Zahvaljujem mentoru doc.dr.sc Stjepanu Grošu, mag.ing. Bruni Štenglu te mag.ing. Ivanu Kovačeviću na iznimnoj strpljivosti, pristupačnosti te usmjeravanju kroz temu rada te općenito kroz područje informacijske sigurnosti.

Također zahvaljujem ostalim predivnim ljudima na ovom Fakultetu, svojim novim i starim prijateljima te kolegama na druženjima i pruženoj pomoći tijekom studija.

I na kraju, najveću zahvalu dugujem svojoj obitelji, ponajviše ocu, majci i sestri, ali i baki i djedu te svima ostalima na neizmjernoj podršci i strpljenju u ovoj petogodišnjoj avanturi.

Sadržaj

1. Uvod

U posljednjih 20 godina, kibernetički napadi postali su realna prijetnja svakog korisnika Interneta. U nastojanjima da se kibernetički kriminal svede na minimum, došlo je do pojave tvrtki koje se bave kibernetičkom sigurnošću. Te tvrtke pružaju vanjske usluge branjenja informatičkih sustava od napadača te edukacije zaposlenika o tome kako svojim djelovanjem svesti mogućnost napada na minimum.

Međutim, jednom kada se napad dogodi, iskustvo je pokazalo kako je broj zaposlenika koji znaju donijeti pravovremenu odluku vrlo malen. Samim time, unutar svake tvrtke poželjno je održavanje kibernetičkih vježbi koje mogu simulirati uvjete slične onima u slučaju napada. Svrha tih vježbi je uvježbavanje timova zaduženih za obranu kibernetičkih sustava.

Vježbe se provode u dva tima. Crveni tim simulira napadača koji pokušava provaliti u sustav dok plavi tim simulira branitelje koji nastoje umanjiti štetu koja nastaje organizaciji te napadaču onemogućiti dodatne pravce kretanja kroz sustav [1]. Za potrebe vježbi najčešće se koriste virtualizacijske tehnologije ili simulatori. Razlog tome je taj da je korištenje produkcijskih sustava za uvježbavanje napada ili obrane jednostavno prevelik rizik za svaku organizaciju. Umjesto njih, koriste se poligoni izrađeni prema topologijama organizacija koji na što vjerniji način nastoje prikazati sustav koji se koristi u produkciji. Što je poligon detaljniji i vjerniji nekom sustavu, to će vježba biti poučnija i uspješnija. Jednom kada je poligon dovršen, stavlja ga se u simulator u kojem se provodi napad i obrana.

Jedan od takvih simulatora je i *Cyber Conflict Simulator* (CCS), zajednički projekt FER – ovog Zavoda za elektroniku, mikroelektroniku, računalne i inteligentne sustave (ZEMRIS) te tvrtke Utilis d.o.o [2]. U ovom radu bit će opisan jedan takav poligon s kratkim uvodom u rad CCS – a u prvom poglavlju. U drugom poglavlju dan je pregled složenog kibernetičkog poligona za vježbe napada i obrane. Nadalje, u trećem poglavlju opisan je tijek jednog napada te je na kraju, u četvrtom poglavlju, prezentirana skripta kojom je moguće skalirati poligon, ali i utjecati na neke funkcionalnosti s ciljem da se olakša rukovanje velikim topologijama.

2. Osnove *Cyber Conflict Simulatora*

Cyber Conflict Simulator (u nastavku CCS) sastoji se od dva glavna dijela. Prvi dio je *Editor* u kojem se stvaraju novi te uređuju postojeći scenariji. Svaki scenarij sastoji se od minimalno jedne topologije. Topologije prikazuju napadačku, odnosno braniteljsku stranu te se one sastoje od glavnih mrežnih objekata poput računala, usmjerivača (engl. *router*), vatrozida (engl. *firewall*), poslužitelja (engl. *server*), ali i objekata koji mogu predstavljati fizičke osobe. Samim time, topologija može u potpunosti vjerno simulirati kompletne organizacije do u sitne detalje, uključujući i njihove fizičke lokacije. Drugi dio CCS – a je *Simulator* pomoću kojeg se kontrolira simulacija u kojoj može postojati više igrača gdje pritom svaki igrač kontrolira jednu ili više topologija prethodno napravljenih u *Editoru*.

2.1. CCS *Editor* (osnovni elementi u izradi topologije)

Kao što je prethodno spomenuto, *Editor* služi za izradu topologija koje će se kasnije koristiti u simulaciji. U nastavku će biti opisan svojevrsni uvod u izradu topologija u CCS *Editoru*.

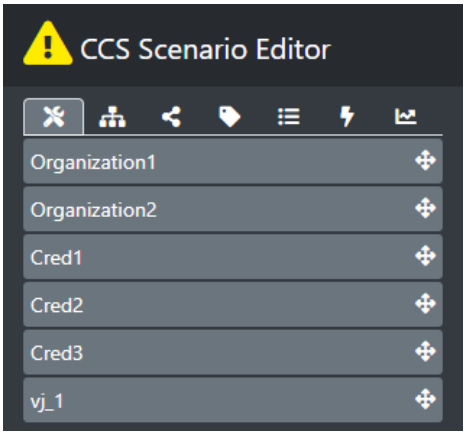
Svaka topologija sastoji se od mnoštva objekata. Svaki objekt sastoji se od mnoštva atributa od kojih su neki zajednički svim objektima dok su neki specifični za svaki objekt. Neki od glavnih zajedničkih atributa su ime, oznaka/e te organizacija. Također, zajednički atribut je i ikona, ali odabir same ikone koja će predstavljati objekt ovisi o korisniku. Dodavanje novih objekata, igrača, oznaka, atributa i slično obavlja se putem alatne trake na vrhu glavnog prozora *Editora* (Slika 2.1). Radi jednostavnosti, koristit će se već postojane oznake i atributi no ukoliko bi korisnik htio napraviti nove oznake ili atribute, to može napraviti trivijalno klikom na gumbove *New label*, odnosno *New Attribute*.

Slika 2.1 Alatna traka na vrhu *Editora*

Na donjoj strani glavnog prozora nalazi se alatna traka s greškama (engl. *errors*) i upozorenjima (engl. *warnings*) (Slika 2.2). Ukoliko postoji greška, simulacija se neće moći pokrenuti, dok će to biti moguće ukoliko postoje samo upozorenja.

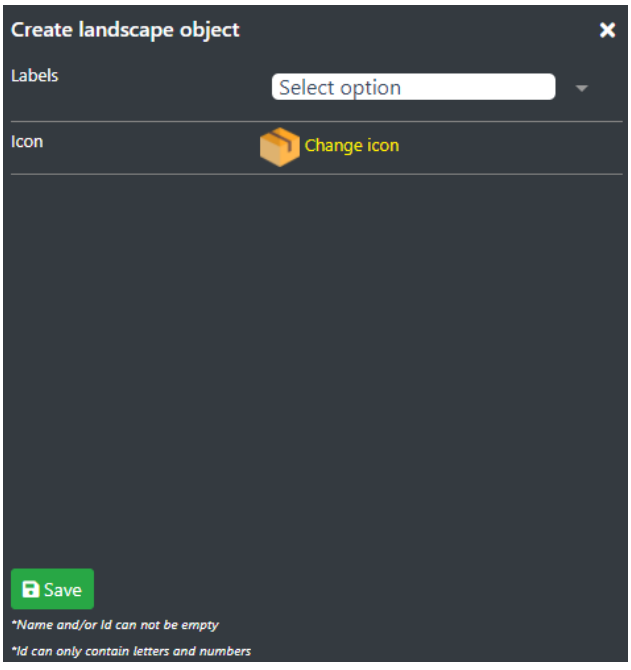
Slika 2.2 Alatna traka s greškama i upozorenjima

S druge strane, popis postojećih objekata, igrača, oznaka itd. dostupan je s lijeve strane glavnog prozora *Editora* (Slika 2.3).



Slika 2.3 Popis postojećih objekata u scenariju

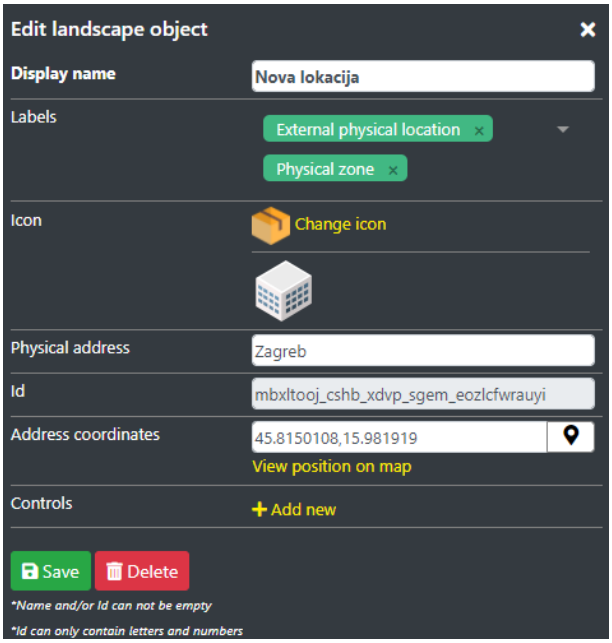
Izrada nove topologije započinje dodavanjem prvog objekta. Klik na gumb *New Item* na gornjoj alatnoj traci otvara početni prozor s desne strane (Slika 2.4).



Slika 2.4 Dodavanje novog objekta

Nadalje, ovisno o odabranoj oznaci (engl. *label*) ili oznakama, otvorit će se prozor s atributima karakterističnim za tu oznaku/e.

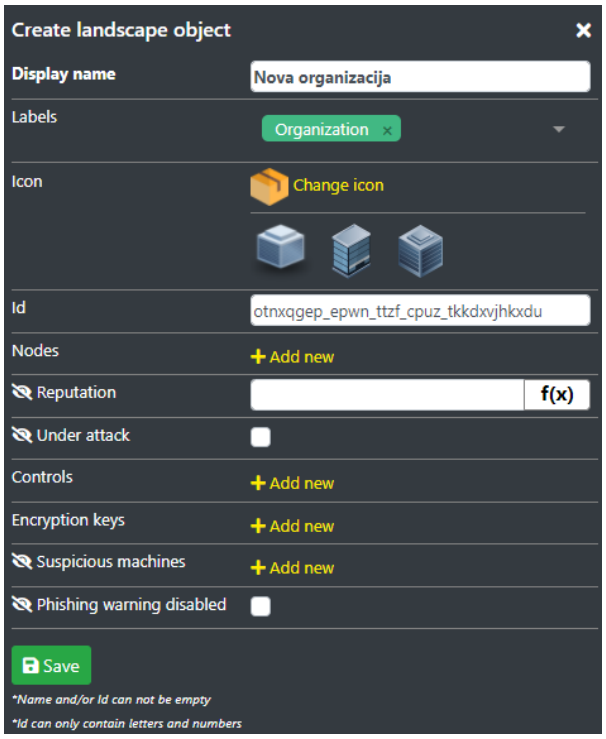
Za početak, recimo da želimo dodati novu fizičku lokaciju na kojoj će naša tvrtka biti smještena. To možemo napraviti odabiranjem oznake *External physical location* (Slika 2.5). Općenito, odabirom neke oznake, uz nju će se odabrati i još neke oznake koje se često koriste zajedno uz odabranu oznaku. U ovom slučaju, dodat će se oznaka *Physical zone*. Akcija odabira oznake automatski otvara prozor i atribute karakteristične za tu kombinaciju oznaka.



Slika 2.5 Dodavanje nove fizičke lokacije

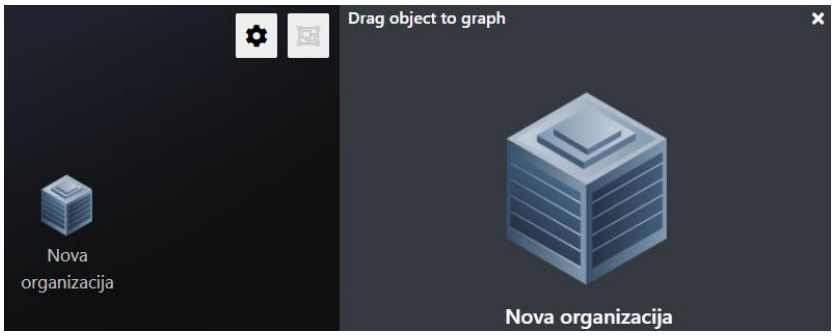
U ovom slučaju, neki od karakterističnih atributa su fizička adresa te koordinate naše fizičke lokacije. Zgodna stvar kod koordinata je ta što nakon unosa adrese, klik na pribadaču automatski generira koordinate na temelju unešene adrese. Klik na *View position on map* vodi nas na *Google karte* gdje je vidljiva unesena adresa, odnosno koordinate lokacije. Nakon popunjavanja željenih atributa (obavezno je popunjavanje onih koji imaju crveni obrub), klik na gumb *Save* stvara novi objekt. *Drag and Drop* objekt koji je moguće dodati u topologiju.

Nadalje, recimo da želimo dodati novu organizaciju u sklopu koje će djelovati naši zaposlenici. To možemo napraviti odabiranjem oznake *Organization* (Slika 2.6). Ta akcija nam automatski otvara prozor i atribute karakteristične za organizaciju.



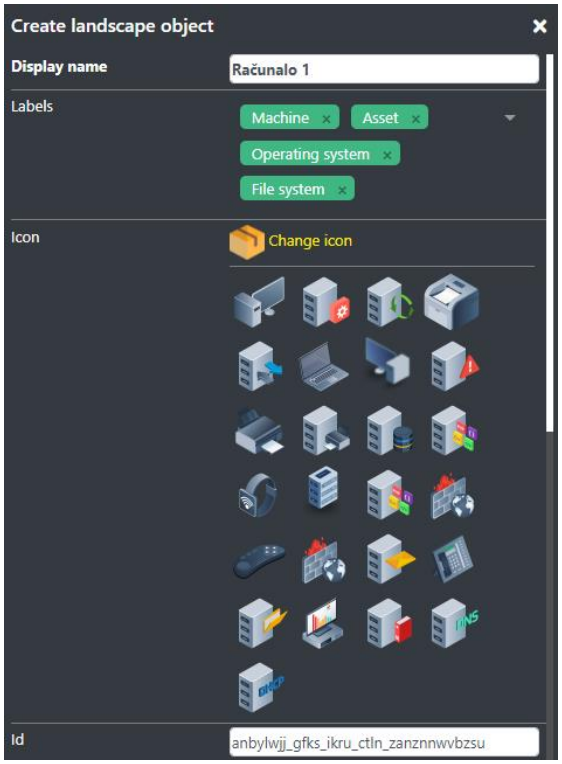
Slika 2.6 Dodavanje nove organizacije

U slučaju „opipljivih“ objekata, klik na gumb *Save* stvara *Drag and Drop* objekt koji je moguće dodati u topologiju (Slika 2.7).



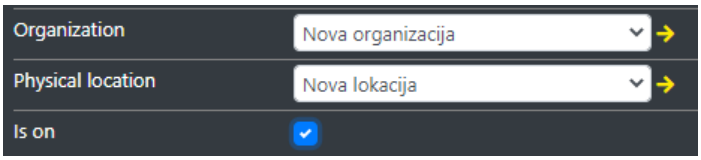
Slika 2.7 *Drag and Drop* objekt organizacije

Iduća kombinacija objekata najčešća u topologijama su računala i fizičke osobe koje rade na njima. Za dodavanje računala, potrebno je upisati oznake *Machine* koja će automatski dodati oznake *Asset* i *Operating system* te *File system* (Slika 2.8). S tim oznakama moguće je dodati mnogo „vrsta“ računala. Kao što je vidljivo po ikonama, tu spadaju ne samo osobna računala već i poslužitelji elektroničke pošte (engl. *e – mail server*), vatrozidi (engl. *firewall*), *DNS* poslužitelji (engl. *DNS server*), pisači itd.

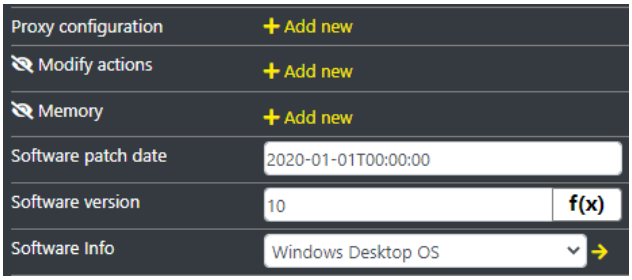


Slika 2.8 Dodavanje novog računala

Ta skupina objekata ima mnoštvo karakterističnih atributa, no najvažniji od njih su *Is on* (Slika 2.9) koji pokazuje je li računalo uključeno, *Machine* što najčešće označava taj isti stroj, odnosno računalo, *Proxy configuration* što omogućuje postavljanje *proxy* poslužitelja (Slika 2.10) te *Software version* i *Software info*, dva atributa vezana uz odabir operacijskog sustava koji će se pokretati na računalu. Isto tako, obzirom da smo prethodno stvorili novu organizaciju te fizičku lokaciju tvrtke, svaku računalo ili osobu moguće je pridružiti željenoj organizaciji, odnosno fizičkoj lokaciji.

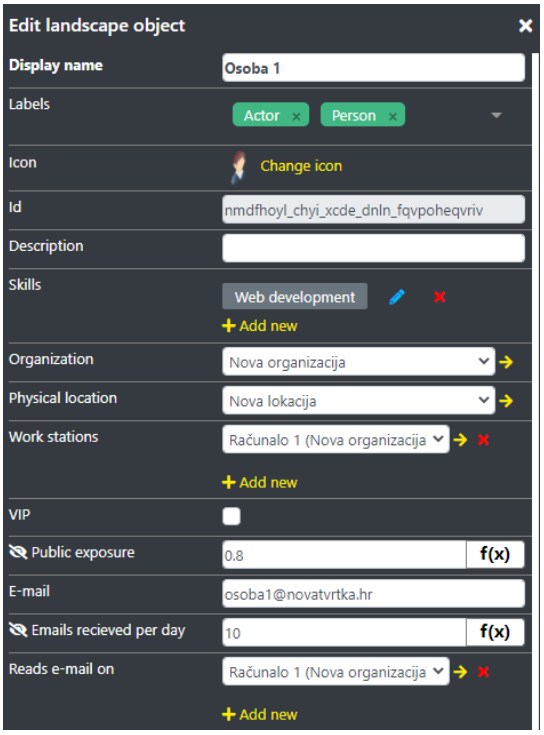


Slika 2.9 Karakteristični atributi računala



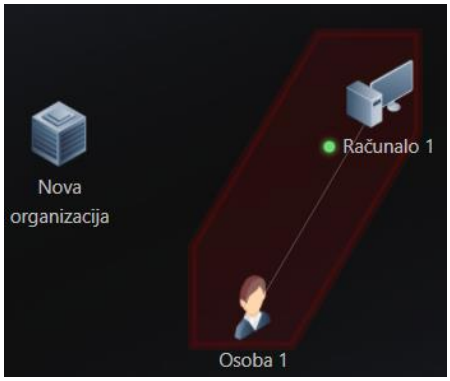
Slika 2.10 Karakteristični atributi računala

Kako bismo dodali fizičku osobu u topologiju, za oznaku je potrebno upisati *Actor* ili *Person* (Slika 2.11). Odabir bilo koje od tih oznaka će automatski odabrati i ovu neodabranu. Što se fizičkih osoba tiče, ključni atributi karakteristični za njih su *Skills* gdje je moguće odabrati vještinu osobe te razinu te vještine (vrijednost između 0 i 1), *Public exposure* što označava koliko je osoba izložena javnosti koja pretražuje Internet (najčešće vrijednost između 0 i 1), *Emails received per day* što predstavlja dnevnu količinu primljenih poruka elektroničke pošte na adresu zadanu također kao atribut te *Work stations* i *Reads e – mail on* koji označavaju računala na kojima ta fizička osoba obavlja posao, odnosno čita elektroničku poštu.



Slika 2.11 Dodavanje nove osobe

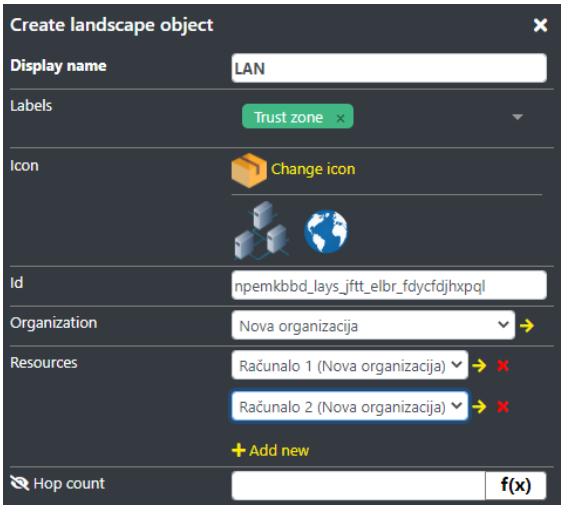
Jednom kada smo u topologiju dodali organizaciju, računalo i osobu, naša trenutna topologija bi trebala izgledati otprilike ovako (Slika 2.12):



Slika 2.12 Izgled osnovne topologije

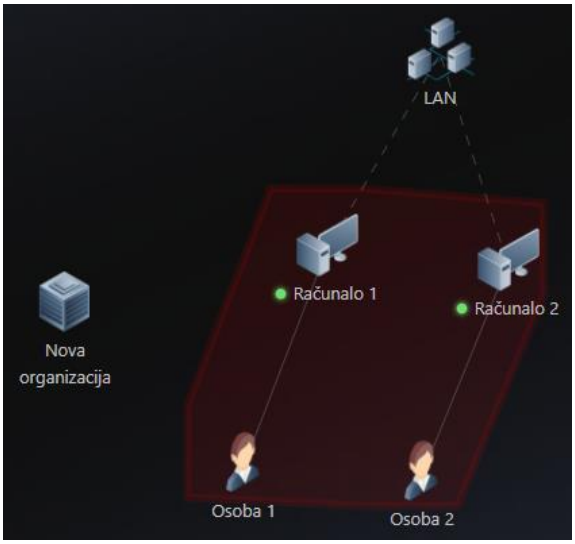
Tamnocrveni obrub oko osobe i računala označava da te osobe pripadaju istoj fizičkoj lokaciji.

Idući element potreban u gotovo svakoj topologiji jest lokalna mreža. To se u CCS – u realizira stvaranjem objekta s oznakom *Trust zone*. Karakterističan atribut za ovu oznaku jest *Resources* (Slika 2.13) koji označava računala koja su povezana s tom mrežom.



Slika 2.13 Dodavanje nove lokalne mreže

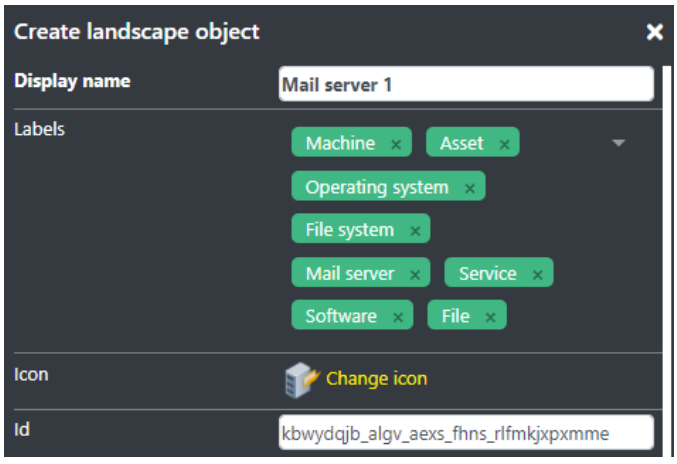
Nakon dodavanja lokalne mreže, topologija izgleda ovako (Slika 2.14):



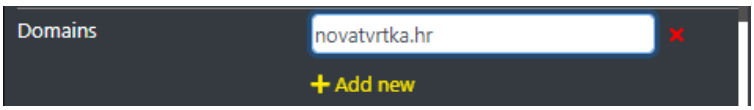
Slika 2.14 Dodavanje lokalne mreže u topologiju

Isprekidane linije koje idu od računala prema lokalnoj mreži označavaju povezanost između tih objekata.

Idući, ujedno i zadnji objekt koji će biti dodan u ovu testnu topologiju jest poslužitelj elektroničke pošte (engl. *e – mail server*). Oznake pridružene poslužitelju elektroničke pošte su identične kao i za osobno računalo (*Asset*, *Machine*, *Operating system* i *File system*) uz dodatak oznaka *File*, *Mail server*, *Service* te *Software* (Slika 2.15). Ključan atribut karakterističan za taj poslužitelj jest *Domains* (Slika 2.16) koji označava za koju domenu će poslužitelj primati poruke.

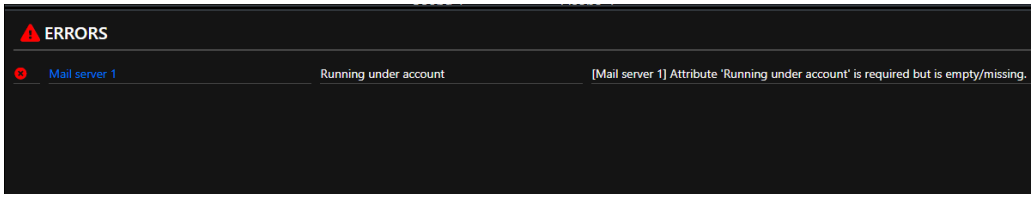


Slika 2.15 Dodavanje novog poslužitelja elektroničke pošte

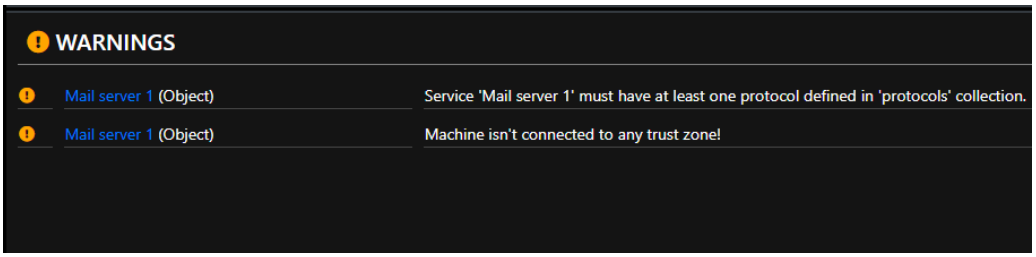


Slika 2.16 Karakteristični atribut poslužitelja elektroničke pošte

Nakon što smo *Mail server 1* dodali u topologiju, vidimo da nam na donjoj alatnoj traci stoji jedna greška (Slika 2.17) te dva upozorenja (Slika 2.18).

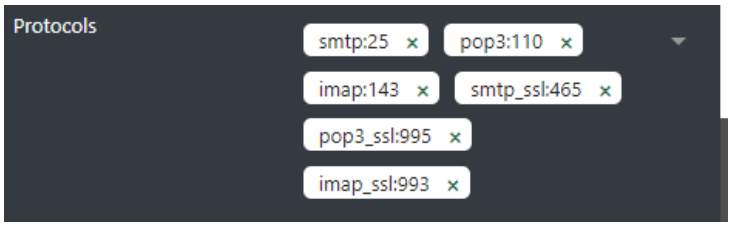


Slika 2.17 Greška vezana uz poslužitelj elektroničke pošte



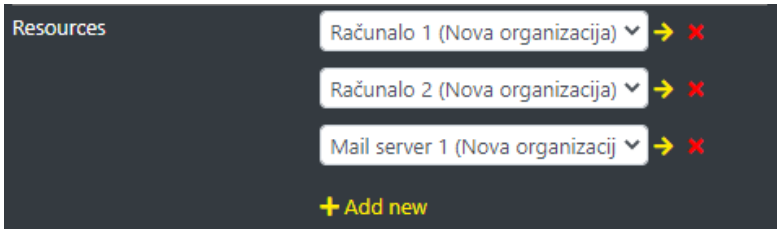
Slika 2.18 Upozorenja vezana uz poslužitelj elektroničke pošte

Greška nam govori kako je potrebno definirati atribut *Running under account* na objektu *Mail server 1*. Taj atribut se najčešće postavlja na *SYSTEM*. Time je greška riješena. Što se upozorenja tiče, prvo upozorenje nam govori da servis *Mail server 1* mora imati definiran bar jedan protokol. Atribut *Protocols* (Slika 2.19) jedan je od zajedničkih atributa svih računala te je njime moguće definirati koji su protokoli, odnosno koja su vrata (eng. *ports*) otvorena na računalu. Što se poslužitelja elektroničke pošte tiče, najčešći protokoli su *SMTP*, *POP3* te *IMAP*, u običnoj i u *SSL*, tj. kriptiranoj verziji.



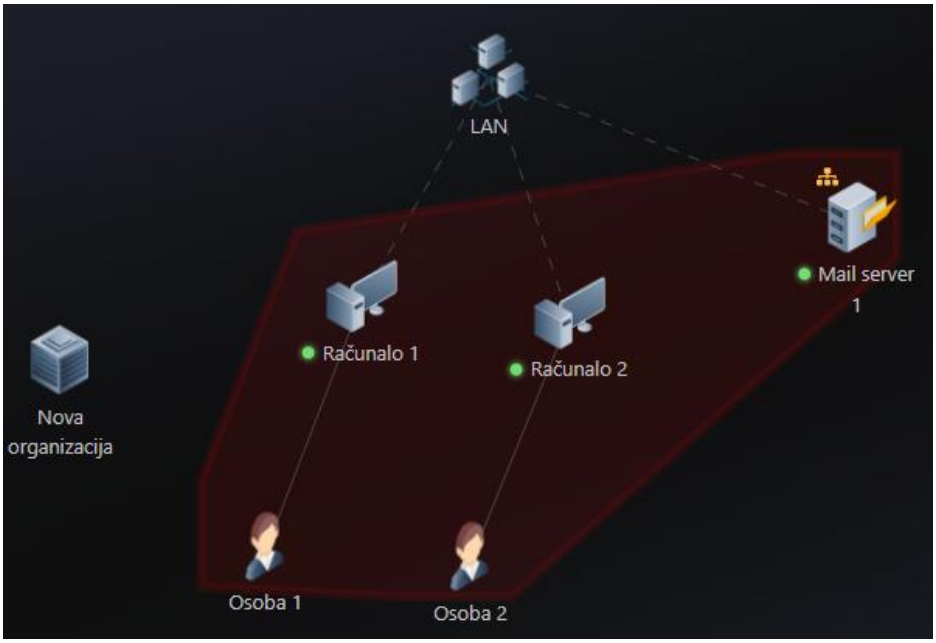
Slika 2.19 Definiranje protokola kod računala

Definiranjem protokola otklonjeno je prvo upozorenje. Što se drugog upozorenja tiče, vidimo kako naš poslužitelj nije povezan na mrežu, odnosno na *LAN* objekt. To ćemo jednostavno napraviti dodavanjem još jednog resursa pod atribut *Resources* objekta *LAN* (Slika 2.20) čime ćemo otkloniti i drugo upozorenje.



Slika 2.20 Dodavanje resursa lokalnoj mreži

Nakon otklanjanja grešaka i upozorenja, naša konačna verzija topologije izgleda ovako (Slika 2.21):



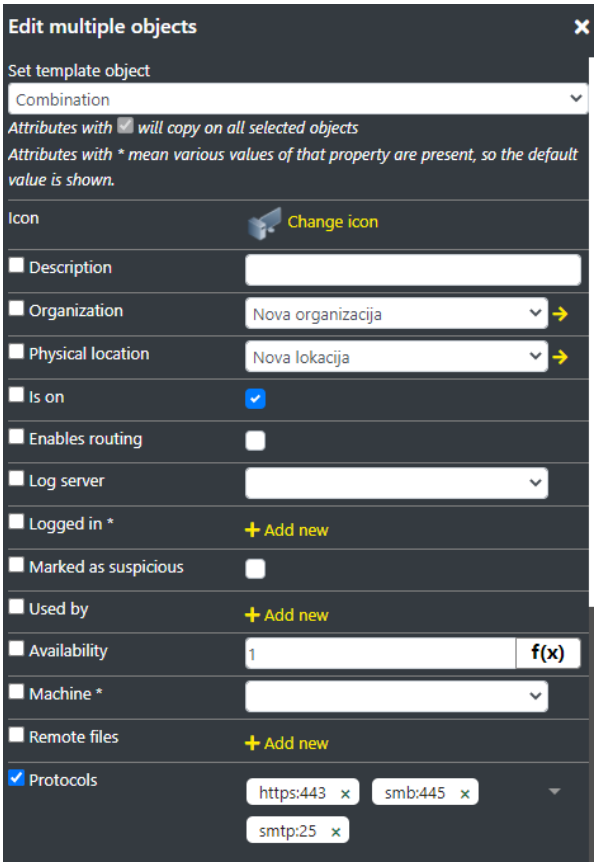
Slika 2.21 Trenutno stanje topologije

Od ostalih stvari koje bi korisniku mogle biti korisne za rukovanje CCS – om vrijedi izdvojiti opciju uređivanja više objekata odjednom koja se aktivira klikom na gumb s gornje desne strane glavnog ekrana, pored gumba za postavke (Slika 2.22).

Slika 2.22 Postavke te opcija uređivanja više objekata odjednom

Za demonstraciju, opcijom uređivanja više objekata dodat ćemo protokole preostalim računalima u topologiji. Prvo je potrebno kliknuti na taj gumb kako bi se aktivirala opcija odabira više objekata. Zatim je potrebno stisnuti na objekte koje želimo uređivati. Nužno je da objekti spadaju pod istu kategoriju, odnosno imaju iste ili slične karakteristike jer inače opcija ne bi imala smisla. Nakon odabira objekata, s desne strane se otvara prozor za

uređivanje svih atributa koje ti objekti dijele (Slika 2.23). Sada dodamo željene protokole pod atribut *Protocols* te pritisnemo *check box* pored imena atributa kako bi se ta promjena primijenila na sve odabrane objekte. Rezultat su isti protokoli definirani i na objektu *Računalo 1* i na objektu *Računalo 2*.



Slika 2.23 Dodavanje istih protokola na više objekata odjednom

3. Opis složenog kibernetičkog poligona za vježbe napada i obrane

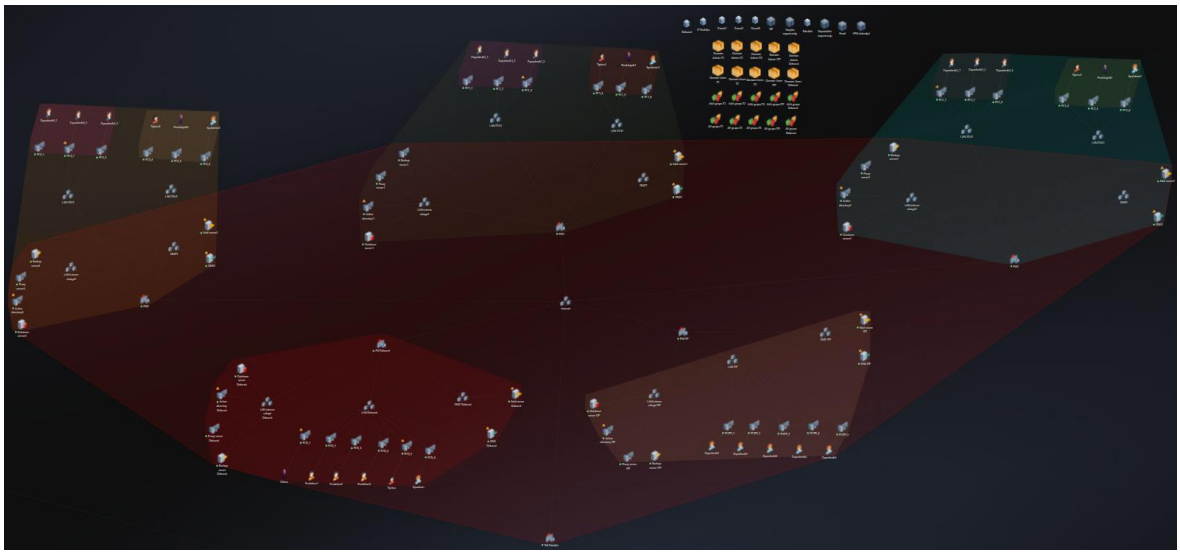
Nakon uvodnog dijela gdje je bila opisana osnovna topologija koja je služila za upoznavanje s CCS – om, u ovom dijelu bit će opisan složeni kibernetički poligon, odnosno topologija koja će služiti za provođenje vježbi napada i obrane. Sama topologija je u potpunosti skalabilna za što je napravljena skripta u programskom jeziku *Python*, ali o tome malo kasnije. Cjelokupni prikaz početnog stanja topologije (prije skaliranja) prikazan je na slici ispod (Slika 3.1), a u nastavku će ona biti opisana dio po dio.

Topologija se sastoji od 2 glavna dijela: braniteljski i napadački. Braniteljski dio predstavlja dio topologije u koju će napadač pokušati upasti. Uz to, postoji i dio topologije koji se odnosi na vanjsku organizaciju koja je tu prvenstveno kako bi doprinijela realnosti simulacije koja će također biti opisana u nastavku. Sve organizacije su preko svojih vatrozida spojene na Internet preko svojeg pružatelja internetskih usluga koji je u ovom slučaju svima zajednički te je nazvan *ISP*. Imena svih objekata u topologiji su generalizirana kako bi se što lakše dodavao proizvoljan broj novih objekata.

Slika 3.1 Kompletan izgled topologije

3.1. Braniteljska topologija

Braniteljska topologija (Slika 3.2) bazirana je na prikazu nekog fakulteta. Samim time, stvoren je objekt *Fakultet* koji predstavlja fizičku lokaciju topologije s adresom negdje u Zagrebu. Nadalje, *Fakultet* je podijeljen za početak na 3 *Zavoda* (svaki *Zavod* je zasebna organizacija) čiji broj je varijabilan i manipulativan pomoću skripte, *Dekanat* te sustav *IT Podrške*. Svaka od tih organizacija preko vatrozida je povezana na *Intranet*, internu mrežu fakulteta koja je zatim preko glavnog vatrozida povezana na *Internet*.



Slika 3.2 Braniteljska topologija

3.1.1. Zavodi

Svaki *Zavod* sastoji se od 2 *Ureda* (Slika 3.3) imena ZavodX_Y gdje X označava broj *Zavoda*, a Y broj *Ureda* unutar *Zavoda* (1 ili 2). Po početnim postavkama, prvi *Ured* sadrži 3 „obična“ zaposlenika (također varijabilno i manipulativno pomoću skripte) imena ZaposlenikX_Y gdje X označava broj *Zavoda*, a Y redni broj zaposlenika unutar *Zavoda* dok drugi *Ured* sadrži predstojnika zavoda, tajnicu te sistemskog administratora. Svaki od njih naravno ima vlastito računalo imena PCX_Y (slijedi prethodno navedenu konvenciju) na kojemu obavlja svoj posao. Oba *Ureda* imaju svoju lokalnu mrežu na koju su povezana računala zaposlenika.

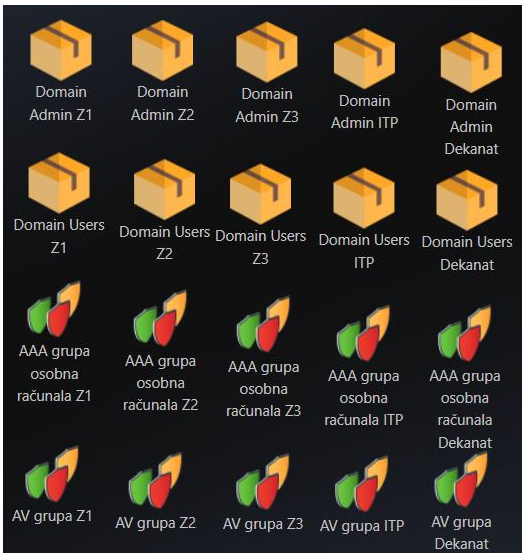
Slika 3.3 Topologija *Ureda* 1 i 2 u sklopu *Zavoda* 1

Osim *Ureda*, u *Zavodu* se nalaze lokalne mreže, demilitarizirane zone te zone internih usluga (Slika 3.4). Unutar demilitarizirane zone nalaze se poslužitelj elektroničke pošte te *DNS* poslužitelj dok su na lokalnu mrežu internih usluga spojeni poslužitelj za pričuvnu kopiju, posrednički poslužitelj, *Active Directory* te poslužitelj baze podataka. Konačno, sve lokalne mreže povezane su na vatrozid koji ima definirana pravila za propuštanje, odnosno nepropuštanje mrežnih paketa izvana/iznutra.

Slika 3.4 Topologija *Zavoda* 1

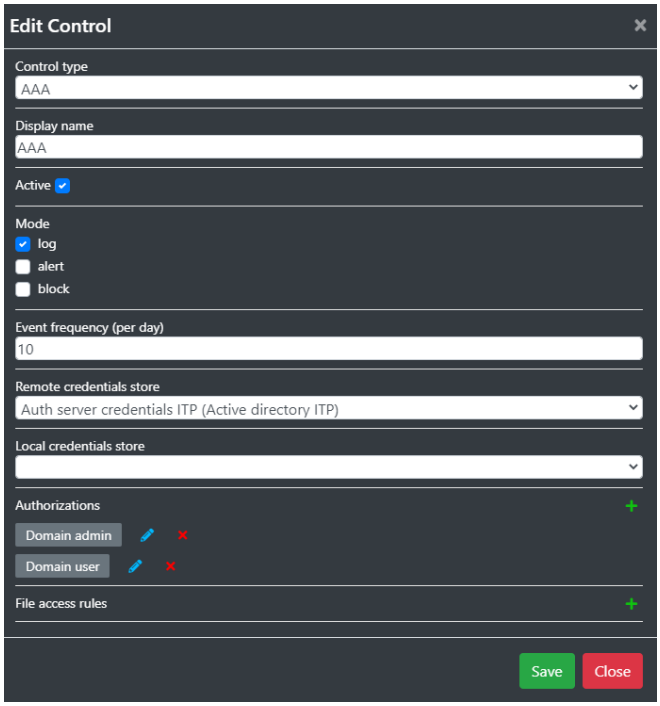
Što se tiče konfiguracije atributa zaposlenika, vrijedi napomenuti kako je *Public exposure* postavljen na 0.3 te da primaju 3 elektroničke poruke na dan. Konfiguracije tajnice, predstojnika i sistemskog administratora se od zaposlenika razlikuju upravo u tim atributima. Tajnici je *Public exposure* postavljen na 0.5, predstojniku na 1, a sistemskom administratoru na 0. S druge strane, tajnica i sistemski administrator dnevno prime 5 elektroničkih poruka dok ih predstojnik primi 10. Također, svaki zaposlenik ima kontrolu *Security awareness* postavljenu na određeni stupanj. Ta kontrola, kao što joj ime kaže, predstavlja svjesnost zaposlenika o sigurnosti što mu primjerice omogućava prijavljivanje primitka potencijalno maliciozne elektroničke pošte. Kod zaposlenika je ta kontrola postavljena na 0.5, što znači da će oni u otprilike pola slučajeva prijaviti sumnjive elektroničke poruke, a u drugoj polovici neće. Tajnici je ta kontrola na 0 što znači da ona nikada neće prijaviti, odnosno prepoznati sumnjive aktivnosti na svojem računalu. Konačno, predstojniku je ta kontrola postavljena na 1, što znači da će on uvijek prijaviti bilo kakvu sumnjivu aktivnost na svojem računalu. Uz to, sistemski administrator ima i postavljen atribut *Skills*, a vještina koju posjeduje je *System administration*.

Što se njihovih računala tiče, sva računala imaju iste konfiguracije. Portovi koji su otvoreni na računalima su 445 (*SMB* protokol) te 3389 (*RDP* protokol), a računala se na mrežu spajaju preko posredničkih poslužitelja koji se nalazi u prethodno spomenutoj lokalnoj mreži internih usluga. Atribut računala koji vrijedi istaknuti jest *Controls* koji je postavljen na *AAA* te *AV*. Obje kontrole su nasljeđene od *AAA* te *AV* grupa koje su definirane posebno za svaki zavod (Slika 3.5).



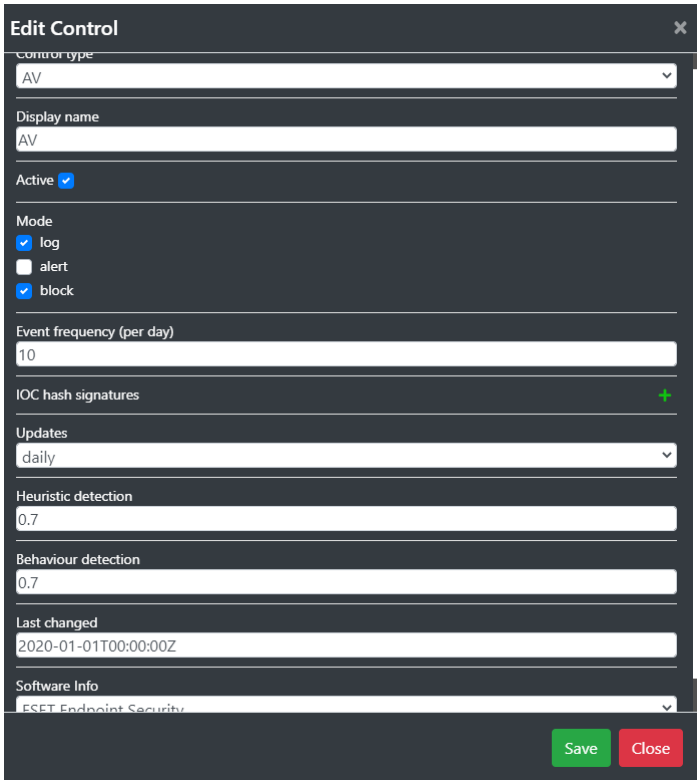
Slika 3.5 Razne grupe korisnika i računala

AAA grupa (Slika 3.6) predstavlja grupu računala koja koriste tzv. *Authentication, Authorization and Accounting* okvir koji prvenstveno služi za kontrolu pristupa. *AAA* kontrola koristi autentifikacijski poslužitelj s vjerodajnicama koji se nalazi na *Active Directory* računalu određenog *Zavoda*. Uz to, svaki zavod ima dvije moguće ovlasti. To su *Domain user* te *Domain admin*. Na svakom *Zavodu* postoji samo i isključivo jedan *Domain admin*, a to je sistemski administrator dok su *Domain useri* svi zaposlenici zavoda osim sistemskog administratora.



Slika 3.6 Konfiguracija *AAA* kontrole

S druge strane, *AV* grupa (Slika 3.7) predstavlja grupu računala koja imaju antivirusni softver ili u ovom slučaju, atribut *Control*. Svaki *Zavod* ima svoju *AV* grupu te su u njoj, kao i u *AAA* grupi, sva računala unutar zavoda osim vatrozida koji se nalazi samo u *AAA* grupi.



Slika 3.7 Konfiguracija *AV* kontrole

Osim *AAA* i *AV* kontrola, jedno, nasumično odabrano računalo zaposlenika unutar zavoda sadrži dokument *OcjeneX*, gdje X označava broj *Zavoda*. Taj dokument predstavlja popis ocjena studenata s njihovim podacima koji inače ne bi trebao biti javan te u ovoj topologiji služi kao meta napadačima. Računalo na kojem se nalazi taj dokument ima atribut *Software Info* postavljen na *Microsoft Office* što će biti bitno kasnije kada se bude provodila simulacija napada.

3.1.2. Dekanat

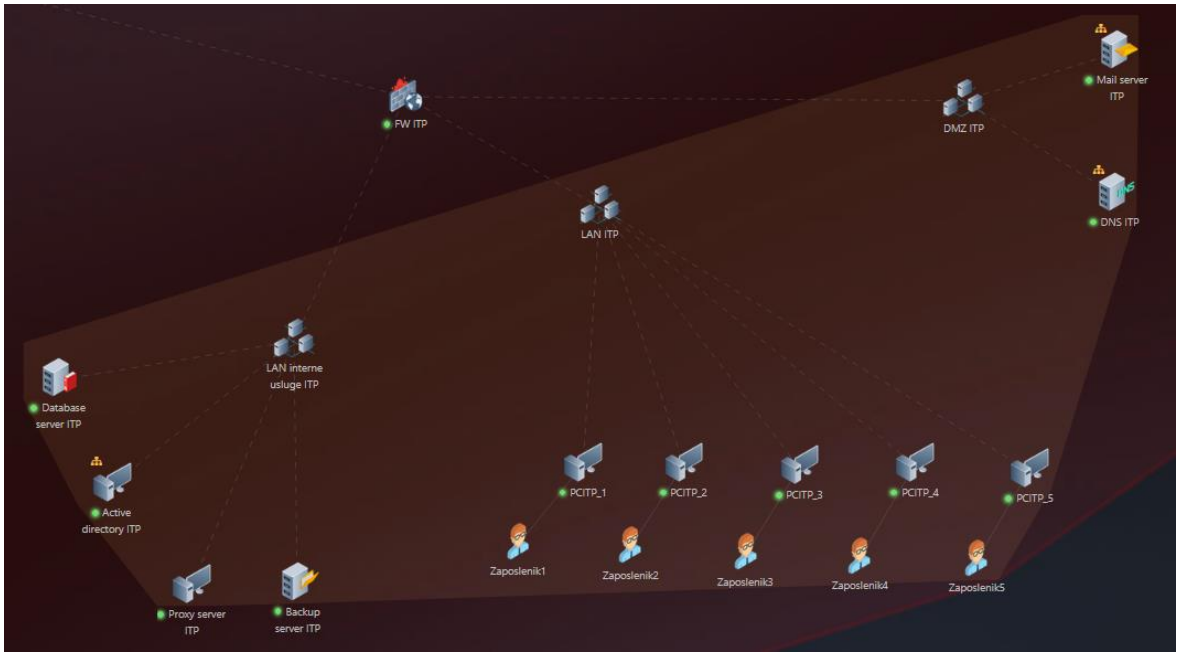
Osim *Zavoda*, u braniteljskoj topologiji nalazi se i *Dekanat*. *Dekanat* (Slika 3.8), kao i ostali uredi, sadrži lokalnu mrežu internih usluga te demilitariziranu zonu s prethodno opisanim objektima te ih stoga ovdje nećemo detaljnije opisivati. Ono što *Dekanat* čini jedinstvenim su zaposlenici koji se nalaze unutar interne mreže. *Dekanat* se sastoji od jednog dekana fakulteta, 3 prodekana, tajnice te sistemskog administratora.

Slika 3.8 Topologija Dekanata

Atributi zaposlenika su uglavnom slični atributima zaposlenika unutar *Zavoda*, osim činjenice da im je atribut *Emails received per day* puno veći. Konkretno, za dekana je on postavljen na 30, za prodekane na 20 dok je za tajnicu i sistemskog administratora postavljen na 15. Svaki od njih radi na svom računalu, a sva računala imaju iste postavke kao i ostatak fakulteta uz iznimke softverskih komponenti. Naime, na računalu dekana nalaze se 2 „fiktivna“ dokumenta: *Popis studenata fakulteta* te *Ugovor o suradnji*. Kao i kod zaposlenika na zavodima, ti dokumenti služe isključivo kao meta napadačima, a njihova imena su tu samo kako bi pridonijela realnosti scenarija. Osim računala dekana, na računalu tajnice se također nalazi dokument imena *Financijski ugovor* čija je svrha identična maloprije opisanim dokumentima na računalu dekana.

3.1.3. IT podrška

U sklopu fakulteta se, osim *Zavoda* i *Dekanata*, nalazi i ured informatičke podrške (Slika 3.9). Uz već prethodno navedene lokalne mreže internih usluga te demilitariziranu zonu, u uredu informatičke podrške se nalazi 5 zaposlenika.

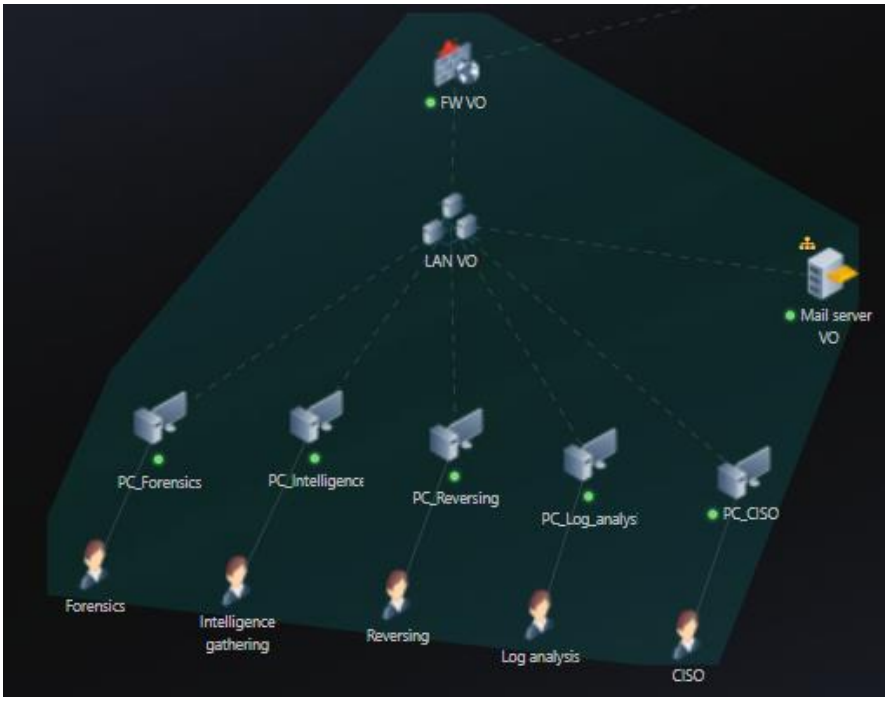


Slika 3.9 Topologija ureda informatičke podrške

Ono što te zaposlenike čini različitima od drugih su njihovi atributi *Skills*. Naime, svaki od zaposlenika ima po jednu vještinu. Te vještine su redom: *Log analysis*, *Backup operator*, *System administration*, *Reversing* te *Business risk analysis*. Uz to, atribut *Emails received per day* svim zaposlenicima je postavljen na 20. Ostale postavke uglavnom se poklapaju s postavkama ostalih dijelova *Fakulteta*.

3.1.4. Vanjska organizacija

Iako nije u sklopu *Fakulteta*, kod opisa braniteljske topologije vrijedi spomenuti i *Vanjsku Organizaciju* (Slika 3.10). To je fiktivna organizacija koja braniteljima „pomaže“ u slučaju nedostatka dostupnih, tehnološki potkovanih zaposlenika. Njen sastav je poprilično jednostavan. Organizacija se sastoji od uobičajenih objekata, odnosno vatrozida i poslužitelja elektroničke pošte te interne mreže u kojoj se nalazi 5 računala te zaposlenici koji rade na njima.

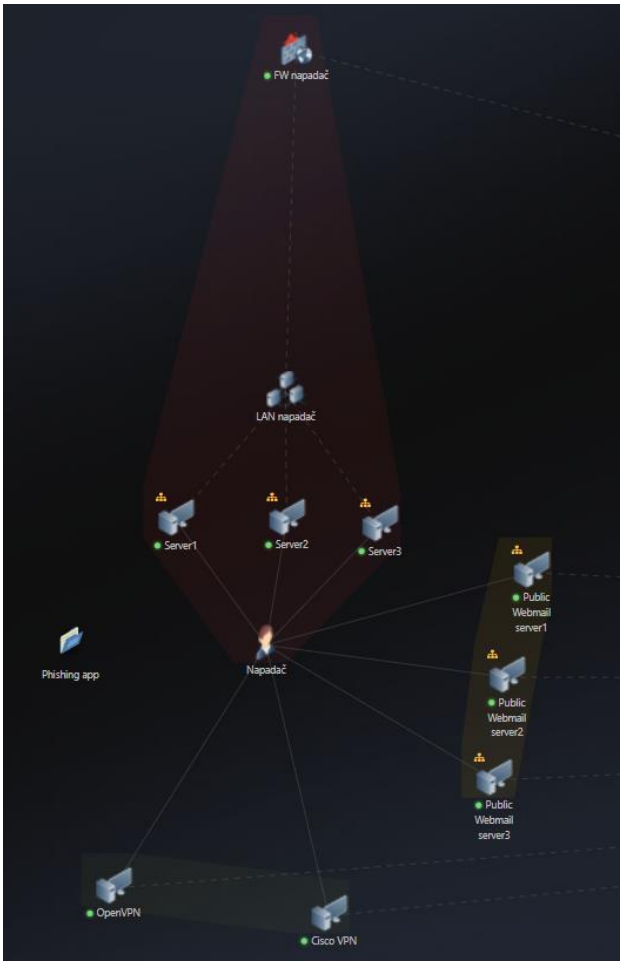


Slika 3.10 Topologija vanjske organizacije

Slično kao i u organizaciji *IT Podrške*, svaki zaposlenik specijaliziran je za jedno područje, s razlikom da su vještine *Vanjske Organizacije* više usmjerene na kibernetičku sigurnost te su vrijednosti tih vještina zaposlenika veće nego one kod zaposlenika *IT Podrške*. Te vještine su redom: *Forensics*, *Intelligence gathering*, *Reversing*, *Log analysis* te *CISO*. Uz to, ono što te zaposlenike čini drugačijima od ostatka jest količina elektroničke pošte koju dnevno prime. Atribut *Emails received per day* kod prva 4 zaposlenika slijeva postavljen je na 20, dok je kod zaposlenika s vještinom *CISO* taj atribut postavljen na 30 obzirom da se tog zaposlenika smatra glavnim u *Vanjskoj Organizaciji*.

3.2. Napadačka topologija

Nakon opisa obrambenog dijela topologije, slijedi pregled napadačke topologije (Slika 3.11). *Napadačka organizacija* sastoji se od napadača koji kontrolira više računala. Među njima su 3 poslužitelja na kojima se nalaze razne datoteke s metodama iskorištavanja za *Windows* i *Linux*, zloćudni programi te servisi, tri javna *webmail* poslužitelja koji se nalaze u *Email* organizaciji, po jedan za FER, PMF i FFZG te dva *VPN* poslužitelja koji su u nadležnosti organizacije *VPN dobavljač*.



Slika 3.11 Napadačka topologija

Na prvom poslužitelju unutar *Napadačke organizacije* nalazi se jedna datoteka s metodama iskorištavanja za *Linux*, 4 datoteke s metodama iskorištavanja za *Windows*, 1 zlćudni program te aplikacija za *phishing*. Struktura svih datoteka s metodama iskorištavanja je više-manje jednaka. Ključni atributi svake od njih su *Labels* koji je postavljen na *Exploit* te *File*, *Exploit Type* koji je postavljen na *Remote*, *Remote privileges* koji je u većini slučajeva postavljen na *user* te *Enables functionalities* koji je postavljen na *Remote access*. Što se zlćudnog programa tiče, atribut *Labels* postavljen je na *File*, *Malware* te *Software*. Nadalje, funkcionalnosti koje zlćudni program ima su *Ransomware*, *Keylogging*, *Remote access* te *Network scanning*. One su su atributom *Functionalities*.

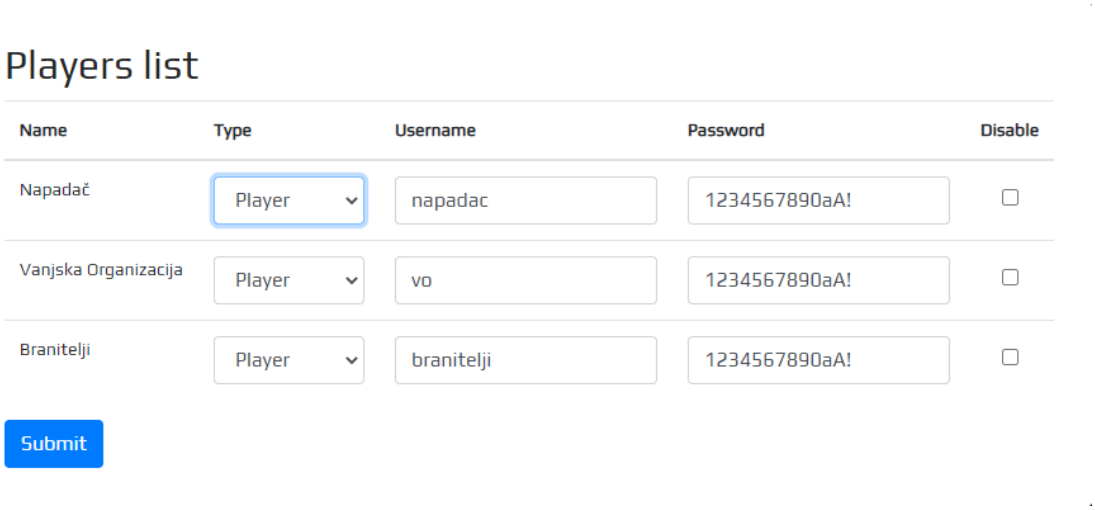
I konačno, na prvom napadačevom poslužitelju *Server1* nalazi se i *phishing* aplikacija koja od važnijih atributa ima atribut *Link* postavljen na fiktivnu stranicu za prijavu u sklopu Sveučilišta u Zagrebu. Uz sve to, prvi napadačev poslužitelj ujedno služi kao *command and control* poslužitelj (*C&C*/*C2* poslužitelj). Takvi poslužitelji obično služe napadaču za

komunikaciju s kompromitiranim računalima [3], a njegova uloga će detaljnije biti opisana u trećem poglavlju pri opisu napada u sklopu simulacije.

Drugi napadačev poslužitelj *Server2* u mreži sadrži iste datoteka s metodama iskorištavanja, ali ne sadrži niti jedan program. Također, jedini servis koji sadrži jest softver za napadačevu elektroničku poštu. Što se tiče trećeg napadačevog poslužitelja *Server3*, on sadrži samo datoteke s metodama iskorištavanja koje su identične onima na poslužiteljima *Server1* i *Server2*.

4. Demonstracija simulacije napada na poligonu

Za provođenje simulacije napada unutar CCS – a, potrebno je prvo otići u *Simulator* klikom na gumb *Go to Simulator* u gornjem desnom kutu početne stranice *Editora*. Nakon ulaska u *Simulator* i odabira željenog scenarija, otvara se izbornik u kojem je moguć pregled igrača koji će sudjelovati u simulaciji (Slika 4.1). Vrijedi podsjetiti da su ti igrači definirani ranije, u *Editoru*, pri izradi topologije. Svaki igrač, uz svoje korisničko ime i lozinku pomoću kojih će se prijaviti u simulaciju, ima i tip koji može biti *Admin*, *Spectator*, *Player* ili *AI*. Za potrebe ove simulacije svi igrači biti će tipa *Player*.



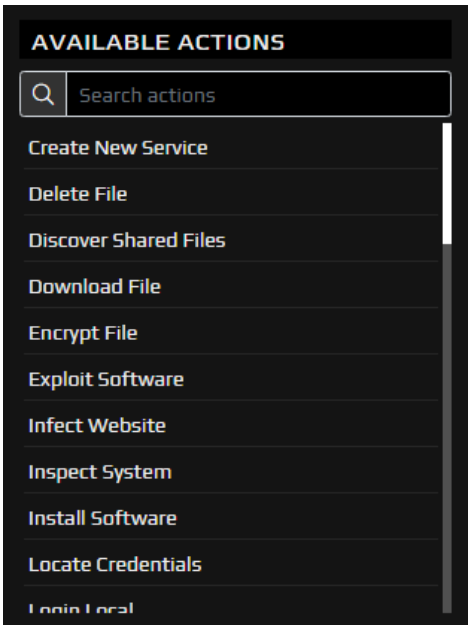
Slika 4.1 Popis igrača u simulaciji

Klikom na gumb *Submit*, otvara se glavni, administratorski prozor za kontroliranje simulacije (Slika 4.2). Iz tog prozora moguće je kontrolirati početak, kraj i brzinu simulacije. Također, iz tog prozora korisnik vidi topologije svih igrača, njihove „poteze“ unutar simulacije te sve dokumente i obavijesti koje igrači dobivaju tijekom simulacije kao posljedice njihovih akcija. Uz to, nakon što administrator odabere ekran pojedinog igrača, istom je moguće poslati pomoć u obliku teksta klikom na gumb *Send hint* u gornjem lijevom uglu.

Slika 4.2 Izgled glavnog administratorskog prozora

Nakon što se svi igrači prijave koristeći istu poveznicu (u ovom slučaju *https://ccsdemo05.utilis.biz*) i administrator klikne na zeleni gumb *Play*, simulacija može početi.

Sve dostupne akcije unutar simulacije igračima stoje na raspolaganju s lijeve strane, pod labelom *Available actions* (Slika 4.3). One akcije koje nije moguće izvršiti jer nisu zadovoljeni svi preduvjeti za izvođenje, nalaze se na dnu padajućeg izbornika, ispod akcija koje je odmah moguće izvesti.



Slika 4.3 Popis dostupnih akcija

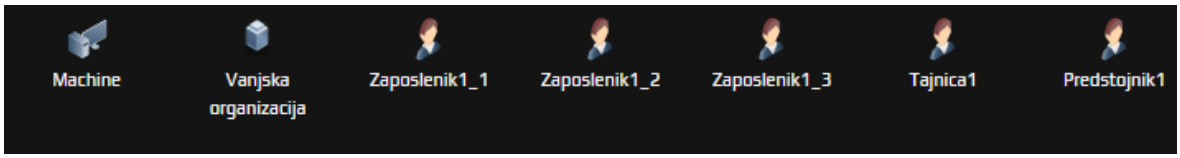
Što se napadačke strane tiče, normalan slijed napada počinje s izviđanjem mete (engl. *recon*). Unutar CCS *Simulatora*, to je moguće napraviti odabirom akcije *Recon*. Klikom na akciju otvara se izbornik (Slika 4.4) u kojem igrač bira dostupnu osobu unutar topologije koja može izvršiti zadanu akciju te metu akcije.

Slika 4.4 Akcija izviđanja mete

Klikom na gumb *Do action*, akcija postaje vidljiva ispod, pod labelom *Actions* (Slika 4.5) te se izvršava u stvarnom vremenu (engl. *in real time*). Izvršavanje akcije moguće je ubrzati ubrzavanjem čitave simulacije. Ta opcija dostupna je administratoru, ali i svakom od igrača.

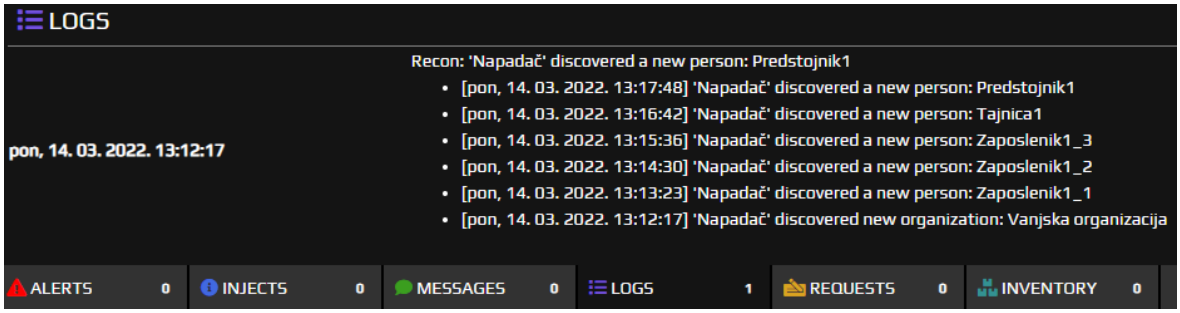
Slika 4.5 Izvođenje akcije u stvarnom vremenu

Po završetku izvođenja akcije, napadač na glavnom ekranu dobiva informacije o skeniranoj meti, u ovom slučaju *Zavoda1* (Slika 4.6).



Slika 4.6 Novootkriveni objekti unutar topologije mete, u ovom slučaju topologije branitelja

Uz to, na dnu ekrana, pod *Logs*, napadač, ali i administrator simulacije, dobivaju detaljne informacije o rezultatima izvedene akcije (Slika 4.7).



Slika 4.7 Informacije o izvedenim akcijama

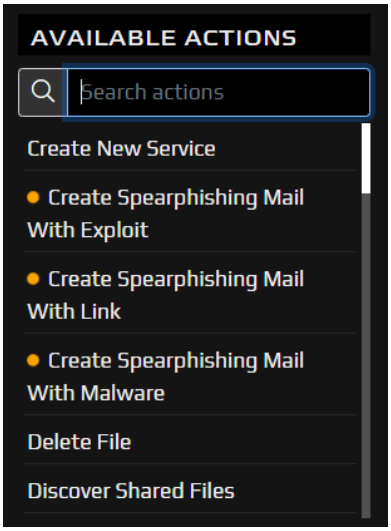
Nakon izvršavanja još 2 operacije *Recona*, po jednu za svaki od preostalih *Zavoda*, napadač otkriva sve *DNS* poslužitelje, organizaciju *Vanjska organizacija* te sve zaposlenike zavoda osim sistemskih administratora. Tome je krivac atribut *Public exposure* koji je kod sistemskih administratora postavljen na 0, dok je kod ostalih vrijednost tog atributa veća od 0. Otkrivene objekte, u ovom slučaju zaposlenike i računala, napadač može dodati u svoju topologiju kako bi vidio odnose među njima, primjerice pripadnost organizaciji, ali i neke od njihovih atributa (Slika 4.8).

Slika 4.8 Osnovne informacije o novootkrivenim osobama unutar braniteljske topologije

Jednom kada je napadač otkrio neke od zaposlenika *Fakulteta* te identificirao mete napada, može prijeći na iduću stavku, a to je detaljno istraživanje pojedinih zaposlenika kako bi došao do još više informacija o njima poput adrese elektroničke pošte koju kasnije može iskoristiti za slanje *phishing* elektroničkih poruka i/ili zloćudnih programa. Istraživanje pojedinih zaposlenika radi se na isti način kao i prvotno istraživanje – pomoću akcije *Recon* koju se ovaj puta, umjesto na *Zavode*, primjenjuje na zaposlenike. Nakon obavljanja akcije *Recon* nad zaposlenicima *Zavoda*, napadač dolazi do novih informacija o njima, među kojima su i njihove adrese elektroničke pošte (Slika 4.9).

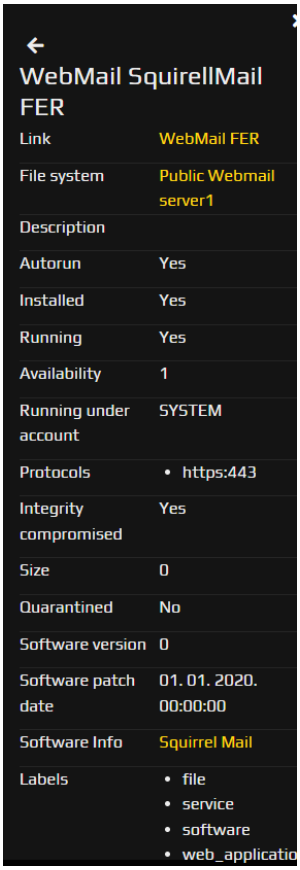
Slika 4.9 Detaljne informacije o novootkrivenim osobama unutar braniteljske topologije

S tom informacijom, napadač se može okrenuti sastavljanju malicioznih datoteka koje će potom elektroničkom poštom poslati zaposlenicima u nadi da će netko od njih kliknuti na privitke poruka te tako aktivirati napadačev zlćudni program ili datoteku s metodama iskorištavanja. Prvi korak jest izrada tzv. *spearphishing* elektroničke poruke za željene zaposlenike. Razlika između *phishing* i *spearphishing* elektroničke poruke je ta što se *spearphishing* elektronička poruka šalje ciljanoj osobi za razliku od *phishing* elektroničke poruke koji je jednak za više meta [4]. Za potrebe demonstracije ovog napada, napravit ćemo 3 vrste elektroničke poruke (Slika 4.10): jedan s poveznicom koja vodi na lažnu stranicu fakulteta za prijavu koju kontrolira napadač, drugi s datotekom s metodom iskorištavanja za *Microsoft Office* aplikaciju za koju će napadač pretpostaviti da se nalazi na žrtvinom računalu obzirom da je to jedan od najčešćih paketa na računalima i treći sa zlćudnim programom koji će, ukoliko žrtva otvori elektroničku poruku, zaraziti njeno računalo te poslati signal (engl. *beacon*) napadačevom *command and control* poslužitelju. Akcije koje omogućuju stvaranje takvih elektroničkih poruka su *Create Spearphishing Mail With Exploit*, *Create Spearphishing Mail With Link* te *Create Spearphishing Mail With Malware*.

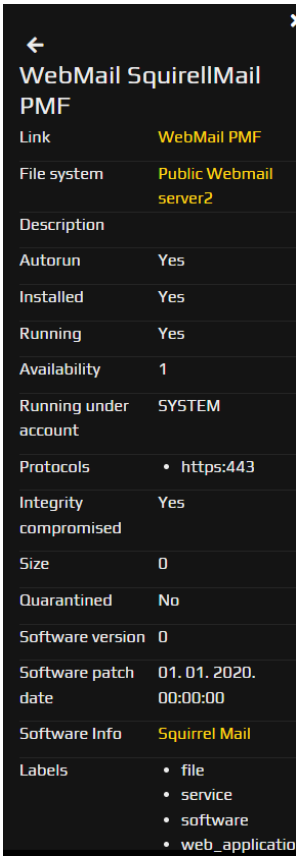


Slika 4.10 Označene 3 različite akcije stvaranja zloćudnih elektroničkih poruka

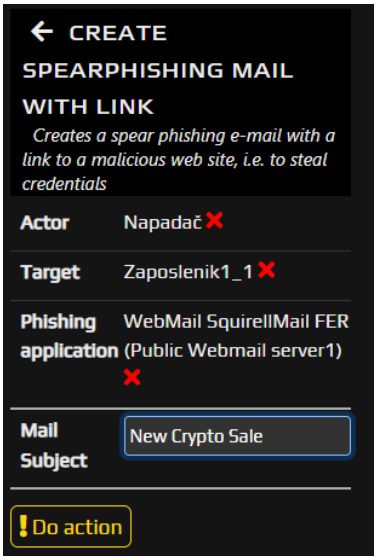
Konfiguracija prve vrste elektroničke poruke vidljiva je u nastavku te će ta elektronička poruka biti poslana zaposlenicima *Zaposlenik1_1* (Slika 4.11, Slika 4.13) te *Zaposlenik1_2* (Slika 4.12, Slika 4.14).



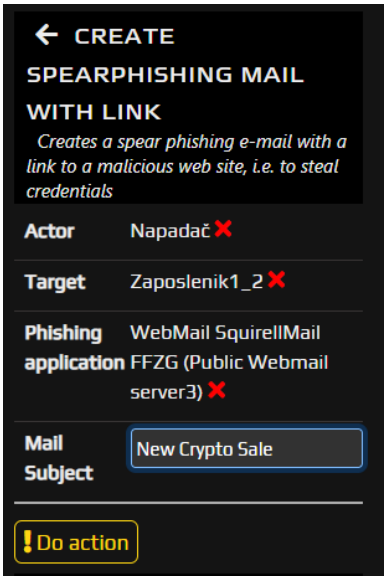
Slika 4.11 Konfiguracija prve zloćudne elektroničke poruke s poveznicom



Slika 4.12 Konfiguracija druge zloćudne elektroničke poruke s poveznicom

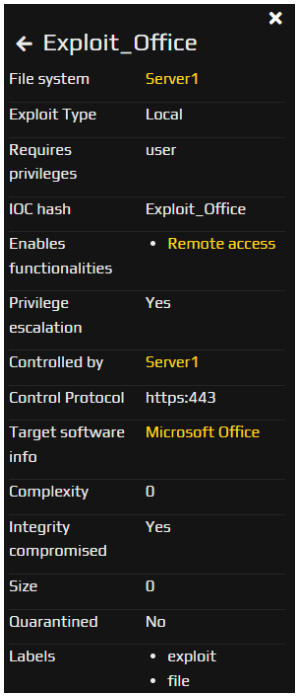


Slika 4.13 Akcija stvaranja prve zloćudne elektroničke poruke s poveznicom

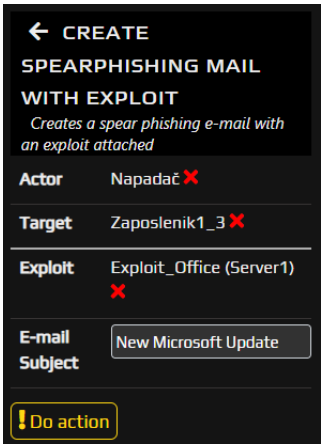


Slika 4.14 Akcija stvaranja druge zloćudne elektroničke poruke s poveznicom

Konfiguracija druge vrste elektroničke poruke također je vidljiva u nastavku, a ta elektronička poruka bit će poslana zaposleniku *Zaposlenik1_3* (Slika 4.15, Slika 4.16).

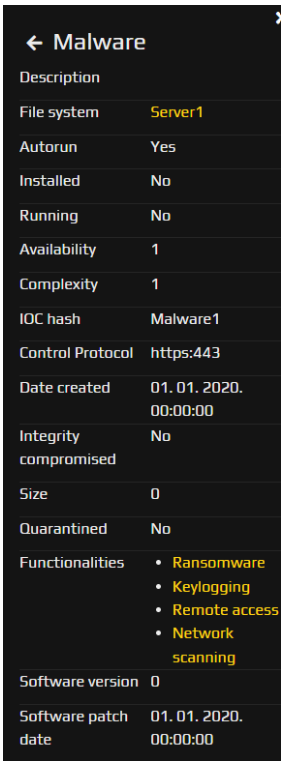


Slika 4.15 Konfiguracija zloćudne elektroničke poruke s datotekom s metodom iskorištavanja

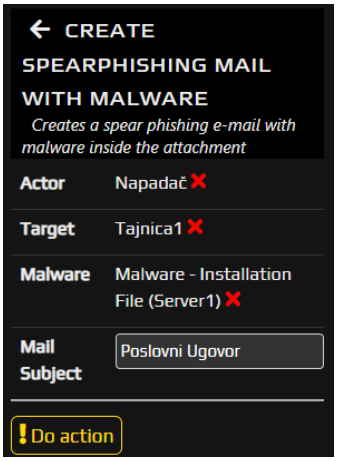


Slika 4.16 Akcija stvaranja elektroničke poruke s datotekom s metodom iskorištavanja

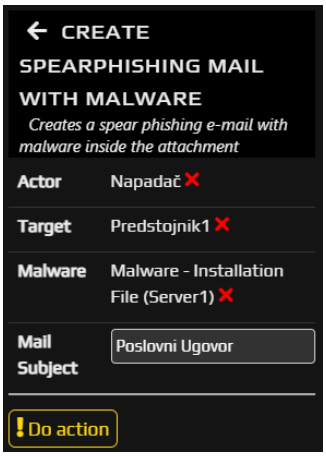
Konfiguracija treće vrste elektroničke poruke prikazana je na idućoj slici (Slika 4.17) te će ta elektronička poruka biti poslana tajnici prvog *Zavoda – Tajnica1* (Slika 4.18) te predstojniku prvog *Zavoda – Predstojnik1* (Slika 4.19).



Slika 4.17 Konfiguracija zlćudne elektroničke poruke sa zlćudnim programom

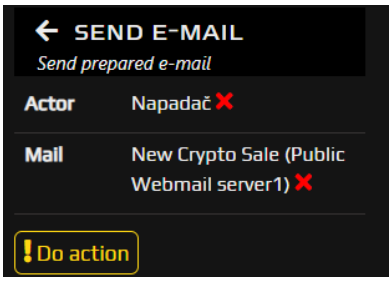


Slika 4.18 Akcija stvaranja prve elektroničke poruke sa zlćudnim programom



Slika 4.19 Akcija stvaranja druge elektroničke poruke sa zlćudnim programom

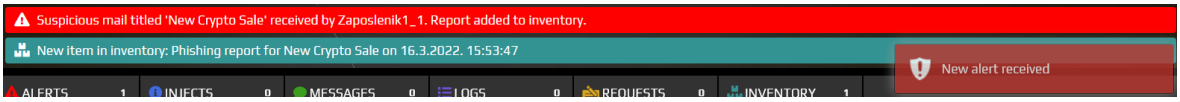
Nakon što su elektroničke poruke konfigurirane, odabirom akcije *Send E-mail* (Slika 4.20) prvo ćemo poslati prvu elektroničku poruku, onu s poveznicom.



Slika 4.20 Akcija slanja prve zlćudne elektroničke poruke s poveznicom

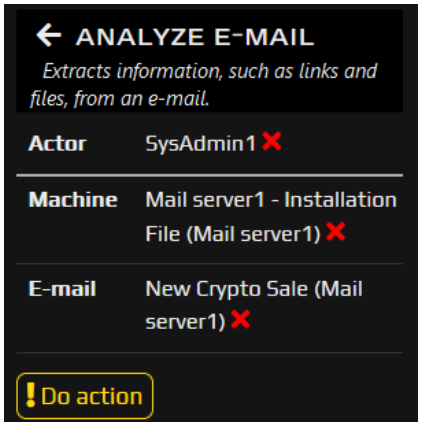
Nakon slanja prve elektroničke poruke, branitelji u svojem prozoru dobivaju obavijest kako su zaprimljeni potencijalno opasne elektroničke poruke te kako se one nalaze na poslužitelju *Mail server1* (Slika 4.21). To se desilo zato što se dogodio slučaj kada zaposlenici odluče prijaviti sumnjive aktivnosti na svojim računalima. Podsjetimo se da je

njihova kontrola *Security awareness* postavljena na 0.5 te bi oni, barem hipotetski, u pola slučajeva trebali prijaviti sve sumnjive aktivnosti, a u pola slučajeva ne.



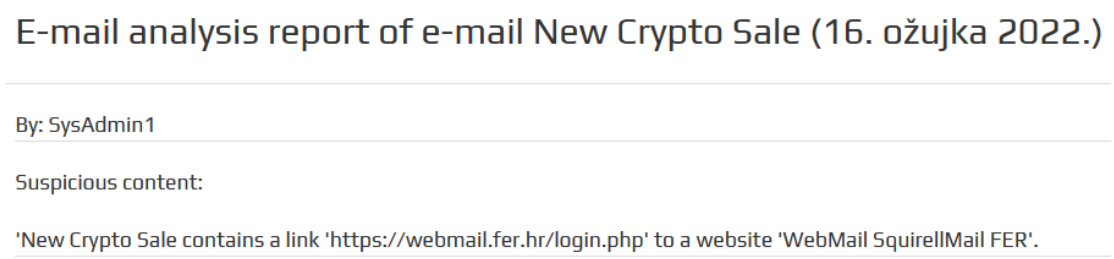
Slika 4.21 Obavijesti, odnosno upozorenja o primitku sumnjive elektroničke poruke

Akcijom *Analyze E-mail* (Slika 4.22) možemo analizirati te elektroničke poruke te vidjeti što se u njima točno nalazi.



Slika 4.22 Akcija analiziranja sumnjive elektroničke poruke

Nakon što analiza završi, pod *Inventory* dobivamo izvješće u kojem vidimo da se unutar elektroničke poruke nalazi sumnjiva poveznica (Slika 4.23).



Slika 4.23 Rezultat analize sumnjive elektroničke poruke s poveznicom

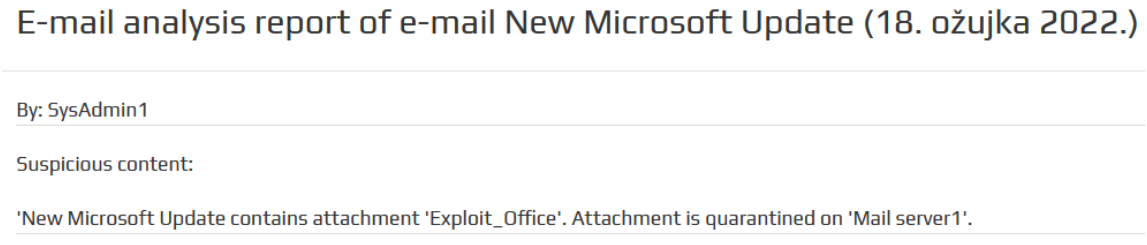
Kako bi sistemski administrator bio siguran da nitko nije „nasjeo“ na *spearphishing* elektroničku poruku, akcijom *Analyze Website Visits* (Slika 4.24) provjerava je li itko posjetio poveznicu navedenu u sumnjivoj elektroničkoj poruci u protekla 3 dana.

Slika 4.24 Akcija analiziranja posjećivanja sumnjive poveznice

Izvješće o obavljenoj akciji mu daje do znanja kako nitko od osoblja nije pristupio sumnjivoj poveznici (Slika 4.25).

Slika 4.25 Rezultat analize posjećivanja sumnjive poveznice

Nedugo nakon slanja prve dvije elektroničke poruke, napadač šalje i elektroničku poruku drugog tipa u kojem se nalazi datoteka s metodom iskorištavanja. Ta elektronička poruka se po primitku također analizira na braniteljskoj strani na isti način kao i prethodne dvije elektroničke poruke, ali je izvješće ovaj puta drugačije; ono upozorava na to da elektronička poruka sadrži datoteku s metodom iskorištavanja (Slika 4.26).



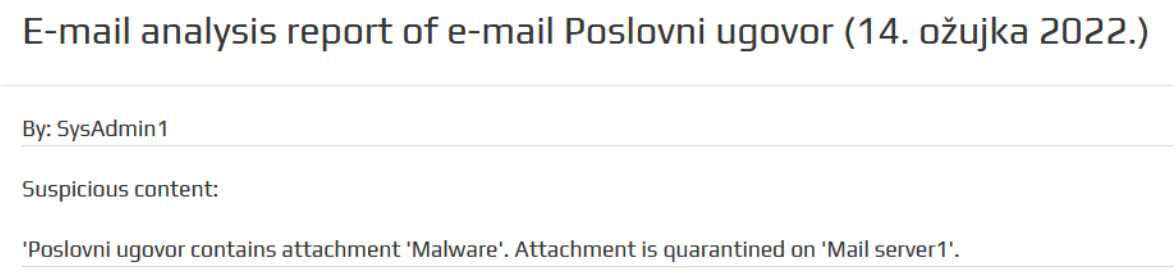
Slika 4.26 Rezultat analize sumnjive elektroničke poruke s datotekom s metodom iskorištavanja

Obzirom da se radi o datoteci s metodom iskorištavanja, braniteljska strana bi mogla odlučiti obaviti reverzni inženjering nad njom. To se postiže akcijom *Perform Reversing*

(Slika 4.27) te je može izvršiti samo osoba s vještinom *Reversing* unutar svog atributa *Skills*. U ovom slučaju, osoba ovlaštena za tu akciju je jedino *Zaposlenik4* unutar ureda *IT Podrške*.

Slika 4.27 Akcija reverzanja datoteke s metodom iskorištavanja

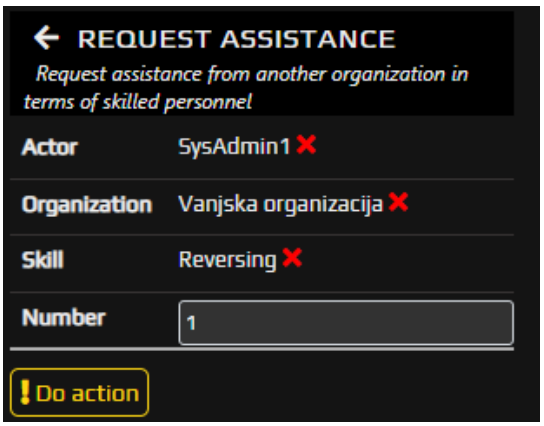
Dok se odvija akcija reverzanja, napadač šalje i preostale dvije elektroničke poruke treće vrste, odnosno one koji sadrže zlćudni program koji, između ostalog, sadrži i *Remote access* funkcionalnost koja će, ukoliko žrtva preuzme zlćudni program te se on instalira na njeno računalo, napadaču omogućiti kontrolu nad žrtvinom računalom s proizvoljne lokacije. Jedna elektronička poruka namijenjena je predstojniku *Predstojnik1*, a druga tajnici *Tajnica1*. Obzirom da *Predstojnik1* ima postavljenu kontrolu *Security awareness* na 1, on će prijaviti primitak sumnjive elektroničke poruke, dok tajnica, čija je kontrola *Security awareness* postavljena na 0, neće. Nakon što se elektroničke poruke pošalju te je *Predstojnik1* prijavi, obavlja se prethodno opisana analiza primljene elektroničke poruke. Rezultati analize (Slika 4.28) pokazuju kako elektronička poruka sadrži zlćudni program koji se potom šalje na reverzanje.



Slika 4.28 Rezultat analize sumnjive elektroničke poruke sa zlćudnim programom

Uzevši u obzir činjenicu da reverzanje nedavno primljene datoteke s metodom iskorištavanja još uvijek traje, a obavlja ga jedina osoba na fakultetu koja ima vještinu za

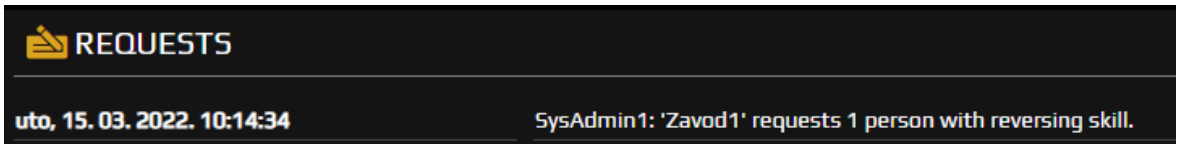
to, potrebno je obratiti se vanjskoj organizaciji za pomoć. To je moguće napraviti akcijom *Request Assistance* (Slika 4.29).



Slika 4.29 Akcija traženja pomoći od *Vanjske Organizacije*

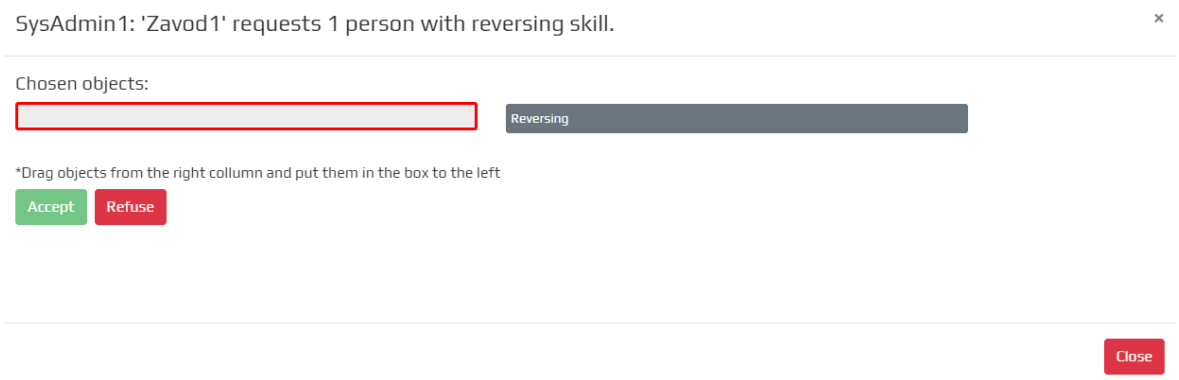
U ovom slučaju, pomoć od *Vanjske Organizacije* traži sistemski administrator *SysAdmin1*. Konkretno, traži jednu osobu koja ima atribut *Skills* postavljen na *Reversing* obzirom da želi reverzanje.

U trenutku kada se izvrši navedena akcija, u ekranu igrača koji kontrolira *Vanjsku Organizaciju* pod *Requests* se pojavljuje zahtjev od osobe *SysAdmin1* (Slika 4.30).



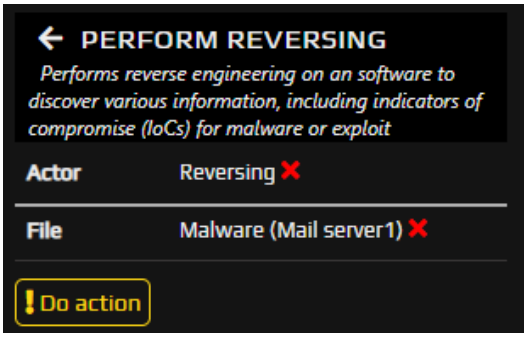
Slika 4.30 Novi zahtjev u sučelju igrača koji kontrolira *Vanjsku Organizaciju*

Kako bi prihvatio zahtjev, igrač mora kliknuti na taj zahtjev te odabrati osobu s kojom će izvršiti taj zahtjev. U ovom slučaju, ta osoba se zove *Reversing* (Slika 4.31).



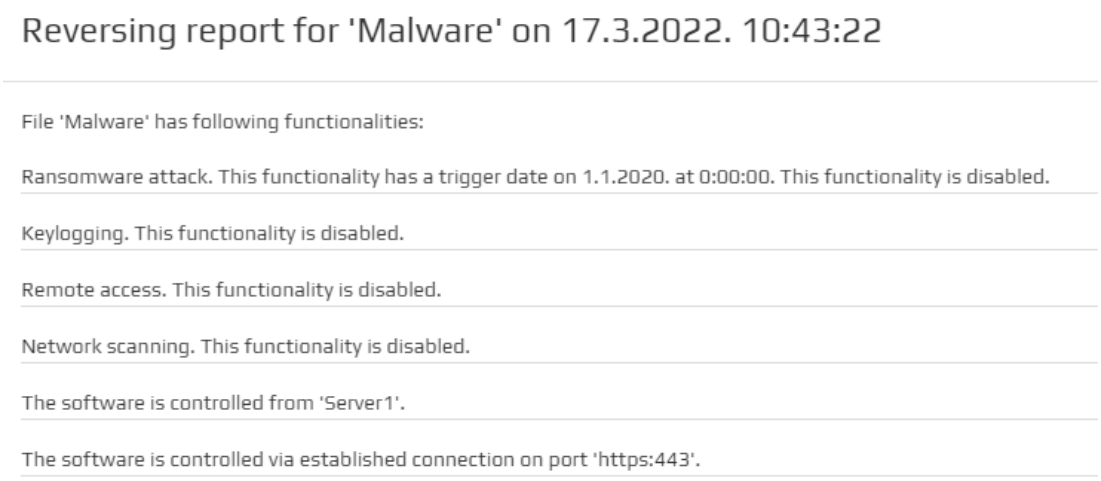
Slika 4.31 Izbornik za prihvaćanje ili odbijanje zahtjeva

Nakon što igrač koji kontrolira *Vanjsku Organizaciju* prihvati zahtjev, osoba *Reversing* je sada dostupna u braniteljskoj topologiji te može izvršiti akciju reverzanja zloćudnog programa.



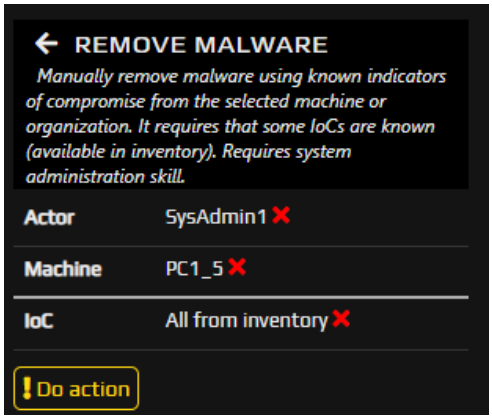
Slika 4.32 Akcija reverzanja od strane osobe iz *Vanjske Organizacije*

Nakon nekog vremena, branitelji dobivaju obavijest kako je reverzanje dovršeno te imaju na uvid izvješće reverzanja. Kao što je vidljivo u izvješću, branitelji znaju koje funkcionalosti zloćudni program ima te da je kontroliran od strane računala *Server1*.



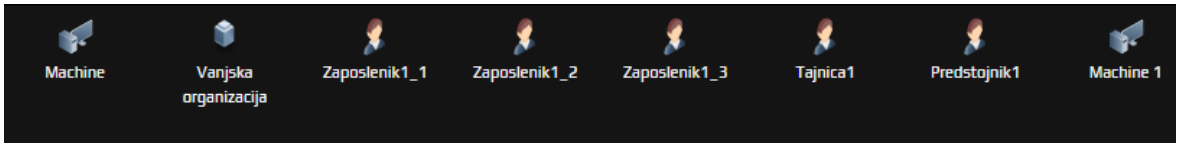
Slika 4.33 Izvješće reverzanja zloćudnog programa

Sada je braniteljima omogućena akcija *Remove Malware* kojom mogu ukloniti zloćudni program za računala osobe *Predstojnik1*.



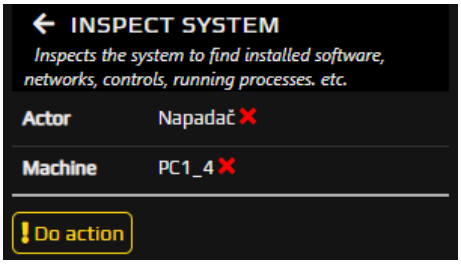
Slika 4.34 Akcija uklanjanja zlćudnog programa

Međutim, unatoč uspješnom reverzanju od strane *Vanjske Organizacije* i uklanjanju zlćudnog programa kojeg je primio *Predstojnik1*, *Tajnica1* je već kliknula na privitak u elektroničkoj poruci te je na taj način, nesvjesno, dozvolila da se zlćudni program instalira na njenom računalu. Samim time, napadač je dobio signal (engl. *beacon*) na svom *command and control* poslužitelju *Server1* te sada u svojoj topologiji vidi i računalo tajnice (Slika 4.35).

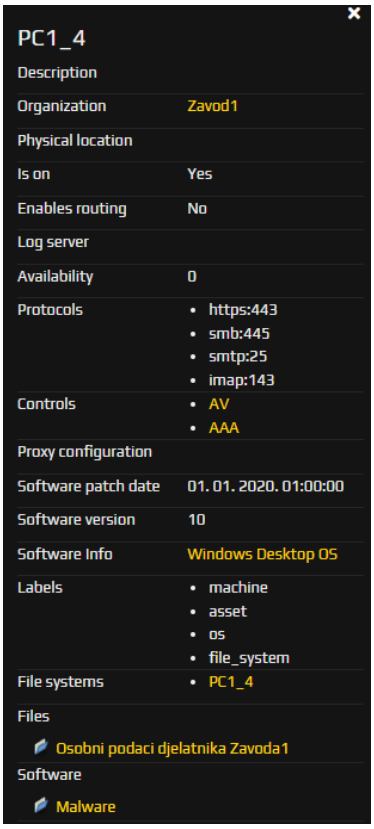


Slika 4.35 Machine1, računalo tajnice, sada je vidljivo napadaču

Napadač sada akcijom *Inspect System* (Slika 4.36) može pregledati računalo tajnice te na taj način pronalazi jedan od osjetljivih dokumenata (Slika 4.37).

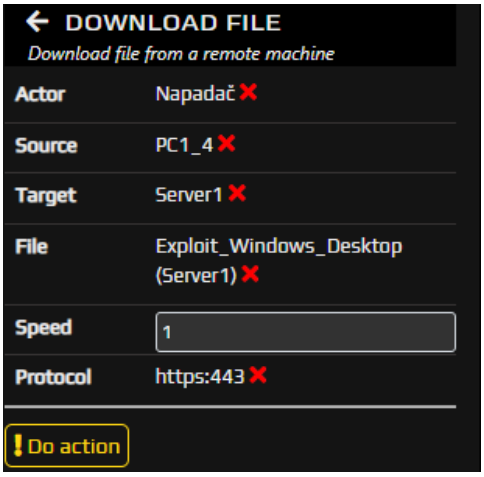


Slika 4.36 Akcija detaljnog pretraživanja sistema računala tajnice



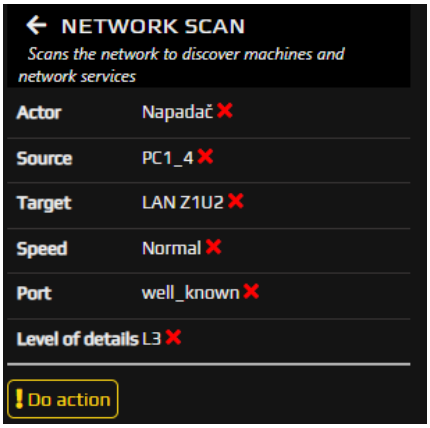
Slika 4.37 Rezultati detaljnog pretraživanja sistema računala tajnice

Nadalje, napadač sada može na tajničino računalo akcijom *Download File* (Slika 4.38) prenijeti proizvoljne datoteke koje će probati iskoristiti za dobivanje pristupa nad drugim računalima u istoj mreži kao i tajničino računalo. Primjerice, može prenijeti datoteku s nekom metodom iskorištavanja. U ovom slučaju, recimo da je napadač pretpostavio da i ostala računala koriste *Windows* operacijski sustav pa odabire datoteku s metodom iskorištavanja za operacijski sustav *Windows*. Pritom je potrebno definirati računalo na koje će se staviti datoteka pod *Source*, računalo s kojeg se šalje datoteka pod *Target*, brzinu prijenosa pod *Speed* te protokol preko kojeg će se izvršiti akcija.



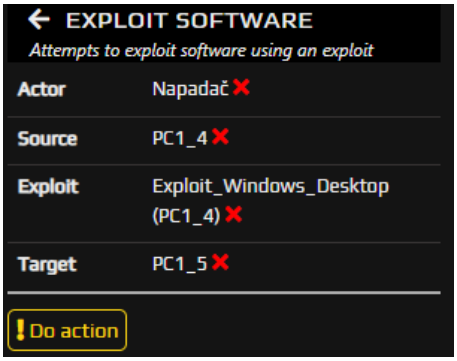
Slika 4.38 Akcija prebacivanja zloćudne datoteke na računalo tajnice

Međutim, kako bi napadač znao koja još računala postoje u mreži, potrebno je skenirati mrežu akcijom *Network Scan* (Slika 4.39) gdje kao *Source*, odnosno izvorišno računalo postavlja računalo tajnice dok za *Target*, odnosno metu, postavlja lokalnu mrežu koju je otkrio pri pregledu računala tajnice. Kako bi skeniranje prošlo neopaženo, napadač može odabrati opciju brzine koja nije prevelika, primjerice *Normal* uz skeniranje samo poznatih vrata (engl. *well – known ports*) kako skeniranje ne bi trajalo predugo te maksimalnu, *L3*, razinu detalja.



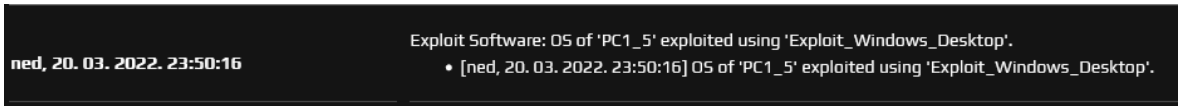
Slika 4.39 Akcija skeniranja lokalne mreže

Nakon skeniranja mreže, napadač ima uvid u sva računala u istoj mreži kao i tajničino računalo te sada može probati dobiti kontrolu nad nekim od tih računala. Akcijom *Exploit Software* (Slika 4.40) napadač pokušava sa tajničinog računala postavljenog kao *Source* dobiti kontrolu nad računalom *PC1_5* postavljenog kao *Target* koristeći datoteku s metodom iskorištavanja za operacijski sustav *Windows* postavljenu kao *Exploit*.



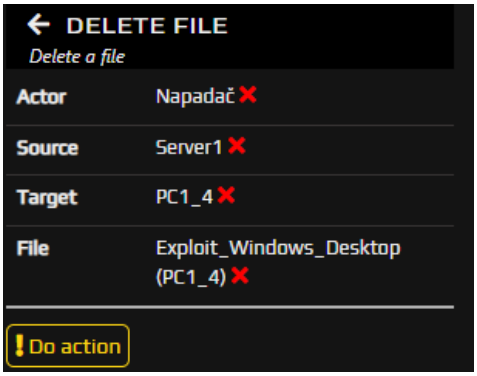
Slika 4.40 Akcija pokušaja iskorištavanja ranjivosti koristeći prethodno postavljenu zlćudnu datoteku

Nakon izvođenja akcije, ako je ona bila uspješna, napadač dobiva obavijest o tome.

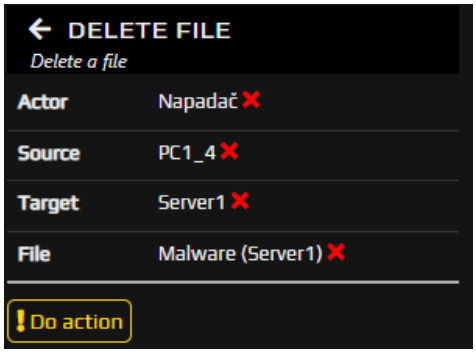


Slika 4.41

Naposlijetku, nakon što prethodna akcija uspije, napadač može izbrisati korištenu datoteku za iskorištavanje ranjivosti drugog računala, ali i prvotni zlćudni program koji se instalirao nakon što je *Tajnica* kliknula na njega kako ne bi ostavio tragove braniteljima koji će dovesti do njega. To može napraviti akcijom *Delete File* (Slika 4.42 i Slika 4.43).



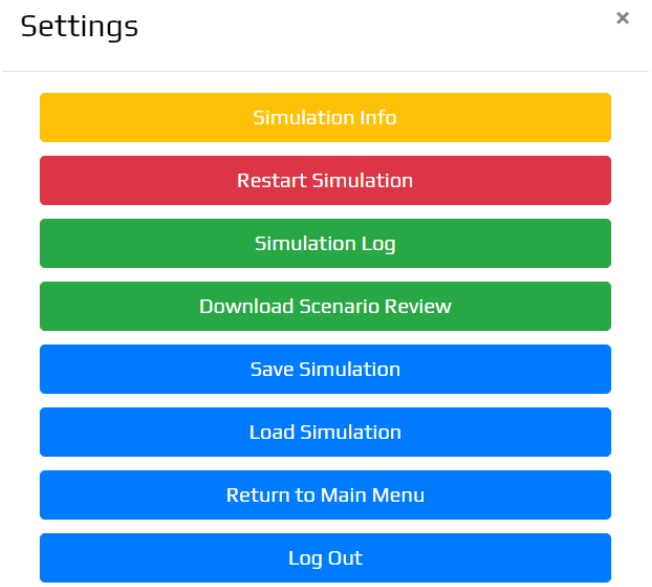
Slika 4.42 Akcija brisanja datoteke za iskorištavanje ranjivosti sa računala tajnice



Slika 4.43 Akcija brisanja zlćudnog programa sa računala tajnice

U tom trenutku, može se zaključiti kako je napadač uzrokovao poprilično štetu te se simulacija može prekinuti sa zaključkom kako je za napadača završila s pozitivnim ishodom te naravno negativnim za branitelje.

Nakon što je simulacija gotova, ali i tijekom simulacije, administratoru simulacije, odnosno *Simulation masteru*, klikom na kotačić u gornjem desnom kutu omogućene su brojne postavke vezane uz simulaciju koja se trenutno izvodi (Slika 4.44).



Slika 4.44 Postavke simulacije u administratorskom sučelju

Jedna od najkorisnijih opcija po završetku simulacije jest *Download Scenario Review* koja nam omogućava preuzimanje tijeka simulacije u obliku *spreadsheet* tablice koju je potom moguće otvoriti primjerice s *Microsoft Excelom* te analizirati provedenu simulaciju korak po korak.

5. Opis skripte za skalabilnost i manipuliranje topologijom

Nakon predstavljanja topologije s napadačkom i braniteljskom stranom te demonstracije napada na istu, u nastavku će biti predstavljena skripta kojom je omogućena manipulacija skalabilnošću topologije, u ovom slučaju ponajviše brojem *Zavoda*. Skripta je napravljena u programskom jeziku *Python*, a sastoji se od nekoliko glavnih dijelova. Obzirom da svaki objekt u CCS – u ima vlastiti ID koji se sastoji od 35 nasumičnih malih slova sa znakom „_“ na pozicijama 8, 13, 18 te 23, u prvom dijelu skripte nalazi se funkcija za generiranje ID – eva objekata. Funkcija, osim što generira ID – eve, također pazi da se generirani ID već ne nalazi u topologiji, iako je vjerojatnost za to poprilično mala.

```
def generate_id(input2_data):
    flag = True
    while True:
        id = ""
        for i in range(36):
            if i == 8 or i == 13 or i == 18 or i == 23:
                id += "_"
            else:
                id += chr(random.randint(97, 122))
        for i in input2_data:
            if id in i["id"]:
                flag = False
        if flag is True:
            return id
```

Kôd 4.1 – Funkcija za generiranje jedinstvenih ID – eva objekata

Drugi dio skripte sastoji se od pripreme struktura te datoteka iz kojih se čita te datoteka u koje će se kasnije upisati rezultat. Sve datoteke su u *JSON* obliku.

```
departments = 10
workers_per_department = 6
av_to_turn_off = 0
input1 = open("D:\Downloads1\kg_diplomski1\ClientInfo.json",
"r+")
input1_data = json.loads(input1.read())
```

```
input2 = open("D:\Downloads1\kg_diplomski1\Global.json",
"r+")
input2_data = json.loads(input2.read())
input3 = open("D:\Downloads1\kg_diplomski1\Players.json",
"r+")
input3_data = json.loads(input3.read())
output1 = open("ClientInfo.json", "w+")
output2 = open("Global.json", "w+")
output3 = open("Players.json", "w+")
startX = 3400
startY = 2500
```

Kôd 4.2 – Priprema struktura te datoteka za čitanje, odnosno pisanje

Varijable `startX` i `startY` odnose se na početne koordinate objekata u topologiji. Treći dio koda je ujedno i glavni dio koji se odnosi na multipliciranje *Zavoda*. Multipliciranje je realizirano `for` petljom čiji je broj iteracija jednak vrijednosti varijable `departments` čija se definicija nalazi iznad, u drugom dijelu koda.

```
for d in range(departments):
…
```

Zavodi se multipliciraju na način da se u postojeću datoteku `Global.json` nadodaju objekti koji se nalaze u svakom *Zavodu* u *JSON* obliku. Primjer dodavanja novog zaposlenika prikazan je u nastavku.

```
input2_data.append({"labels": ["actor", "person"], "id": id3,
"name": "Zaposlenik" + str(d + 4) + "_" + str(j + 1),
"description": "", "skills": [], "organization_id": id,
"physical_zone": id2, "work_stations": [id4], "vip": False,
"publicly_exposed": 0.3, "e - mail": "zaposlenik" + str(d +
4) + "_" + str(j + 1) + "@zavod" + str(d + 4) +
".fakultet.hr", "emails_recieved_per_day": 3, "reads_e -
mail_on": [id4], "accounts": [{"labels": ["user_account",
"data"], "name": "zaposlenik" + str(d + 4) + "_" + str(j + 1)
+ "@zavod" + str(d + 4) + ".fakultet.hr", "user_account_id":
"zaposlenik" + str(d + 4) + "_" + str(j + 1) + "@zavod" +
str(d + 4) + ".fakultet.hr", "frequency": 0, "last_changed":
1577836800000, "disabled": False, "quality": 0, "is_hashed":
False, "natural_key": "zaposlenik" + str(d + 4) + "_" + str(j
+ 1) + "@zavod" + str(d + 4) + ".fakultet.hr1/1/2020 12:00:00
AM"}],"gathered_intelligence": [], "controls":
[{"labels":["control", "securityawareness"], "name":"Security
```

```
awareness", "awareness":0.5, "isactive":True, "mode":["log",
"alert", "block"], "event_frequency":10}], "assets": [],
"enable_messaging": False, "natural_key": "Zaposlenik" +
str(d + 4) + "_" + str(j + 1)})
```

Kôd 4.3 – Primjer dodavanja novog objekta u JSON obliku

Uz to, novododani objekt se nadodaje u postojeću datoteku `ClientInfo.json` u kojoj se nalaze koordinate svih objekata unutar topologije te njihove ikone. Tu se koriste prethodno spomenute varijable `startX` te `startY` kako bi se izračunale koordinate novih objekata. Željena lokacija objekata dobivena je metodom pokušaja i pogreške. Primjer dodavanja novog zaposlenika u datoteku `ClientInfo.json` dan je u nastavku.

```
input1_data[0]["Objects"][id3] = {"X": startX + (j * 150),
"Y": startY, "IconPath": "/graphIcons/actor-000.png"}
```

Redoslijed dodavanja objekata u `for` petlji jest slijedeći. Prvo se dodaje nova organizacija te nova interna fizička lokacija *Zavoda*. Zatim se u još jednoj `for` petlji s 2 iteracije dodaju 2 ureda sa zaposlenicima u jednom uredu te tajnicom, predstojnikom i sistemskim administratorom u drugom uredu. Nakon ureda dodaju se ostali objekti unutar *Zavoda* poput posredničkog poslužitelja, poslužitelja elektroničke pošte itd. te softverski elementi poput *AAA* i *AV* grupa te konfiguracija pravila vatrozida. Nakon završetka glavne `for` petlje provjerava se je li varijabla `av_to_turn_off` različita od 0 te ako je, gasi se antivirusna zaštita tog *Zavoda*.

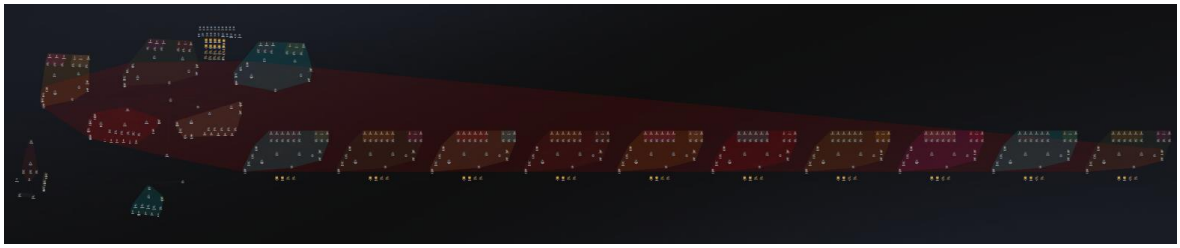
```
if av_to_turn_off != 0:
    for i in range(len(input2_data)):
        if "AV grupa Z" + str(av_to_turn_off) in
input2_data[i]["name"]:
            input2_data[i]["members"] = [""]
            input2_data[i]["controls"] = []
```

Kôd 4.4 – Dio koda zadužen za gašenje vatrozida određenog *Zavoda*

Na kraju skripte obavlja se preslikavanje ažuriranih *JSON* objekata u nove datoteke kako se izvorne datoteke ne bi mijenjale.

```
json.dump(input1_data, output1, indent=2)
json.dump(input2_data, output2, indent=2)
```

Globalni rezultat izvođenja skripte s parametrima prikazanim u prvom dijelu vidljiv je u nastavku (Slika 5.1) (topologija je umanjena maksimalno kako bi se cijela vidjela).



Slika 5.1 Izgled topologije nakon izvođenja skripte

Što se pojedinog *Zavoda* tiče, to izgleda ovako (Slika 5.2):

Slika 5.2 Primjer *Zavoda* nastalog izvođenjem skripte

Kao što je vidljivo na slici, zbog manipuliranja koordinata objekata, svi objekti su poravnati te ih nije potrebno ručno namještati.

6. Zaključak

Sve u svemu, jasno je da će porastom tehnologije u budućnosti računalni incidenti biti sve češći te provođeni od strane sve vještijih napadača. Upravo zato su potrebne platforme poput *Cyber Conflict Simulatora* (CCS) kojima je cilj obučiti zaposlenike raznih tvrtki o konkretnim reakcijama na napade koji će se neizbježno dogoditi. Međutim, potpuna obrana nije i nikada neće biti moguća, ali, osim korištenja CCS – a kao poligona za obuku, potrebna je i konstantna edukacija te podizanje kolektivne svijesti zaposlenika o kibernetičkoj sigurnosti kako bi se šansa za uspješan napad svela na minimum.

Neki od najčešćih savjeta su korištenje sigurnih lozinki, neotvaranje sumnjivih poveznica te privitaka unutar elektroničke pošte te neobjavljivanje poslovnih tajni na Internetu. Tek ako zaposlenici počnu primjenjivati te prakse, tvrtka se može nadati da čak i ako dođe do napada, šteta neće biti prevelika.

Nadam se da će ovaj poligon zajedno sa skriptom pomoći tvrtkama, ali i studentima koji tek ulaze u područje kibernetičke sigurnosti te kako će doprinijeti podizanju svijesti o važnosti kibernetičke sigurnosti u današnjim poslovanjima.

7. Literatura

[1] Firch, J. *Red Team VS Blue Team: What's The Difference?*, PurpleSec, 2021., rujan. Poveznica: https://purplesec.us/red-team-vs-blue-team-cyber-security/; pristupljeno 15. svibnja 2022.

[2] *Cyber Conflict Simulator – često postavljana pitanja*. Poveznica: https://ccs.utilis.biz/Home/Faq; pristupljeno: 20. ožujka 2022.

[3] Larsen, R., *What are command-and-control (C2) callbacks?*, Dualog, 2021., kolovoz. Poveznica: https://www.dualog.com/blog/what-are-command-and-control-c2-callbacks; pristupljeno 30. svibnja 2022.

[4] Dmarc as a service, Brand protection, *Spear Phishing vs Phishing: What's the Difference?*, Valimail, 2021., listopad. Poveznica: https://www.valimail.com/blog/phishing-vs-spear-phishing/; pristupljeno: 01. travnja 2022.

[5] Englesko-hrvatski rječnik, Groš S., http://www.zemris.fer.hr/~sgros/stuff/rjecnik.shtml; pristupljeno 22. lipnja 2022.

Sažetak

Izgradnja složenog kibernetičkog poligona za vježbe napada i obrane

Ovaj rad započinje opisom *Cyber Conflict Simulatora* (CCS) u obliku uputa za izradu poligona s osnovnim, najčešćim elementima. Zatim je dan pregled složenog kibernetičkog poligona za vježbe napada i obrane koji se sastoji od dva glavna dijela: napadačkog i braniteljskog. Braniteljski dio modeliran je na način da predstavlja fiktivni fakultet koji se sastoji od mnoštva zavoda te dekanata i ureda IT podrške. Cijela topologija je detaljno opisana te je potom u trećem poglavlju prezentirana simulacija napada u kojoj kao igrači sudjeluju napadač, branitelji te vanjska organizacija. Na kraju, dan je pregled skripte kojom je moguće utjecati na skalabilnost poligona te manipulirati funkcionalnostima poligona, primjerice gašenjem antivirusa.

Ključne riječi: kibernetička sigurnost, *cyber conflict simulator*, napadač, branitelji, simulacija, kibernetički poligon, topologija, skalabilnost

Summary

Building complex cyber ranges for offense and defence exercises

This thesis begins with a description of Cyber Conflict Simulator (CCS) in the shape of a tutorial for building a simple landscape with some basic, most common elements in it. Then, a complex cybernetic range intended for attacking and defending practices is presented. It consists of two parts: attacking part and defensive part. Defensive part of the range is shaped in a way that it represents a fictional college which then consists of various departments, dean's office and an IT support office. Entire range is described in details and then, in the third chapter of the thesis, an attack simulation, which consists of three players, i.e. attackers, defenders and an external organization, is described. In the last chapter of the thesis, an overview of the scalability script is given. The purpose of the script is automated object adding and also manipulating range functionalities, e.g. antivirus.

Keywords: cybernetic security, cyber conflict simulator, attacker, defenders, simulation, cybernetic range, topology, scalability

Skraćenice

CCS	*Cyber Conflict Simulator*	simulator kibernetičkih napada

Privitak

Cijeli kod skripte opisane u zadnjem poglavlju rada nalazi se na poveznici https://github.com/kristijan-g/diplomski_rad