganje, razgovor s učenicima, metoda demonstracija, rad na tekstu, suradničko učenje, rad na računalu. Metode za razvoj kritičkog mišljenja učenika (RWCT) po ERR sustavu. Metodički oblici rada: frontalni, timski rad, rad u paru, individualni.	- hrvatski jezik - povijest - fizika - matematika - fizika	udžbenik, priručnici, stručni časopisi, radni listići računala, projektor, CD-i, USB stick šk. ploča, kreda, kreda u boji grafoskop, prozirnice	specijalizirana učionica informatike, klasična učionica	rujan ——— listopad ——— studeni	Udžbenik: Grundler, Šutalo: Računalstvo,, udžbenik za 1. i 2. razred četverogodišnjih strukovnih škola, Školska knjiga, 2007.
	INFORMATIKA (1)									
2.	Podatak, informacija, dokument, publikacija	- opisati pojmove podatak, informacija, dokument, publikacija	1							
3.	Informatika - računalstvo	- opisati osnovne pojmove iz područja informatike - računalstva	1							
	POVIJESNI RAZVOJ RAČUNALA (2)									
4,5.	Povijesni razvoj računala	- prikazati kratki povijesni razvoj računala	2							
	OSNOVNA GRAĐA RAČUNALA (15+2)									
6,7.	Temeljna građa računala, CPU	- objasniti funkcionalnu shemu računala (von Neumann), opisati građu i rad procesora	2							
8.	Memorija, U/I sklopovi	- opisati radnu memoriju, sabirnice te U/I sklopove	1							
9.	Vrste računala	- raspraviti vrste računala	1							
10.-12.	Ulazni uređaji	- raspraviti ulazne uređaje	3							
13,14.	Izlazni uređaji	- raspraviti izlazne uređaje	2							
15.	Ponavljanje gradiva	- ponoviti i sistematizirati gradivo	1							
16,17.	**Pismeni ispit br. 1 i analiza pismenog ispita**	- provjera znanja	2							
18,19.	Uređaji za pohranu	- opisati uređaje za pohranu (magnetske i optičke)	2							
20,21.	Uređaji za povezivanje	- opisati uređaje za povezivanje računala	2							
22.	Računalne mreže	- usvojiti pojam i vrste računalnih mreža	1							

0	1	2	3	4	5	6	7	8	9	10
	ZAPIS PODATAKA (6+2)				Nastavne metode: usmeno izlaganje, razgovor s učenicima, metoda demonstracija, rad na tekstu, suradničko učenje, rad na računalu.		udžbenik, priručnici, stručni časopisi, radni listići	specijalizirana učionica informatike, klasična učionica	studeni	Način organizacije nastave: s obzirom na broj učenika u razredu (28) nastava se organizira tako da nastavnik ima 3 sata tjedno nastave rasporedenih tako da je 1 sat tjedno teorijska nastava s cijelim razredom, a za vježbe se učenici dijele u dvije skupine pa nastavnik ima po 1 sat tjedno vježbi sa svakom skupinom.
23.	Dekadski i binarni brojevni sustav	- odrediti dekadski i binarni broj. sustav	0,5	0,5						
24.	Oktalni i heksadekadski brojevni sustav	- odrediti oktalni i heksadekadski broj. sustav	0,5	0,5						
25.	Binarno računanje	- protumačiti binarno zbrajanje i množenje		1		- matematika	računala, projektor, CD-i, USB stick		———	
26.	Bit, byte, ASCII kod	- usvojiti pojmove bit, byte, kod, kodiranje, ASCII kod	1							
27.	Ponavljanje gradiva	- ponoviti, uvježbati i sistematizirati gradivo		1					prosinac	
28,29.	**Pismeni ispit br. 2 i analiza pismenog ispita**	- provjera znanja	1	1			šk. ploča, kreda, kreda u boji		———	
	PROGRAMSKA PODRŠKA (3)				Metode za razvoj kritičkog mišljenja učenika (RWCT) po ERR sustavu					
30.	Podjela programske podrške	- pokazati podjelu programske podrške (sistemski i namjenski)	1				grafoskop, prozirnice			
31.	Operacijski sustavi	- objasniti zadaću operacijskog sustava, pokazati vrste OS	1							
32.	Računalni virusi	- usvojiti pojam rač. virusa, načine prenošenja te zaštitu	1			- biologija				
	OPERACIJSKI SUSTAV MICROSOFT WINDOWS (6+2)				Metodički oblici rada: frontalni, timski rad, rad u paru, individualni.				siječanj	
33.	Operacijski sustav Windows, pokretanje programa	- opisati osnovna obilježja Windows-a, pokazati pokretanje programa		1		- engleski jezik				
34.	Operativni sustav OS X	- sigurnosni mehanizmi OS X sustava	1							
35.	Datoteka, mapa, disk, prečac	- usvojiti pojmove datoteka, mapa, disk, prečac	1						———	
36.-38.	Program za rukovanje mapama i datotekama	- objasniti osn.naredbe za rukovanje mapama i datotekama	1	2					veljača	
39,40.	Ponavljanje, provjera znanja na računalu	- ponoviti i sistematizirati gradivo, provjeriti znanje		2						

0	1	2	3	4	5	6	7	8	9	10
	INTERNET (7+2)				Nastavne		udžbenik,			
41.	Osnovni pojmovi o Internetu	- objasniti osn. pojmove i protumačiti povijest Interneta	1		metode: usmeno		priručnici, stručni			
42.	Usluge Interneta	- upoznati usluge Interneta		1	izlaganje,	- engleski	časopisi,		veljača	
43.	Web preglednik	- pokazati rad s web pregled-nikom (Internet Explorer)		1	razgovor s učenicima,	jezik	radni listići			
44.	Pretraživanje Interneta	- upoznati tražilice, istražiti portale, izvesti pretraživanje		1	metoda demonstracija,	- pretraživanje i diskusije	računala, projektor,			
45.	Pohrana sadržaja s Interneta	- pohraniti pronađene sadržaje		1	rad na tekstu,	povezati sa	CD-i,		_____	
46.	Elektronička pošta	- usvojiti osnovnu ideju elektroničke pošte	1		suradničko učenje,	sadržajima drugih	USB stick			
47.	Webmail (i-Pernica)	-poslati elektroničku poštu putem webmaila (i-Pernica)		1	rad na računalu.	predmeta	šk. ploča, kreda,		ožujak	
48,49.	Ponavljanje, provjera znanja	- ponoviti i sistematizirati gradivo, provjeriti znanje		2			kreda u boji		_____	
	OBRADA TEKSTA (14+2)				Metode za razvoj kritičkog		grafoskop,			
50.	Pokretanje i izgled prozora Worda	- pokazati pokretanje Worda te opisati izgled prozora Worda	1		mišljenja učenika	- oblici referata, eseja	prozirnice			
51.	Pisanje i brisanje teksta	- objasniti pisanje i brisanje		1	(RWCT) po	i plakata iz				
52.	Označavanje i oblikovanje slova	- pokazati označavanje teksta te oblikovanje odlomka		1	ERR sustavu	raznih predmeta,			travanj	
53.	Pohrana i otvaranje dokumenta	- pokazati pohranjivanje i otvaranje dokumenta		1	Metodički	posebno izrada				
54.	Kopiranje i premještanje dijelova teksta	- izvesti kopiranje i premještanje dijelova teksta		1	oblici rada: frontalni,	životopisa i molbi				
55,56.	Oblikovanje odlomka	- pokazati oblikovanje odlomka, uvlake, točkanje i brojčanje te okvire i sjenu		2	timski rad, rad u paru, individualni.	(hrvatski jezik, strani jezik)			_____	
57.	Postava stranice, zaglavlje i podnožje, numeriranje stranica	- pokazati postavke stranice, umetanje zaglavlja i podnožja te numeriranje stranica		1						
58.	Simboli i formule	- pokazati umetanje simbola i pisanje formula		1					svibanj	
59,60.	Rad s tablicama	- pokazati rad s tablicama		2						
61,62.	Umetanje slika i crteža	- primijeniti umetanje slika, gotovih crteža te crtanje		2						
63.	Ispis dokumenta	- izvršiti ispis dokumenta		1						

specijalizirana učionica informatike, klasična učionica

0	1	2	3	4	5	6	7	8	9	10
64,65.	Ponavljanje, provjera znanja na računalu	- ponoviti i sistematizirati gradivo, provjeriti znanje		2	Nastavne metode: usmeno izlaganje, razgovor s učenicima, metoda demonstracija, rad na tekstu, suradničko učenje, rad na računalu. Metode za razvoj kritičkog mišljenja učenika (RWCT) po ERR sustavu Metodički oblici rada: frontalni, timski rad, rad u paru, individualni.	- hrvatski jezik, likovna umjetnost - sva područja ljudskog djelovanja	udžbenik, priručnici, stručni časopisi, radni listići računala, projektor, CD-i, USB stick šk. ploča, kreda, kreda u boji grafoskop, prozirnice	specijalizirana učionica informatike, klasična učionica	lipanj	
	PREZENTACIJE (4+1)									
66.	Osnove rada u Power Pointu	- pokazati osnove rada u Power Pointu	1							
67,68.	Izrada prezentacije	- objasniti postupak izrade prezentacije		2						
69.	Prikaz prezentacije. Animacije	- pokazati prikaz prezentacije te ubacivanje animacija		1						
70.	Zaključivanje ocjena	- zaključiti ocjene	1							
			35	**35**						

7 ZAKLJUČAK

Kroz godine jedan od glavnih razloga za korištenje Mac računala i OS X sustava je bilo korištenje bez velike brige oko sigurnosti operativnog sustava. Većina korisnika odabire OS X sustava radi bolje sigurnosti bez potrebe za poznavanjem naprednih opcija i korištenja raznih sigurnosnih programa. Unatoč boljoj sigurnosti OS X sustava, on je i dalje podložan raznim ranjivostima i propustima isto kao i ostali operativni sustavi. Ovo je i razlog zašto je potrebno provođenje procjene ranjivosti sustava, posebno kada se Mac računala i OS X sustav koriste u poslovnom okružju.

Cilj ovog rada bio je detaljno upoznavanje sa sigurnosti OS X sustava u svrhu provođenja testiranja njegovih sigurnosnih mehanizama. Kroz kratak uvod u povijest OS X upoznali smo se s konstantnim napretkom sigurnosti OS X sustava kroz uvođenje novih funkcionalnosti sa svakom novom inačicom. Većina funkcionalnosti je nova i inovativna pa ubrzo bude ugrađena i ostale operativne sustave. Detaljan opis sigurnosnih mehanizama pruža nam uvid u sigurnosne mogućnosti OS X sustava. S ovim pregledom dobili smo dobar uvod za sljedeći korak testiranja sigurnosti sustava.

Testiranje sigurnosti nam pruža pravi uvid u sigurnost samog sustava. Procjena ranjivosti provodi se u fazama, te dobivamo detaljne informacije o stanju ranjivosti naše inačice OS X sustava koja je korištena za testiranje. Korišten je poznati alat Nessus koji je bogat mogućnostima ali i jednostavan za korištenje. Ovo ga čini odličnim alatom za napredniju procjenu u poslovnom okruženju ali i za procjenu ranjivosti osobnog računala. Odlična mogućnost preporučenih akcija za poboljšanje sigurnosti u našem slučaju riješila bi 96% sigurnosnih propusta. Testiranje ranjivosti sustava proveo sam alatom Metasploit te nam je pružena mogućnost pokretanja dva pronađena eksploita. Pokretanje eksploita nije bilo uspješno, te nije zadobivena mogućnost pristupa OS X sustavu.

Kroz provedena testiranja sigurnosti u ovom diplomskom radu OS X sustav pokazao se kao vrlo siguran operativni sustav. Većina pronađenih ranjivosti može se otkloniti dostupnim sigurnosnim nadogradnjama, dok testiranje ranjivosti nije pokazalo mogućnost njihovog iskorištavanja za dobivanje pristupa samom sustavu. Zaključak je da je OS X siguran od trenutno pronađenih ranjivosti, ali je potrebno konstantno nadograđivanje sustava, jer svakim danom se pronalaze nove ranjivosti koje mogu biti zlonamjerno korištene i uvijek je potrebno biti korak ispred.

8 LITERATURA

[1] Jonathan Levine: Mac OS X and iOS Internals, To the Apple's Core, John Wiley & Sons, Inc., 2013, str. 5-9; 17-18.

[2] OS X Mountain Lion, Wikipedia.

Dostupno 05.04.2015. na https://en.wikipedia.org/wiki/OS_X_Mountain_Lion

[3] OS X Mavericks, Wikipedia.

Dostupno 12.04.2015. na https://en.wikipedia.org/wiki/OS_X_Mavericks

[4] OS X Yosemite, Wikipedia.

Dostupno 13.04.2015. na https://en.wikipedia.org/wiki/OS_X_Yosemite

[5] Utente:Sassospicco, Diagram of Mac OS X architecture, Wikipedia.

Dostupno 14.04.2015 na
https://upload.wikimedia.org/wikipedia/commons/f/f2/Diagram_of_Mac_OS_X_architecture.svg

[6] App Sandbox Design Guide, Mac Developer Library.

Dostupno 27.04.2015 na
https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide

Dostupno 27.04.2015 na
https://developer.apple.com/library/mac/documentation/Security/Conceptual/AppSandboxDesignGuide/Art/about_sandboxing.png

[7] Apple Support, OS X: About Gatekeeper.

Dostupno 13.05.2015.
https://support.apple.com/library/content/dam/edam/applecare/images/en_US/osx/security_preferences_options.png

[8] Apple Technical White Paper, Security for Mac Computers in the Enterprise, Apple Inc., Listopad 2012.

Dostupno 20.04.2015. na http://training.apple.com/pdf/osx_wp_security_108.pdf

[9] Mac OS X Security Configuration, OS X Version 10.6 Snow Leopard, Apple Inc., 2010.

Dostupno 02.05.2015. na https://www.apple.com/support/security/guides/

[10] Joe Kissell: Mac Security Bible, Wiley Publishing, Inc; 2010, str. 636

[11] Himanshu Kumar: Learning Nessus for Penetration Testing, Packt Publishing, 2014, str. 8; 12-13.

[12] Abhinav Singh: Metasploit Penetration Testing Cookbook, Packt Publishing, 2012, str. 7-9.

[13] Shema odgojno-obrazovnog sustava RH.

Dostupno 10.06.2015 na http://public.mzos.hr/

[14] Hrvatski kvalifikacijski okvir.

Dostupno 10.06.2015 na
http://www.hzz.hr/UserDocsImages/Hrvatski_kvalifikacijski_okvir_prirucnik.pdf-