HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

SQL Recon

CCERT-PUBDOC-2005-04-116

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

Baze podataka vrlo su često jedan od najkritičnijih dijelova informacijskog sustava budući da se u njima pohranjuju različite informacije, najčešće od velikog poslovnog značaja. To mogu biti financijski podaci, zapisi o klijentima, poslovne tajne i razne druge informacije, što baze podataka svakako čini jednim od najzanimljivijih meta za potencijalne napadače, bez obzira da li se radi o napadima s javnog Interneta ili sa interne računalne mreže.

Napade na baze podataka moguće je provoditi na različite načine, korištenjem raznih posrednih i neposrednih metoda kao što su npr. iskorištavanje ranjivosti u operacijskim sustavima na kojima su pokrenute, iskorištavanjem ranjivosti u aplikacijama koje pristupaju bazama podataka, lošim podešavanjem prava pristupa, napadima umetanjem SQL koda (eng. *SQL injection*), iskorištavanjem propusta u samim bazama i sl. Zbog svih tih mogućnosti kompromitacije te važnosti koje baze podataka imaju, vrlo je važno voditi računa o njihovoj sigurnosti te imati potpunu kontrolu nad njima.

SQL Server, odnosno SQL Desktop Edition (MSDE) su Microsoftove baze podataka koje predstavljaju konkurenciju Oracle, MySQL, PostgreSQL, DB2 i drugim bazama. U zadnjih nekoliko godina upravo su SQL Server, odnosno MSDE bili česte mete napada, a jedan od najpoznatijih incidenata svakako je onaj izazvan širenjem poznatog SQL Slammer mrežnog crva koji je ugrozio iznimno velik broj informacijskih sustava na Internetu. Također, poznati su i brojni drugi sigurnosni propusti unutar navedenih programskih paketa koji su neovlaštenim korisnicima omogućavali provođenje različitih malicioznih aktivnosti. Upravo je iz tog razloga mrežnim administratorima i sigurnosnim stručnjacima u Microsoft baziranim okruženjima vrlo važno da imaju potpunu kontrolu nad svim SQL Server poslužiteljima i MSDE instancama pokrenutim na računalnoj mreži.

SQL Recon je besplatni alat tvrtke SpecialOps Security (http://www.specialopssecurity.com) koji služi za aktivnu i pasivnu detekciju Microsoft SQL Server i MSDE instanci baza podataka korištenjem svih poznatih metoda njihove detekcije. Trenutno dostupna inačica je 1.0, a može se dohvatiti s Web stranica proizvođača.

U nastavku ovog dokumenta opisan je postupak instalacije SQL Recon alata, njegova konfiguracija i ponašanje pri radu.

2. Instalacija

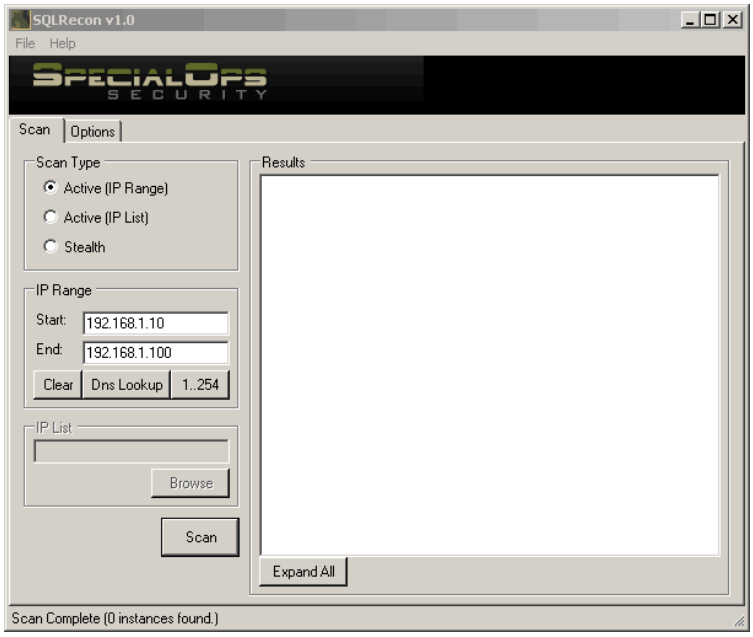
Instalacija alata SQL Recon 1.0 vrlo je jednostavna. Alat je potrebno dohvatiti s referentne lokacije (http://www.specialopssecurity.com/labs/sqlrecon/1.0/down.php), a ovisno o tome da li je na ciljnom računalu instaliran .NET Framework v1.1, moguće je dohvatiti inačicu koja funkcionira sa ili bez .NET Framework okruženja.
Nastavak instalacije provodi se pokretanjem instalacijske datoteke, prihvaćanja uvjeta licence i odabira direktorija u kojem će SQL Recon pohraniti svoje datoteke.

3. Konfiguracija

Rad s alatom i njegova konfiguracija također su vrlo jednostavni. GUI sučelje alata podijeljeno je u dvije kartice:
- *Scan* i
- *Options*.

3.1. Načini skeniranja

Kartica *Scan* sadrži parametre pomoću kojih je moguće odrediti opseg skeniranja (*Slika 1*). Moguće je odabrati dva aktivna i jedan pasivni način skeniranja.
Aktivna skeniranja mogu se provoditi navođenjem područja IP adresa (eng. *IP range*), gdje SQL Recon predefinirano odabire lokalne mrežne postavke koje je moguće promijeniti ručnim unosom ili korištenjem liste IP adresa pohranjene u tekstualnoj datoteci (eng. *IP list*). Uvjetni nedostatak aktivnih skeniranja jest da će takva skeniranja gotovo sigurno biti zabilježena ukoliko na mreži postoje sustavi za detekciju neovlaštenih aktivnosti (*host based* IDS ili *network based* IDS).
Pasivni način skeniranja uklanja ovaj nedostatak, pa se kod SQL Recon paketa ujedno naziva i "nevidljivi" način rada (eng. *stealth*). Nevidljivi način rada koristi indirektne metode pronalaženja instanci SQL Server poslužitelja, o čemu će više riječi biti u nastavku dokumenta.
Drugi dio *Scan* kartice služi za pregled rezultata skeniranja, što će također biti detaljnije opisano u nastavku.

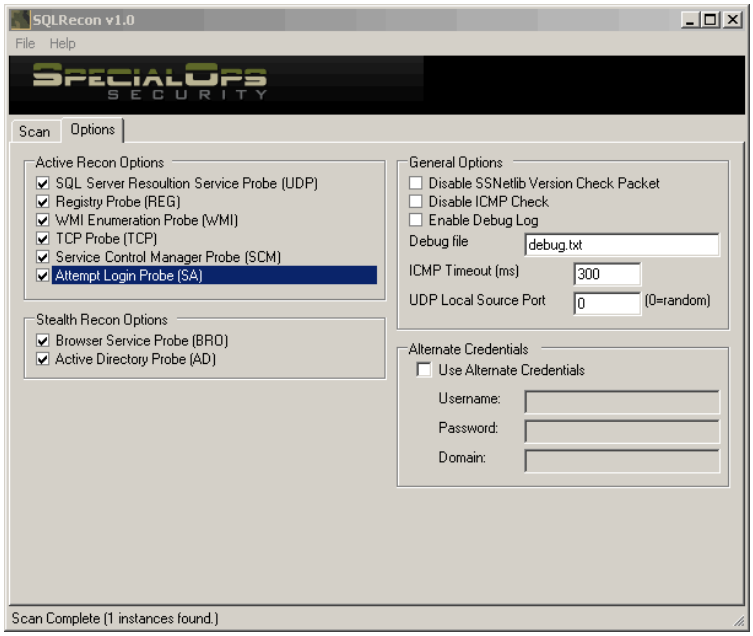


Slika 1: Podešavanje načina skeniranja i odabir IP adresa

3.2. Podešavanje parametara skeniranja

Kartica *Options* omogućava podešavanje parametara skeniranja. Kartica je podijeljena u četiri dijela:

- *Active Recon Options* – služi za podešavanje parametara aktivnih skeniranja,
- *Passive Recon Options* – služi za podešavanje parametara pasivnog skeniranja,
- *General Options* – služi za podešavanje općih parametara i opcionalno podešavanje alternativnih korisničkih podataka.



Slika 2: Podešavanje parametara skeniranja

Podešavanje parametara aktivnih skeniranja podrazumijeva uključivanje ili isključivanje sljedećih načina aktivnog skeniranja:

SQL Server Resolution Service Probe (UDP) –temelji se na standardnoj "SQL ping" detekciji slanjem UDP paketa na port 1434 udaljenog računala.

Registy Probe (REG) –provjerava *registry* datoteku udaljenog računala i traži instance SQL Server poslužitelja. *Registry probe* zasad radi samo s predefiniranim (eng. *default*) inačicama SQL Server poslužitelja i zahtijeva administrativne ovlasti na udaljenom računalu.

WMI Enumeration Probe (WMI) – koristi WMI (eng. *Windows management instrumentation*) upite za detekciju instanci SQL Server poslužitelja. Pouzdani rezultati ovog načina skeniranja mogu se dobiti jedino uz administrativne ovlasti na udaljenom računalu.

TCP Probe (TCP) – koristi standardno skeniranje TCP portova 1433 (predefinirani port za SQL Server i MSDE instance) i 2433 (predefinirani SQL Server port ukoliko je na poslužitelju uključena "*hide server*" mrežna opcija).

Service Control Manager Probe (SCM) – za skeniranje koristi se *Service control manager* servis na udaljenom računalu. Za ovu vrstu skeniranja potrebne su korisničke ovlasti na udaljenom računalu.

Attempt Login Probe (SA) – za razliku od ostalih vrsta skeniranja, koja detekciju SQL Server ili MSDE instanci provode isključivo na temelju odgovarajućih odgovora udaljenih računala, ova metoda skeniranja uključuje i pokušaj prijave na udaljenu instancu korištenjem predefiniranog "SA" korisničkog računa. Ovakav način skeniranja funkcionira u slučajevima kad ostale metode ne daju očekivane rezultate.

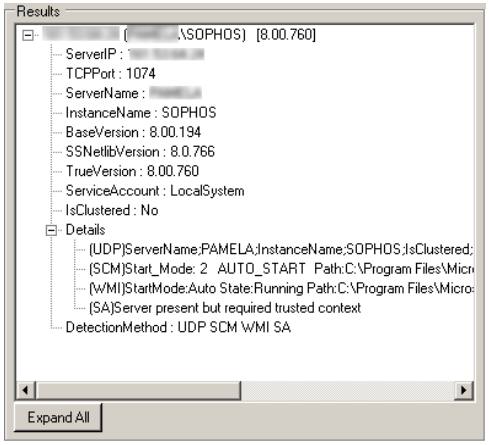
Podešavanje parametara pasivnog skeniranja podrazumijeva sljedeće opcije:

Browser Service Probe (BRO) – provjerava Browser Service servis udaljenog računala. Iako ne daje detaljne rezultate, ovo skeniranje može biti korisno za neopaženo otkrivanje instanci SQL Server poslužitelja.

Active Directory Probe (AD) – šalje upite *Active Directory* servisu i traži registrirane instance SQL Server poslužitelja. Pošto registracija SQl Server poslužitelja unutar *Active Directory*-ja nije obvezna, ovaj način skeniranja otkriti će samo registrirane SQL Server poslužitelje. Također, za korištenje ovog načina skeniranja potrebne su korisničke ovlasti na ciljnoj domeni.
Podešavanje općih parametara uključuje podešavanje onih postavki koje skeniranje mogu učiniti efikasnijim:
Disable SSNetlib Version Check Parent – isključuje provjeru inačice `SSNEtlib.dll` (sučelje SQL Server *engine-a* prema protokolima nižih slojeva) biblioteke. Isključivanje ove opcije može umanjiti opasnost od generiranja upozorenja od strane IDS sustava.
Disable ICMP check – isključuje korištenje ICMP provjera udaljenih računala. Isključivanje ove opcije pomaže kod računala koja blokiraju ICMP pakete, no može značajno usporiti rad SQL Recon alata.
Enable Debug Log – omogućava generiranje log zapisa u cilju detaljne provjere odgovora koje SQL Recon program dobiva prilikom skeniranja.
ICMP Timeout – omogućava podešavanje vremena koliko će SQL Recon čekati ICMP odgovor udaljenog računala. Na brzim lokalnim mrežama s velikim brojem računala smanjivanje ove vrijednosti može ubrzati rad, dok se kod sporih modemskih veza preporuča podizanje njene vrijednosti.
UDP Source Port – omogućava ručno podešavanje izvorišnog porta s kojeg će se šalju paketi za skeniranje. Na ovaj način nekad je moguće zaobići vatrozide koji filtriraju pakete (npr. podešavanjem *source* porta na UDP 53).
Alternate Credentials – omogućava podešavanje alternativnih korisničkih informacija. Podešavanje tih parametara koristi se obično kod skeniranja koja zahtijevaju ovlasti na udaljenim računalima ili na ciljnoj domeni.

4. Rad

Nakon što je konfiguracija podešena, moguće je, pritiskom na gumb *Scan*, kartice *Scan* pokrenuti skeniranje. Ovisno o broju IP adresa koje su uključene u skeniranje, konfiguraciji mreže i ICMP postavkama, sam proces skeniranja može trajati dulje ili kraće.
Po završenom skeniranju u desnom dijelu prozora kartice *Scan* pojavit će se sve detektirane SQL Server ili MSDE instance. Odabirom bilo koje od njih moguće je pregledati detaljne informacije o detektiranoj instanci, isto kao i načine skeniranja koji su bili uspješni.



Slika 3: Pregled informacija od detektiranoj SQL Server (MSDE) instanci

Dobivene rezultate moguće je pohraniti za kasniju analizu (izbornik *File -> Save -> Full Report*), a moguće je korištenje i pomoći pri radu (izbornik *Help*), pri čemu je potrebno biti povezan na Internet, budući da *Help* naredba otvara Web stranicu na adresi http://www.specialopssecurity.com/labs/sqlrecon/1.0/doc.php.
Općenito, rad SQL Recon-a je pouzdan, a nisu uočeni nikakve nestabilnosti niti problemi pri radu, što je ponekad uobičajeno kod alata ovog tipa. Ukoliko se za detekciju SQL Server i MSDE instanci koriste metode koje ne podrazumijevaju korisničke ili administrativne ovlasti, u nekim slučajevima je moguće

da detekcije neće biti pozitivne, no u većini slučajeva alat daje zadovoljavajuće rezultate. Mali nedostatak alata jest dosta ograničen način odabira IP adresa.

5. Zaključak

SQL Recon vrlo je jednostavan i praktičan alat za detekciju SQL Server i MSDE instanci, koji mrežnim administratorima može znatno olakšati održavanje svojih sustava te detekciju nelegitimno pokrenutih servisa. Alat također može pomoći i sigurnosnim stručnjacima prilikom ispitivanja sigurnosti informacijskih sustava, budući da su navedeni programski paketi poznati po brojnim ranjivostima koje su omogućavale neovlašteni pristup sustavu. Program podržava brojne metode detekcije SQL Server i MSDE instanci, a također je moguće i podešavanje parametara kojima je moguće zaobići postavke vatrozida ili detekciju od strane sustava za detekciju neovlaštenih aktivnosti.

Iako korištenje alata ne garantira uspješnu detekciju svih SQL Server i MSDE instanci na mreži, na temelju provedenih testiranja može se zaključiti kako se radi o vrlo korisnom i perspektivnom alatu.