HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Unicornscan alata

CCERT-PUBDOC-2004-11-99

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.
Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr**- laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 4

2. INSTALACIJA I KONFIGURACIJA 5

2.1. KONFIGURACIJSKA DATOTEKA 5
2.2. PODRŠKA ZA RELACIJSKE BAZE PODATAKA 5

3. KORIŠTENJE ALATA 7

3.1. VRSTE SKENIRANJA ..... **ERROR! BOOKMARK NOT DEFINED.**
3.1.1. TCP skeniranje 7
3.1.2. UDP skeniranje 8
3.1.3. Prikupljanje poruka aktivnih servisa 8
3.2. MODIFIKACIJA TCP/IP STOGA 8
3.3. PCAP FILTRIRANJE 9

4. ALICORN WEB SUČELJE 10

4.1. INSTALACIJA 10
4.2. KORIŠTENJE ALICORN PROGRAMA 10

5. ZAKLJUČAK 13

1. Uvod

Unicornscan je moćan i svestran alat namijenjen IT profesionalcima koji se bave ispitivanjem sigurnosti i testiranjem rada računalnih mreža i servisa. Projekt nastao na temelju jednostavnog alata za pregledavanje UDP mrežnih portova, pod nazivom udpscan, čiji je koncept bio idealan za nadogradnju novim funkcionalnostima. Osnovna ideja alata je da istraživačima pruži jedinstveno i fleksibilno sučelje za obavljanje različitih vrsta testova. Budući da se ovaj alat vrlo brzo razvija i nadograđuje, broj funkcija koje podržava mijenja se iz dana u dan. Neke od trenutno najpopularnijih funkcija obuhvaćaju:

- Asinkrono TCP skeniranje sa mogućom varijacijom svih TCP zastavica,
- Automatsko prikupljanje poruka koje poslužitelji prijavljuju prilikom spajanja na odgovarajući port (engl. *banner*),
- Asinkrono skeniranje UDP portova s dodanom podrškom za specifične protokole korištene od strane skeniranih servisa,
- Aktivna i pasivna identifikacija udaljenog operacijskog sustava,
- Filtriranje dobivenih podataka i spremanje u PCAP formatu,
- Spremanje izlaznih podataka u relacijsku bazu podataka,
- Podrška za korisnički definirane module.

Ideja je da s vremenom svojom funkcionalnošću ovaj alat zamijeni što je više moguće različitih alata korištenih u testiranju računalnih mreža i mrežnih servisa, kao bi stručnjacima zaduženima za testiranje olakšao njihov posao.

Program je licenciran pod GPL licencom što omogućuje njegovo slobodno korištenje i eventualnu izmjenu izvornog koda.

2. Instalacija i konfiguracija

Paket sa izvornim kodom programa, kao i RMP i DEB paketi za Fedora i Debian distribucije Linux-a mogu se dohvatiti sa adrese http://www.dyadsecurity.com/s_unicornscan.html. Alat je trenutno moguće instalirati na svim Linux operacijskim sustavima, SUN Solaris, NetBSD, OSX i FreeBSD sustavima, a očekuje se da će sljedeća inačica biti kompatibilna i s HP-UX i AIX sustavima. Korisnicima Debian i Fedora sustava preporučuje se korištenje gotovih paketa jer se na taj način znatno ubrzava i olakšava instalacijski proces, dok će korisnici ostalih operacijskih sustava morati ručno prevesti paket iz izvornog koda. RPM paket je, uz manje dodatne zahvate, moguće instalirati i na većini RPM baziranih distribucija poput Mandrake ili SuSe Linux-a, budući da je ovisan isključivo o libpcap paketu.

U trenutku pisanja ovog dokumenta ne postoji skripta za automatsku konfiguraciju, već se prije prevođenja izvornog koda ručno podešavaju parametri sustava. U datotekama `src/config.h` i `src/Makefile.inc` nalaze se uobičajene postavke parametara koje je za specifične slučajeve potrebno prilagoditi. Uz same konfiguracijske parametre, u ovim datotekama nalaze se i opsežne upute za podešavanje istih, što bi trebalo proces podešavanja učiniti manje mukotrpnim.

Nakon podešavanja, paket se prevodi pomoću naredbe `make` i instalira pomoću naredbe `make install`. Instalacija obuhvaća kopiranje datoteka u razne sistemske direktorije, što podrazumijeva da se `make install` naredba izvodi pod ovlastima administratora sustava.

Nakon uspješne instalacije, programi `unicornscan` i `fantaip` moraju se (ukoliko drugačije nije navedeno prilikom izmjene konfiguracijskih datoteka) nalaziti unutar `/usr/local/bin` direktorija. Dokumentacija i dodatni moduli programa nalaze se unutar `/usr/local/doc` i `/usr/local/libexex/unicornscan` direktorija. Uz program se instalira i 'man' stranica koja opisuje sve parametre koji se koriste prilikom pokretanja alata iz naredbenog retka.

2.1. Konfiguracijska datoteka

Uobičajeno ponašanje Unicornscan alata kontrolira se parametrima `unicorn.conf` konfiguracijske datoteke. Ova datoteka nalazi se unutar `/usr/local/share/unicornscan/` direktorija u koji su također smještene i ostale konfiguracijske datoteke bitne za rad programa. Značenje pojedinih datoteka je sljedeće:

- `p0f.fp`, `p0fa.fp` i `p0fr.fp` – baze potpisa za pasivnu identifikaciju udaljenih operacijskih sustava
- `payloads.conf` – u ovoj datoteci definirani su različiti protokoli kojima se koriste servisi koji osluškuju mrežni promet na UDP portovima. Sadržaj ove datoteke vrlo je bitan za pregledavanje UDP portova.
- `port-numbers` – lista svih TCP i UDP portova i pripadajućih servisa,
- `unicorn.conf` – glavna konfiguracijska datoteka Unicornscan alata.

Svi zapisi u glavnoj konfiguracijskoj datoteci pohranjeni su u sljedećem formatu (detaljan opis opcija nalazi se u man stranici):

```
opcija: vrijednost;
```

Pri svakom pokretanju, Unicornscan će analizirati parametre proslijeđene iz naredbenog retka i smatrati ih važećima. Ukoliko u naredbenom retku nisu navedeni svi potrebni parametri, koristiti će se vrijednosti iz konfiguracijske datoteke.

2.2. Podrška za relacijske baze podataka

Kao što je u uvodu spomenuto, Unicornscan je sposoban rezultate skeniranja pohraniti u relacijsku bazu podataka. Tako pohranjeni podaci mogu se kasnije uspoređivati s rezultatima ostalih skeniranja, što omogućuje detaljniju analizu dobivenih rezultata, a baza podataka koristi se i za rad s Web sučeljem pod nazivom Alicorn. Za sada je podržano isključivo spajanje na Postgresql poslužitelj za upravljanje bazama podataka.

Podaci o lokaciji baze podataka, kao i korisničkom imenu i zaporci za pristup istoj, nalaze se u binarnim datotekama alata, što znači da je postavke potrebno podesiti prije prevođenja izvornog koda.

Svi parametri potrebni za spajanje na bazu podešavaju se unutar datoteke `src/output_modules/database/logininfo.h`, čiji je sadržaj dan u nastavku.

```
#ifndef _LOGININFO_H
#define _LOGININFO_H

#define USERNAME       "korisničko_ime"
#define PASSWORD       "zaporka"
#define DBHOST        "poslužitelj"
#define DBNAME         "ime_baze"

#endif
```

Parametar `OPT_MODS=db_module` koji se nalazi u `src/Makefile.inc` datoteci uključuje podršku za bazu podataka prilikom prevođenja programa. Sama baza kreira se pomoću pgsql naredbe, a kako bi program ispravno pohranjivao podatke, u kreiranu bazu potrebno je inicijalno učitati sadržaj `src/output_modules/database/psql_schema.sql` datoteke.

Ukoliko je Unicornscan instaliran iz predkompajliranih RPM ili DEB paketa, rezultate skeniranja nije moguće pohraniti u bazu podataka, niti je moguće koristiti Web sučelje za rad s alatom.

3. Korištenje alata

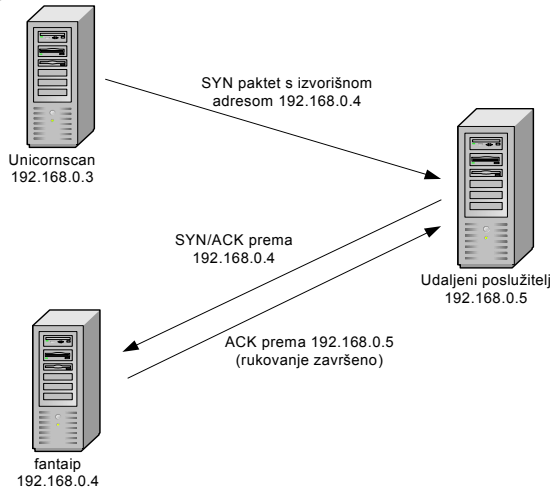
Korištenje Unicornscan programa vrlo je jednostavno. Program se pokreće iz naredbenog retka i izvršava skeniranje ovisno o proslijeđenim parametrima. Detaljan opis svih parametara nalazi se unutar man stranice alata, kratak opis moguće dobiti njegovim pokretanjem sa `-help` opcijom. Kako bi skeniranje bilo uspješno, Unicornscan se obavezno mora pokrenuti sa ovlastima administratora sustava.

Sintaksa za pokretanje jednostavnog pregledavanja računalne mreže od 255 IP adresa na svim mrežnim portovima je sljedeća:

```
# unicornscan 192.168.0.0/24:a
```

, pri čemu parametar `:a` iza IP adrese označava sve mrežne portove. Broj poslanih paketa u sekundi dodatno se može kontrolirati opcijom `-r`, a detaljnost izlaznih podataka povećava se korištenjem `-v` opcije. Uobičajena vrijednost za brzinu slanja paketa je 300 paketa po sekundi. Na modernim sustavima sa jakim procesorima, brzinu slanja moguće je povećati čak do 40,000 paketa u sekundi, ali pri tome treba imati u vidu kapacitete računalne mreže koja se nalazi između računala sa Unicorscan alatom i testiranog sustava. Kod mrežne opreme lošije kvalitete, a pogotovo SOHO vatrozida i mrežnih usmjerivača, zagušenje mreže može se pojaviti već pri nekoliko tisuća paketa u sekundi.

Kod specifičnih skeniranja računalnih mreža, povratne informacije tj. paketi često se razlikuju od standardnih paketa koje jezgra operacijskog sustava očekuje, pogotovo u slučajevima kada povratni paketi sadrže ciljnu IP adresu različitu od adrese sustava. Zbog toga se uz Unicornscan koristi i dodatni „Phantom IP" program pod nazivom `fantaip`. Zadatak ovakvog programa je da na posebnom mrežnom sučelju prihvaća povratne pakete koje bi inače jezgra operacijskog sustava odbacila kao nelegalne. Tako npr. klasično TCP rukovanje u tri koraka (engl. *three way handshake*)korištenjem `fantaip` programa izgleda ovako:



Slika 1: TCP three way handshake pomoću fantaip alata

Adresa povratnog sučelja specificira se parametrom `-s` prilikom pokretanja Unicornscan alata.

Ovakav pristup skeniranju mrežnih portova omogućuje znatno brži rad, jer proces koji šalje pakete ne mora čekati na odgovor udaljenog računala, već se za to brine `fantaip` program. Negativna strana korištenja dvostrukog sučelja je velik broj grešaka prilikom provođenja postupka skeniranja, u slučaju da se na istom računalu paralelno provode testovi sa nekim drugim alatima.

3.1. Metode pregledavanja portova

3.1.1. TCP skeniranje

Prilikom pregledavanja TCP portova također je moguće zasebno definirati vrijednosti pojedinih zastavica TCP paketa, što omogućuje različite vrste skeniranja i testiranja sustava. Opcija `-m`, iza koje

slijede imena zastavica TCP zaglavlja kojima se pridjeljuje vrijednost jedan, omogućuje ovakvo ponašanje alata. Neki od tipova skeniranja koje je moguće definirati su sljedeći:

- `-mT` – SYN skeniranje
- `-mTsA` – ACK skeniranje
- `-mTsF` – Fin skeniranje
- `-mTsFPU` – slanje Xmas paketa

Osim navedenih skeniranja, ovisno o potrebama, moguće je proizvoljno varirati sadržaj TCP zaglavlja i definirati vlastite tipove skeniranja. Npr. opcija `-mTFSRPAUEC` uključiti će sve zastavice u TCP zaglavlju.

3.1.2. UDP skeniranje

Postupak pregledavanja UDP portova kod Unicornscan alata prilično se razlikuje u odnosu na klasične metode UDP skeniranja. Kod klasičnog skeniranja, računalo koje provodi skeniranje poslati će na odredišnu adresu UDP paket bez sadržaja, te iščekivati ICMP odgovor na temelju kojega je moguće odrediti stanje testiranog UDP mrežnog porta. Ukoliko ciljno računalo odgovori sa ICMP T3C3 (Destination Unreachable, Port Unreachable) porukom, port će se označiti kao zatvoren. Ukoliko generirani upit rezultira ICMP T3C3 paketom sa bilo koje druge IP adrese, skenirani port proglasit će se filtriranim, budući da se smatra da je paket blokiran na svom putu prema testiranom računalu. Ukoliko slanje testnog paketa ne rezultira nikakvim odgovorom program će označiti port kao otvoren.
Budući da ovakav koncept često rezultira lažno detektiranim portovima, Unicornscan je osmišljen tako da pokuša komunicirati sa servisom koji osluškuje određeni mrežni port. Tako će npr. kod skeniranja porta 53 (DNS poslužitelj) Unicornscan pokušati poslati „`localhost A record`“ zahtjev. Ukoliko dobije pozitivan odgovor, port će sa sigurnošću biti označen kao otvoren. Trenutno je podržana komunikacija s 54 najčešće korištena UDP servisa.

```
# unicornscan 192.168.3.0/24:53 -mU -s 192.168.3.12
Open         domain[53]   From 192.168.3.3     ttl 64
Open         domain[53]   From 192.168.3.4     ttl 64
Open         domain[53]   From 192.168.3.1     ttl 128
Open         domain[53]   From 192.168.3.16    ttl 64
Open         domain[53]   From 192.168.3.24    ttl 128
Open         domain[53]   From 192.168.3.211   ttl 128
```

3.1.3. Prikupljanje poruka aktivnih servisa

U Bannergrab načinu rada Unicornscan program se pokušava spojiti na zadane IP adrese i mrežne portove te sa njih dohvatiti poruke koje poslužitelji javljaju prilikom spajanja. Zbog svoje brzine, Unicornscan je pogodan za masovno dohvaćanje poruka sa velikog broja IP adresa. Poruke se dohvaćaju tako da se definira klasičan TCP connect način pregledavanja portova (`-msf` opcija).

```
#unicornscan 192.168.3.0/24:25 -msf -s 192.168.3.12
Open smtp[25] From 192.168.3.3   `220 iva.domain.local ESMTP Postfix
Open smtp[25] From 192.168.3.4   `220 petra.domain.local ESMTP Postfix
Open  smtp[25]  From  192.168.3.10   `220  ana.domain.local  Microsoft  ESMTP
MAIL
Open smtp[25] From 192.168.3.14  `220  marija.domain.local ESMTP Sendmail
Open smtp[25] From 192.168.3.16  `220 maja.domain.local ESMTP Postfix
Open smtp[25] From 192.168.3.17  `220 ivona.domain.local ESMTP Sendmail
Open smtp[25] From 192.168.3.20
Open smtp[25] From 192.168.3.160 `220 vlatka Microsoft ESMTP MAIL Service
Open smtp[25] From 192.168.3.211 `220 marija.domain.local Microsoft ESMTP
MAIL
Open smtp[25] From 192.168.3.240 `220 nina.domain.local - tea.domain.local
SMTP
Open smtp[25] From 192.168.3.250 `220 test.domain.local ESMTP Sendmail
```

3.2. Modifikacija TCP/IP stoga

Svaki operacijski sustav unutar svoje jezgre ima specifičnu implementaciju TCP/IP stoga. Na principu prepoznavanja različitosti između tih implementacija zasniva se rad alata za pasivnu identifikaciju operacijskih sustava.
Unicornscan definira parametre paketa izvan jezgre sustava i zbog toga je (korištenjem `-W` opcije) moguće pakete oblikovati tako da oponašaju TCP/IP stog drugih operacijskih sustava. U trenutnu

inačicu alata uključena je emulacija Cisco, OpenBSD, Windows XP, FreeBSD i Linux operacijskih sustava te p0fsendsysn, nmap i Crazy lint alata.
Modificiranje TCP/IP stoga moguće je koristiti za zbunjivanje alata za detekciju neovlaštenog pristupa (IDS) i alata za pasivnu identifikaciju operacijskih sustava, kao i komunikaciju s određenim OpenBSD vatrozidima koji dozvoljavaju konekcije isključivo sustavima sa određenim TCP/IP stogom.

3.3. Pcap filtriranje

U većini slučajeva, rezultati skeniranja sadrže mnoštvo beskorisnih podataka koje je moguće zanemariti. Takva gomila podataka beskorisno odvraća pozornost korisnika i često rezultira previdom važnih podataka. Unicornscan podržava PCAP filtriranje izlaznih podataka, što omogućuje generiranje preglednih izvještaja.
Filtar se uključuje opcijom `-P` iza koje se navodi PCAP niz koji definira ponašanje filtra. Tako će na primjer opcija `-P not host 192.186.0.3` iz skeniranja izbaciti sve rezultate koji se odnose na poslužitelj sa IP adresom 192.168.90.3.
Više podataka o definiranju PCAP filtara može se pronaći na adresi http://www.tcpdump.org/tcpdump_man.html.
Izlazne podatke je također moguće pohraniti u PCAP formatu, u proizvoljnu datoteku. Pohranjene datoteke kasnije je moguće analizirati raznim alatima koji podržavaju ovakav tip zapisa.

4. Alicorn Web sučelje

Kako bi se olakšao rad sa Unicornscan alatom i omogućilo udaljeno pokretanje testova sa bilo kojeg računala koje posjeduje Web preglednik i vezu na Internet, kreirano je specijalizirano Web bazirano sučelje sa podrškom za relacijsku bazu podataka, nazvano Alicorn. Osim što olakšava postupak pokretanja testova, Alicorn sadrži i sučelje za usporedbu rezultata skeniranja.

4.1. Instalacija

Za ispravan rad Alicorn programom potrebno je na sustav instalirati odgovarajuću inačicu Unicorscan alata (trenutno 0.4.2) s uključenom podrškom za baze podataka i sljedeće programe:

- apache-1.3.31
- mod_ssl-2.8.18
- libmcrypt-2.5.7
- mhash-0.8.18
- PHP-4.3.7
- PostgreSQL-7.4.1

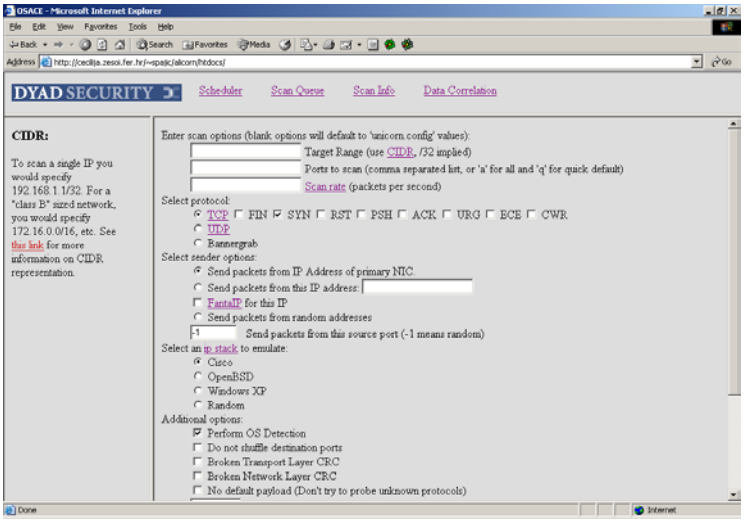
Alicorn.tar.gz paket, koji se može dohvatiti sa adrese http://www.dyadsecurity.com/s_unicornscan.html, potrebno je otpakirati u korijenski direktorij apache poslužitelja, kako bi sučelje bilo dostupno sa udaljenog računala. Parametri za spajanje na bazu podataka i ostale postavke sučelja podešavaju se unutar `./alicorn/unicorn-lib/db_config.php` i `./alicorn/htdocs/config.php` datoteka. Ukoliko to već nije učinjeno prilikom instalacije Unicornscan programa, potrebno je kreirati odgovarajući bazu podataka i u nju učitati sadržaj `pgsql_schema.sql` datoteke.

Instalirano Web sučelje ne posjeduje vlastiti mehanizam za autentikaciju korisnika te se u tu svrhu preporučuje korištenje odgovarajućih direktiva Apache poslužitelja. Preporučuje se ograničavanje pristupa samo sa određenih IP adresa i samo za određene korisnike, kako bi se na taj način spriječilo neovlašteno korištenje programa.

Budući da je Alicorn program još u razvojnoj fazi, postoji mogućnost (ovisno o sustavu) da će za ispravan rad sučelja biti potrebno napraviti određene izmjene u php kodu stranica.

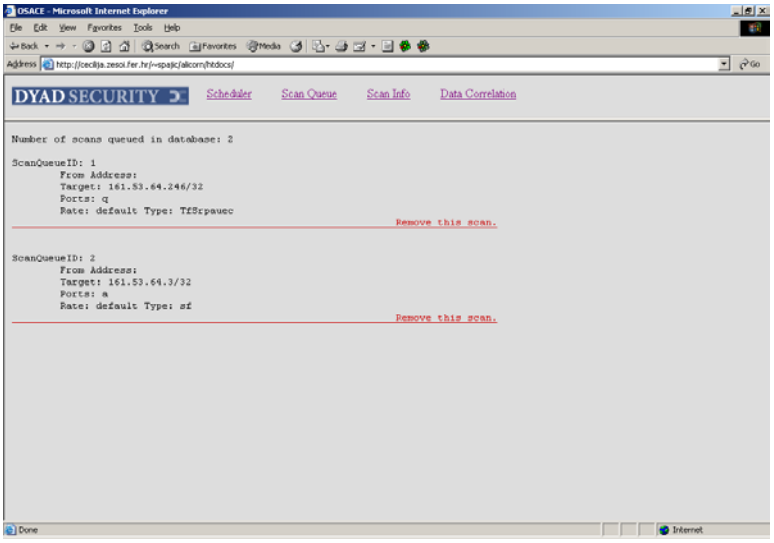
4.2. Korištenje Alicorn programa

Glavni prozor Alicorn programa (Slika 2) podijeljen je u tri okvira. Gornji okvir služi za navigaciju kroz program, a odabirom ponuđenih hiperlinkova, korisnik se prebacuje između sučelja za pokretanje skeniranja te pregled i usporedbu rezultata. Desni okvir služi kao pomoć korisniku i prikazuje opis pojedinih opcija skeniranja, ovisno o odabranoj opciji u lijevom okviru.



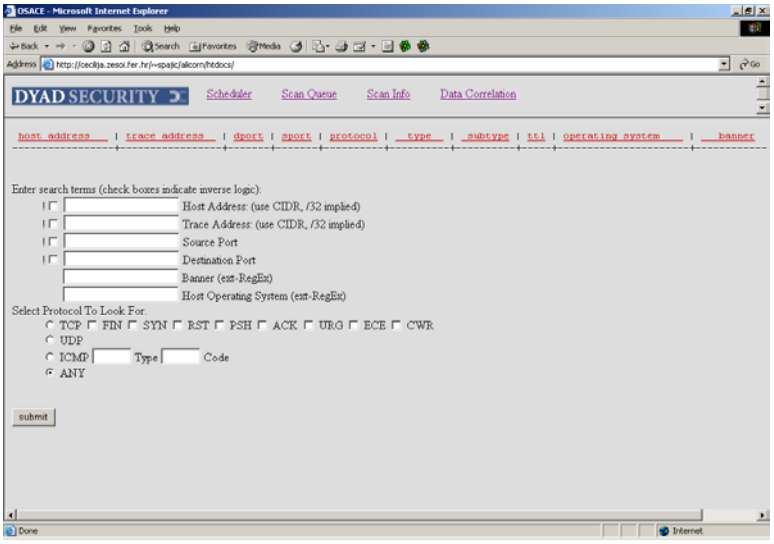
Slika 2: Glavni prozor Alicorn Web sučelja

Sučelje za definiranje parametara postupka skeniranja odabire se pomoću veze '**Scheduler**', a skeniranje se definira tako da se u odgovarajuće forme u sučelju upišu željene vrijednosti parametara skeniranja. Kada su opcije skeniranja podešene, klikom miša na gumb **Submit**, skeniranje se zakazuje i njegov status moguće je pratiti u '**Scan_Queue**' prozoru (Slika 3). Ukoliko neki od parametara nije definiran, koristiti će se uobičajene vrijednosti definirane unutar `unicorn.conf` konfiguracijske datoteke.



Slika 3: Scan Queue prozor

Sučelje za usporedbu rezultata skeniranja (Slika 4), do kojeg se dolazi pomoću veze '**Data_Correllation**', korisniku nudi brojne mogućnosti za pronalaženje zajedničkih točaka dvaju skeniranja. Rezultati se mogu uspoređivati prema izvorišnim i ciljnim IP adresama, izvorišnim i ciljnim mrežnim portovima, protokolima, itd.



Slika 4: Sučelje za usporedbu rezultata skeniranja

5. Zaključak

Kada se sagleda broj alata slične namjene trenutno dostupan na tržištu, nameće se logično pitanje, zašto uopće pokretati projekte kao što je Unicornscan. Kao što je u uvodu spomenuto, Unicornscan je alat namijenjen stručnjacima za ispitivanje sigurnosti i testiranje rada računalnih mreža i poslužitelja i kao takav sadrži određene specifične funkcije koje kod drugih alata manjkaju.

Glavna odlika ovog alata je vrlo precizno skeniranje UDP portova, koje objedinjuje funkcije nekoliko pojedinačnih alata i omogućuje precizno određivanje otvorenih portova i identifikaciju servisa. Uz to, Udpscan je i vrlo skalabilan alat, koji sa odabirom brzine slanja paketa (više od 40,000 paketa u sekundi) omogućuje relativno brzo skeniranje velikih računalnih mreža i olakšava radnje kao što su dohvat poruka koje servisi prijavljuju prilikom izravnog spajanja na portove.

Ipak, unatoč svim dobrim stranama, Unicornscan je softver koji je trenutno u vrlo ranoj razvojnoj fazi i kao takvoga ga treba koristiti s oprezom. Mnoge funkcionalnosti nisu temeljito testirane i mogu se ponašati nepredviđeno, stoga nije poželjno koristiti ovaj alat u produkcijskim (sigurnosno osjetljivim) okruženjima.