HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Nessus alata

CCERT-PUBDOC-2007-01-181

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

U vrijeme kada je potrebno voditi sve više računa o sigurnosti na Internetu zbog velikog broja zlonamjernih korisnika, korištenje alata za provjeru ranjivosti postalo je učestalo u velikom broju organizacija. Provjera ranjivosti (eng. *vulnerability scanning*) je postupak koji se provodi u svrhu određivanja sigurnosnih nedostataka, a potom i uklanjanja tih propusta u informacijskim, odnosno računalnim sustavima. Postupci kojima se obavlja provjera identični su onima koje napadači koriste kod zlonamjernih aktivnosti, a na temelju izvješća nakon izvođenja tih postupaka određuju se koraci potrebni za otklanjanje sigurnosnih nedostataka. Jedan od alata iz ove skupine je i Nessus. Na početku razvoja alat je bio namijenjen isključivo Linux operacijskim sustavima, ali se s vremenom pokazala potreba za prilagodbom na ostale značajnije operacijske sustave kao što su, primjerice, Windows i BSD operacijski sustavi.

Aplikacije za provjeru ranjivosti primjenjuju se na osobnim računalima i, mnogo učestalije, nad računalnim mrežama, pri čemu se podrazumijeva provjera prisutnih poslužitelja, web stranica, usmjerivača (eng. *router*) i vatrozida (eng. *firewall*). Najčešće ih se svrstava u dvije skupine:

- analizatore koji su usmjereni na pretragu ranjivosti u okviru registra računala (eng. *registry*) i konfiguracijskih datoteka te
- alate koji pokušavaju iskoristiti ranjivost tražeći ju na svakom od elemenata mrežne infrastrukture.

Nessus pripada drugoj skupini alata. Na tržištu je dostupan velik broj sličnih alata koji omogućuju provjeru ranjivosti udaljenih i lokalnih računala. Nessus nosi titulu vodećeg alata na ovom području, a dodatna prednost mu je i besplatno korištenje. Mogućnosti i performanse ove aplikacije nadmašuju brojna druga komercijalna rješenja visokih cijena. Velik broj korisnika sudjeluje u razvoju paketa, tako da je omogućeno i redovito osvježavanje popisa ranjivosti, odnosno stvaranje modula za ispitivanje novih sigurnosnih propusta.

2. Općenito o Nessus paketu

Programski paket Nessus distribuira se pod GPL licencom, što znači da je riječ o besplatnom paketu otvorenog programskog koda. Namijenjen je administratorima za provjeru postojanja sigurnosnih ranjivosti. Njihovo pravovremeno uočavanje i ispravljanje neophodno je ako se zlonamjernog korisnika želi spriječiti u njihovom iskorištavanju.

Važnije značajke Nessus paketa su:

- arhitektura poslužitelj-klijent,
- baza modula za provjeru ranjivosti koja se redovito osvježava novim modulima,
- udaljena detekcija propusta (iskoristivih lokalno, ali i udaljeno),
- podrška za korištenje sigurnosne komunikacije (SSL),
- dobro korištenje resursa bez obzira radi li se i slabijem računalu ili, na primjer, višeprocesorskom računalu s velikim količinama raspoložive memorije,
- posebno razvijen skriptni jezik NASL (eng. *Nessus Attack Scripting Language*) kojim se opisuju propusti i izrađuju testovi za pojedine ranjivosti,
- moduli za provjeru ranjivosti razvijeni NASL skriptnim jezikom mogu se jednostavno analizirati budući da su dostupni u obliku čitljivom čovjeku,
- prepoznavanje usluga se obavlja inteligentnom metodom – ne pretpostavlja se određena usluga prema broju priključka (eng. *port*); IANA (eng. *Internet Assigned Numbers Authority*) standard, npr. aktivan priključak 21 ne mora podrazumijevati FTP uslugu,
- predviđeno postojanje više istovjetnih usluga na jednom računalu (određeni broj sličnih aplikacija to ne podrazumijeva),
- postojanje dva načina provjere: sigurnosne i potpune pri čemu sigurnosna ne ugrožava provjeravano računalo, dok potpuna može pregledavano računalo dovesti u DoS (eng. *Denial of Service*) stanje – stanje uskraćivanja resursa, te
- postojanje velike baza korisnika - procjenjuje se da oko 75 000 organizacija u svijetu koristi ovaj paket.

Pregled ranjivosti sastoji se od tri koraka

1. Pregled (snimanje, eng. *scanning*) - obuhvaća detekciju uključenih računala odnosno aktivnih IP adresa u zadanom mrežnom segmentu. Pregled se obavlja odašiljanjem ICMP *echo-request* paketa. Pritom se računala koja ne odgovaraju ne smatraju nepostojećima, jer su možda osigurana vatrozidom. Opisanom tehnikom stvara se popis odredišta koja će se koristiti u sljedećem koraku sigurnosne provjere.
2. Pregled mrežnih usluga odnosno servisa koji se izvode na provjeravanim računalima. Ovim se korakom dolazi do pozdravnih poruka čijom se analizom pokušava odrediti operacijski sustav ciljnog računala. Ovisno o provjeravanoj usluzi, moguće je i korištenje tzv. *brute force* napada iscrpljivanjem velikog broja korisničkih imena i zaporki za pokušaj uspješne autentikacije.
3. Određivanje ranjivosti prema zadanim specifikacijama u modulima. U ovom koraku provjeravaju se potencijalni sigurnosni propusti udaljenih servisa kao što su nedovoljna provjera ulaznih parametara, nepravilne postavke usluge, pogreške prepisivanja spremnika i brojne druge vrste sigurnosnih ranjivosti.

Iako tvrtka Tenable distribuira Nessus pod GPL licencom, licence njegovih modula su dvojake. Postoje licence za preuzimanje modula pod nazivom *Registered Feed* i *Direct Feed*. Potonja vrsta licence se plaća i preporuča većim tvrtkama ili organizacijama. Ona donosi promptnu tehničku podršku, pristup zaštićenom dijelu web portala, priključke vezane uz provjeru sigurnosnih standarda i preuzimanje najnovijih modula odmah po njihovom objavljivanju. *Registered* licenca donosi module sa zadrškom od sedam dana od trenutka njihovog izdavanja i ne obuhvaća sve prethodno navedene povlastice.

3. Nessus poslužitelj

Poslužitelji su razvijeni dvojako. Za Windows i Mac OS X operacijske sustave klijent i poslužitelj dio su istog paketa te se instaliraju nužno jedan s drugim. Za ostale podržane operacijske sustave poslužitelj i klijent odvojene su aplikacije te se shodno tome, zasebno i instaliraju. Slijedi opis instalacije i

pokretanja poslužitelja za Linux odnosno Unix operacijske sustave. Windows poslužitelj opisan je zajedno s pripadnim klijentom.

3.1. Nadogradnja, instalacija i pokretanje Linux/Unix poslužitelja

Nessus poslužitelj za Unix, Linux i Mac OS X operacijske sustave razvijen je u obliku pozadinske aplikacije (eng. *daemon*). Instalacija započinje preuzimanjem odgovarajućeg paketa s web stranice proizvođača u ovisnosti o korištenom operacijskom sustavu. Budući da je niz podržanih operacijskih sustava velik, u ovom poglavlju je opisan postupak instalacije za Fedora Core 6 i Debian 3.1 operacijske sustave. Postupci za ostale inačice Fedora Core sustava i za Linux Red Hat te SuSE sustave slični su onima opisanim za FC6, a u nastavku teksta izraz FC će se koristiti za sve navedene sustave iz te skupine. Dodatno, radi jezgrovitosti će primjeri naredbi za FC sustave imati početnu oznaku u obliku

```
FC#
```

dok će primjeri naredbi za Debian sustave imati naredbenu početnu oznaku oblika

```
Debian#
```

Instalacijska procedura značajno je pojednostavljena korištenjem specijaliziranih alata za ovu namjenu poput *apt-get* (Debian) i *yum* (FC, RH, SuSE). Za Windows operacijske sustave i klijent i poslužitelj dolaze u istom paketu te nisu razdvojivi poput inačica za ostale sustave.

3.1.1. Nadogradnja

Nadogradnja je istovjetna instalaciji osim što zahtijeva prekid rada stare, aktivne inačice pozadinske aplikacije *nessusd* naredbom

```
# killall nessusd
```

što će zaustaviti i sve aktivne provjere sigurnosnih ranjivosti. Nadogradnja sustava obavlja se naredbom:

```
FC# rpm –Uvh <ime_nove_inacice>
Debian# dpkg –i <ime_nove_inacice>
```

Pokretanje pozadinske aplikacije jednako je za obje opisane skupine sustava:

```
FC&Debian# /opt/nessus/sbin/nessusd –D
```

Slijedećim ispisom prikazan je približan izgled procedure nadogradnje:

```
# killall nessusd
# rpm -Uvh Nessus-3.0.5-es3.i386.rpm
Preparing...           ########################################### [100%]
Shutting down Nessus services:
   1:Nessus            ########################################### [100%]

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
 - Please run /opt/nessus/sbin/nessus-add-first-user to add an admin user
 - Register your Nessus scanner at http://www.nessus.org/register/ to
   obtain all the newest plugins
-  You can start nessusd by typing /sbin/service nessusd start

# /opt/nessus/sbin/nessusd -D
nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
```

Po završetku nadogradnje osvježava se popis informacija o sigurnosnim ranjivostima.

3.1.2. Instalacija

Ukoliko korisnik nije prethodno imao instaliran Nessus paket na svom računalu, primjenit će postupak instalacije koji je vrlo sličan prethodno pojašnjenom postupku nadogradnje. Primjeri su dani za instalaciju najnovijih inačica paketa u trenutku pisanja dokumenta – Nessus 3.0.5.

```
FC# rpm –ivh Nessus-3.0.5-fc6.i386.rpm
Debian# dpkg –i Nessus-3.0.5-debian3_i386.deb
```

Programski paket bit će instaliran u `/opt/nessus/` direktorij. Kao i kod nadogradnje, i u ovom će se slučaju na koncu instalacije obaviti postupak osvježavanja popisa sigurnosnih ranjivosti.
Po završetku instalacijske procedure slijedi inicijalna konfiguracija poslužitelja. Osim toga, potrebno je stvoriti barem jedan korisnički račun kako bi klijentske aplikacije poput NessusWX i Tenable Security Center mogle pristupiti poslužitelju i koristiti ga za pokretanje provjere ranjivosti i dohvat rezultata provjera. Na početku se koristi naredba `nessus-add-user-first` za dodavanje prvog korisnika i obavljanje autentikacije korištenjem zaporke. Sljedeći ispis pokazuje proceduru dodavanja prvog korisnika.

```
# /opt/nessus/sbin/nessus-add-first-user
nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

Using /var/tmp as a temporary file holder

Add a new nessusd user
----------------------


Login : admin
Authentication (pass/cert) [pass]:
Login password:
Login password (again):

User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that admin has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)


Login      :admin
Password      :********
DN        :
Rules       :


Is that ok ? (y/n) [y]
User added.
Thank you. You can now start Nessus by typing:
/opt/nessus/sbin/nessusd -D
```

Ostale korisnike može se dodati korištenjem naredbe `nessus-adduser`. Obje se datoteke nalaze u direktoriju `/opt/nessus/sbin/`. Korisnike se može dodati i naredbom za stvaranje sigurnosnih potvrda (eng. *certificate*) jer se na taj način mogu precizirati određeni podaci o korisniku. Naredba kojom se stvara potvrda je `nessus-mkcert-client`. Naziv datoteke sa svim podacima počinje nizom "`cert_nessuswx_`", nastavlja se imenom korisnika te završava ekstenzijom "`.pem`". Primjerice, za korisnika s nazivom "korisnik" stvoriti će se datoteka imena "`cert_nessuswx_korisnik.pem`". Čitav postupak prikazan je na sljedećem ispisu. Iz ispisa su izbačeni neki nevažni odsječci radi preglednosti.

```
Debian# nessus-mkcert-client
Do you want to register the users in the Nessus server
as soon as you create their certificates ? (y/n): y
This script will now ask you the relevant information to create the SSL
client certificates for Nessus.
Client certificates life time in days [365]:730
Your country (two letter code) [HR]:
Your state or province name [none]: Grad Zagreb
Your location (e.g. town) [Paris]: Zagreb
Your organization [none]: FER
Your organizational unit [none]:LSS
**********
We are going to ask you some question for each client certificate
If some question has a default answer, you can force an empty answer by
entering a single dot '.'
*********
```

```
User #1 name (e.g. Nessus username): mojkorisnik
Client certificates life time in days [730]:
Country (two letter code) [HR]:
State or province name [Grad Zagreb]:
Location (e.g. town) [Zagreb]:
Organization [FER]:
Organization unit [LSS]:
e-mail []: mojkorisnik@lss.fer.hr
Generating RSA private key, 1024 bit long modulus
........++++++
..............++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [FR]:State or Province Name (full name)
[Some-State]:Locality Name (eg, city) []:Organization Name (eg, company)
[Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section)
[]:Common Name (eg, your name or your server's hostname) []:Email Address
[]:Using configuration from/tmp/nessus-mkcert.4653/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'HR'
stateOrProvinceName   :PRINTABLE:'Grad Zagreb'
localityName          :PRINTABLE:'Zagreb'
organizationName      :PRINTABLE:'FER'
organizationalUnitName:PRINTABLE:'LSS'
commonName            :PRINTABLE:'mojkorisnik'
emailAddress          :IA5STRING:'mojkorisnik@lss.fer.hr'
Certificate is to be certified until Jan 20 22:16:30 2009 GMT (730 days)
Write out database with 1 new entries
Data Base Updated
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that  has the right to test. For instance, you may want
him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax
Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
User added to Nessus.
Another client certificate? n
Your client certificates are in /tmp/nessus-mkcert.4653
You will have to copy them by hand
```

Inicijalno nisu postavljena pravila o tome koje mrežne segmente korisnik smije provjeravati u svrhu pronalaska sigurnosnih propusta. Pri završetku dodavanja korisnika kao i na završetku stvaranja sigurnosnih potvrda, moguće je unijeti odgovarajuća pravila ukoliko je to potrebno. Slijedi primjer nekoliko pravila:

```
accept 192.168.1.0/24
default deny
```

Nešto naprednije postavljanje određenih svojstava poslužitelja može se izvesti izmjenama unutar konfiguracijske datoteke `/opt/nessus/etc/nessus/nessusd.conf`. Moguće je odrediti najveći broj provjeravanih računala u jednom trenutku, resurse koje se daje poslužitelju na raspolaganje i još brojne druge postavke.

Slijedi pokretanje poslužitelja, a na ispisu je prikazan primjer pokretanja na Fedora sustavu:

```
FC# /opt/nessus/sbin/nessusd -D

nessusd (Nessus) 3.0.5 for Linux
(C) 2005 Tenable Network Security, Inc.

Processing the Nessus plugins...
[##################################################]

All plugins loaded
```

Radi cjelovitosti slijede naredbe za pokretanja poslužitelja na ostalim operacijskim sustavima:

```
FC&RedHat# /sbin/service nessusd start
SuSE# /etc/rc.d/nessusd start
Debian# /etc/init.d/nessusd start
```

Zaustavljanje se izvodi jednom od naredbi:

```
# killall nessus
Debian# /etc/init.d/nessusd stop
```

Korisnici Security Center alata ovime završavaju postupak instalacije budući da se ostale postavke mogu obaviti korištenjem te aplikacije.

3.1.3. Napredno podešavanje poslužitelja

Ukoliko je potrebno, prilikom pokretanja poslužitelja, mogu se navesti određeni parametri u naredbenom retku:

- `-c <konfiguracijska_datoteka>` čime se određuje datoteka iz koje će poslužitelj učitati postavke,
- `-a <IP_adresa>` određuje IP adresu na kojoj poslužitelj očekuje konekcije,
- `-S <ip[, ip2, …]>` određuje izvorne adrese uspostavljenih veza koje korisnik želi koristiti umjesto podrazumijevane,
- `-p <broj_priključka>` određuje na kojem priključku program očekuje pokušaj uspostave veze (podrazumijevana vrijednost je 1241),
- `-D` uključuje aplikaciju kao pozadinsku (eng. *daemon*),
- `-v` ispisuje inačicu poslužitelja,
- `-h` ispisuje naredbe koje se mogu zadati poslužitelju.

Preostaje još unos aktivacijskog koda kojeg korisnik prima elektroničkom poštom u trenutku preuzimanja paketa s web stranica proizvođača. Zato je važno da se ispravno popune traženi podaci, posebice adresa elektroničke pošte korisnika. Unos aktivacijskog koda obavlja se izvođenjem sljedeće naredbe:

```
# /opt/nessus/bin/nessus-fetch –register <aktivacijski_kod>
```

Ispis trenutnih podataka o skupu modula koje korisnik posjeduje dobiva se naredbom:

```
cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
PLUGIN_SET = "200701050046"
PLUGIN_FEED = "Release"
```

Osvježavanje programskih priključaka (eng. *plugin*) pokreće se naredbom:

```
# /opt/nessus/sbin/nessus-update-plugins
```

Baza se osvježava svakodnevno budući da se i propusti otkrivaju na dnevnoj bazi. Postupci u slučaju kada Nessus nema osiguranu vezu na Internet su relativno jednostavni. Ukoliko korisnik nema aktivacijski kôd, na adresi http://www.nessus.org/register treba ispuniti elektronički obrazac i tek tada prima kôd na danu adresu elektroničke pošte. Naredbom

```
# /opt/nessus/bin/nessus-fetch -challenge
```

dohvaća se niz oblika

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Unutar web preglednika zatim se upisuje adresa http://www.plugins.nessus.org/offline.php te se ondje unese dobiveni niz u odgovarajuće polje. Na taj način korisniku se stvara nova URL adresa kojom može pristupiti programskim priključcima kao i datoteci `nessus-fetch.rc` koju je nakon preuzimanja potrebno kopirati u direktorij `/opt/nessus/etc/nessus/`. URL je potrebno sačuvati jer se koristi kod daljnjih osvježavanja. Sa spomenute generirane web adrese dohvaća se arhivska datoteka s priključcima koju je potrebno raspakirati na slijedeći način:

```
# tar -zxvf all-2.0.tar.gz -C /opt/nessus/lib/nessus/plugins/
```

Za svako osvježavanje informacija o ranjivostima ovaj postupak je potrebno ponoviti.

3.1.4. Uklanjanje Nessus poslužitelja

Postupak uklanjanja započinje zaustavljanjem poslužitelja:

```
FC&Debian# killall nessus
```

a nastavlja se dohvaćanjem trenutno instalirane inačice paketa:

```
FC# rpm -qa | grep Nessus
Debian# dpkg -l | grep nessus
```

Izlaz navedenih naredbi može biti npr. *Nessus-3.0.5-es3* (FC) ili *nessus* (Debian).
Zatim treba pokrenuti naredbu za uklanjanje paketa:

```
FC# rpm -e <ime_paketa_dobiveno_prethodnom_naredbom>
Debian# dpkg -r nessus
```

Dodatno, za uklanjanje datoteka koje nisu nastale instalacijom potrebno je pokrenuti naredbu:

```
FC&Debian# rm -rf /opt/nessus
```

4. Klijenti za Nessus poslužitelj

Prisutno je nekoliko klijenata za Nessus poslužitelj, a razvile su ih različite tvrtke uključujući i Tenable. U nastavku će biti opisane najvažnije klijentske aplikacije.

4.1. Nessus3 - klijent i poslužitelj za Windows operacijske sustave

Za Windows operacijske sustave klijent i poslužitelj dolaze unutar istog paketa pa će na isti način biti i opisani.

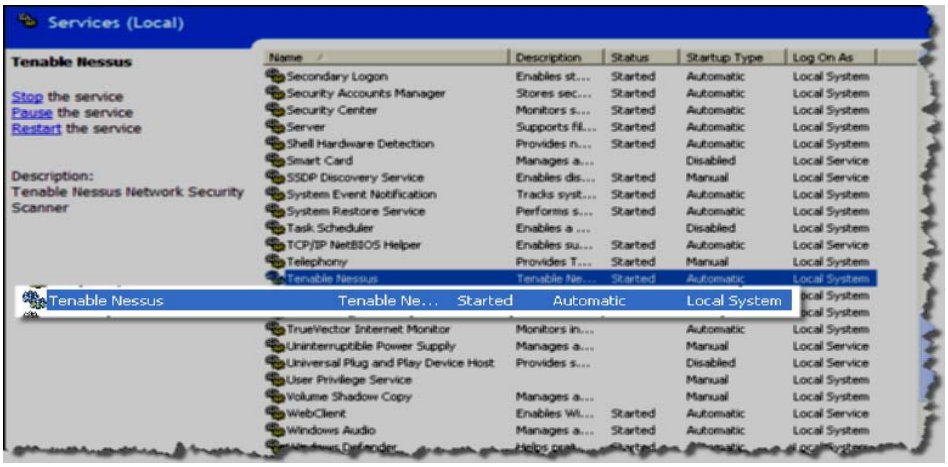
4.1.1. Nadogradnja

Postupak nadogradnje obuhvaća preuzimanje nove inačice paketa s web stranica proizvođača čija je veličina oko 15MB. Uklanjanje prethodne inačice paketa nije potrebno budući da se tijekom

instalacije nove svi postojeći podaci premještaju u odgovarajuću mapu. Korisnicima koji su prethodno koristili NeWT klijent aplikaciju, postupak nadogradnje zamjenjuje postojeću aplikaciju Nessus3 Windows klijent aplikacijom.

4.1.2. Instalacija

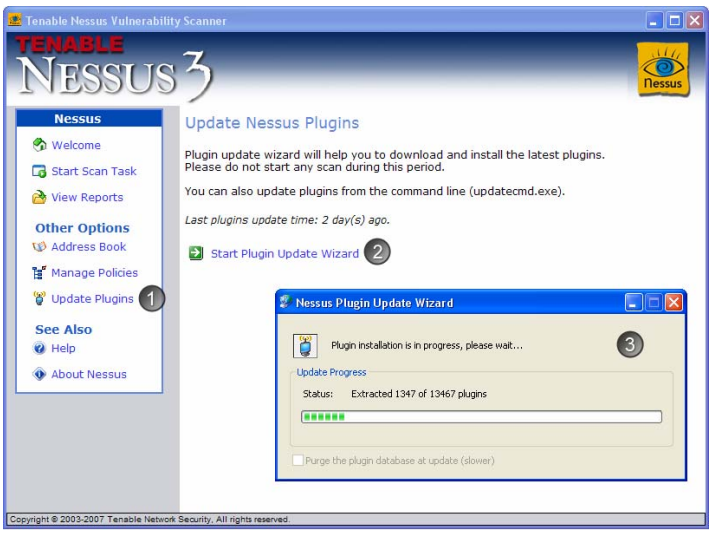
Paket se distribuira u obliku izvršne datoteke, a obuhvaća instalaciju i klijenta i poslužitelja. Na Win2000 i Win2003 sustavima, Nessus treba instalirati korištenjem administratorskog korisničkog računa. Korisnici koji su paket preuzeli s web stranica prilikom preuzimanja ispunili su obrazac u kojem su dali i svoju adresu elektroničke pošte. Na nju bi trebali primiti poruku s aktivacijskim kodom. Tako na koncu instalacije mogu odabrati unos aktivacijskog koda korištenjem *Product Registration* aplikacije. Svaka promjena aktivacijskog koda unosi se na isti način.
Na Windows operacijskim sustavima poslužitelj se instalira u obliku servisa (eng. *service*) te se inicijalno postavlja kao servis koji se automatski pokreće s pokretanjem sustava.



Slika 1: Nessus kao servis na Windows sustavima

4.1.3. Preuzimanje najnovijih modula

Za potpuno valjanu analizu potrebno je imati najnoviju listu modula ranjivosti. Nadogradnja se izvodi korištenjem Nessus klijent aplikacije i odabirom *Update Plugins* izbornika. Preuzimanje najnovijih modula se obavlja bez obzira na odabranu skupinu modula (eng. *plugin family*). Sljedeća slika prikazuje vrlo jednostavan postupak osvježavanja sačinjen od tri koraka.



Slika 2: Osvježavanje modula

Osvježavanje paketa bez Internetske veze zahtijeva nešto više truda od prethodno pojašnjenog postupka. Prvo, ukoliko to već nije obavljeno, potrebno je paket registrirati unosom podataka na stranici http://www.nessus.org/register te primanjem aktivacijskog koda porukom elektroničke pošte. Korištenjem web preglednika treba pristupiti stranici http://plugins.nessus.org/manual-register.php te unijeti dobiveni kod u odgovarajuće polje. Na taj način korisniku se osigurava URL adresa s koje može dohvatiti arhivsku datoteku s najsvježijim modulima naziva, primjerice, *all-2.0.tar.gz*. Datoteku treba otpakirati u `C:\Program Files\Tenable\Nessus\plugins\scripts` mapu. Posebnu pozornost valja obratiti na postojeći problem s automatskom pretvorbom CR/LF znakova koji se izbjegava isključenjem te mogućnosti u aplikaciji za raspakiranje arhive. Nakon toga potrebno je pokrenuti program `C:\Program Files\Tenable\Nessus\build.exe`.

4.1.4. Dodavanje korisničkih računa

Dodavanje korisničkih računa obavlja se pokretanjem *User Management* alata. Treba odabrati jedinstveno korisničko ime i postaviti željenu zaporku. Ti se korisnički računi koriste kod udaljenog pristupa poslužitelju.

Za postavljanje udaljenog pristupa koristi se alat naziva *Scan Server Configuration*. Njime je omogućeno postavljanje odgovarajuće vrijednosti na mrežno sučelje servisa. Podrazumijevana TCP/IP adresa na kojoj servis čeka veze je 127.0.0.1:1241. Za pristup s mreže potrebno je dodijeliti IP adresu odgovarajućeg mrežnog sučelja, a ukoliko se želi alatu omogućiti prisutnost na svim sučeljima, u odgovarajuće polje upisuje se 0.0.0.0 vrijednost. Indikator trenutne aktivnosti servisa poprima crvenu boju ukoliko servis nije pokrenut, odnosno zelenu ukoliko jest. Za provjeru se može pokrenuti naredba

```
C:\> netstat -an
```

unutar naredbenog retka koja prikazuje popis svih otvorenih priključaka. U popisu bi se trebao nalaziti i Nessus servis. Korisnici vatrozida (eng. *firewall*) moraju osigurati potrebne dozvole za uspostavljanje veza ukoliko koriste Nessus servis.

4.1.5. Uklanjanje paketa

Aplikaciju je najjednostavnije ukloniti preko upravljačke ploče (eng. *Control panel*) odabirom *Add or Remove programs* opcije. Potrebno je odabrati Nessus paket, a odabirom opcije *Change/Remove* pokreće se procedura za uklanjanje paketa.

4.1.6. Pokretanje provjere ranjivosti

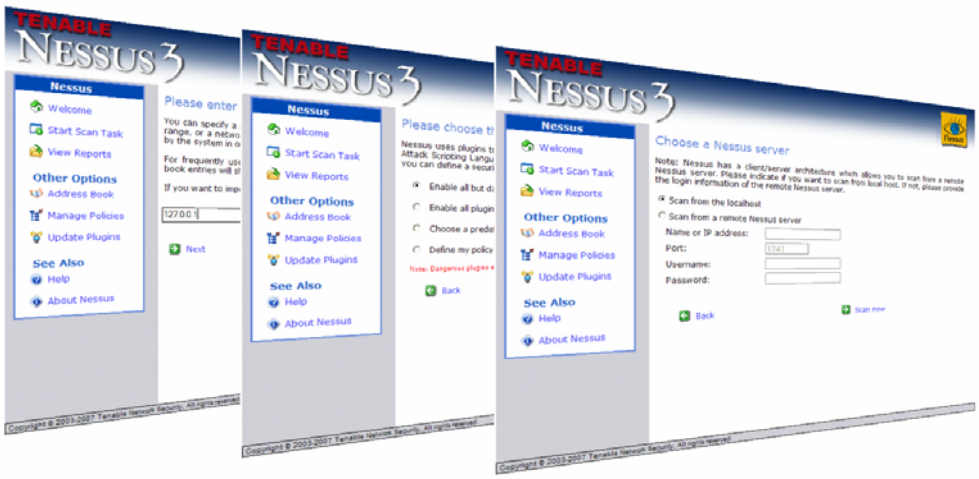
Odabirom *Start Scan Task* mogućnosti s početne stranice, pokreće se prvi korak postavki prije provjere ranjivosti. Slijedi unos IP adrese ili adrese podmreže čija je računala potrebno provjeriti, pri čemu je unos u CIDR (eng. *Classless Inter-Domain Routing*) formatu (A.B.C.D/N, gdje N određuje broj bitova podmreže) ili kao ime računala dohvatljivo korištenjem DNS usluge. Za pokretanje provjere na istom računalu na kojem je pokrenut i Nessus poslužitelj, potrebno je upisati IP adresu 127.0.0.1.

Idući korak je odabir vrste sigurnosnog pregleda, a može se odabrati jedna od mogućnosti:

- *Enable all but dangerous plugins with default settings* – pregled se obavlja samo s modulima koji nisu potencijalno opasni, isključeni su moduli za pregled DoS (eng. *Denial of Service*) ranjivosti jer zbog sličnosti provjere s pravim napadom mogu dovesti do DoS stanja.
- *Enable all plugins with default settings* – koriste se svi moduli u sigurnosnom pregledu, a potencijalna opasnost prijeti od DoS modula jer mogu onemogućiti ispravan rad pregledavanog računala.
- *Choose a predefined policy* – odabir unaprijed određenog skupa pravila pregleda.
- *Define my policy* – određivanje vlastitog skupa pravila pregleda, što je podrobnije opisano u nastavku dokumenta.

Slijedi određivanje Nessus poslužitelja kojeg će se koristiti pri sigurnosnom pregledu ranjivosti računala ili skupine računala određenih u jednom od prethodnih koraka. Moguće je odabrati pregled s lokalnog ili s udaljenog računala. Poslužitelj na udaljenom računalu mora biti inačice 3.x jer ranije inačice poslužitelja nisu podržane ovom klijent aplikacijom. Potencijalni problemi mogu nastati kod korištenja različitih vrsta pretplata (*Registered Fed*, *Direct Feed*) te je stoga za ispravno korištenje

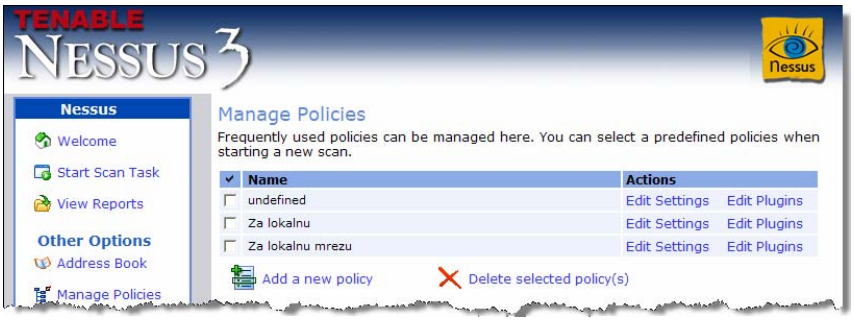
udaljenog poslužitelja potrebno imati jednake vrste pretplate te jednake module za provjeru ranjivosti na klijentu i na poslužitelju.
Preostaje odabir *Scan now* opcije nakon čega započinje sigurnosni pregled prikazan na sljedećoj slici. Sigurnosnu provjeru je moguće privremeno zaustaviti te ju naknadno nastaviti ili ju potpuno zaustaviti.



Slika 3: Pokretanje provjere ranjivosti

4.1.7. Stvaranje pravila

Odabirom *Manage Policies* poveznice korisnik može uređivati postojeća pravila ili stvarati nova. Nakon inicijalnog stvaranja potrebno je i odabrati skupine modula u ovisnosti o željenim ranjivostima koja se provjeravaju te prilagoditi različite postavke. Odabir modula izborom *Edit Plugins* poveznice omogućuje pojedinačan izbor modula kao i izbor grupe modula sa sličnim karakteristikama – skupine modula (eng. *plugin family*).
Opcija *Edit Settings* omogućava postavljanje vrlo velikog broja različitih mogućnosti raspoređenih u sedam opcija. Ovo je jedan od najvažnijih dijelova paketa i implementiran je kod svih klijentskih aplikacija na sličan način pa je detaljnije opisan u nastavku trenutnog poglavlja.



Slika 4: Ispis pravila

4.1.7.1. Opcija *General*

Omogućava uređivanje općenitih parametara vezanih uz programske priključke odnosno module. Najvažniji su pojašnjeni sljedećim popisom:

- *Safe check* – isključuje module koji mogu uzrokovati DoS stanje na pregledavanim računalima,
- *Max number of hosts* – određuje najveći broj računala koja će se istovremeno provjeravati i
- *Max number of security checks* – najveći broj modula koji će se upogoniti za pojedino pregledavano računalo (prilikom sigurnosnog pregleda računalo se može preopteretiti pa je potrebno odabrati prikladan broj modula).

Valja primijetiti da umnožak najvećeg broja paralelno pregledavanih računala i najvećeg broja istovremenih pregleda jednog računala daju ukupan broj procesa pokrenutih na poslužitelju.
Slijedi nekoliko postavki vezanih uz izvješća koja generira aplikacija (eng. *report*):

- *Report verbosity* – postavlja količinu ispisa vezanu uz pojedini modul, a
- *Report paranoia* – određuje najnižu razinu važnosti prikazanih poruka u ispisu.

Ugrađene su i mogućnosti prilagodbe naprednih postavki vezanih uz pregled priključaka (eng. *port scanning control*):

- *Port range to scan* – odabir priključaka koji će se pregledavati,
- *Max number of packets per second for port scan* – može se umanjiti kako bi se dobilo na točnosti pregleda priključaka i
- *No simult ports* – određivanje priključaka na kojima se ne smiju ispitivati dvije ili više ranjivosti istovremeno.

Ovdje se korisnicima Windows XP sustava zbog određenih ograničenja ovih sustava preporuča postavljanje sljedećih vrijednosti:

- *Max number of hosts*: 10
- *Max number of security checks*: 4
- *Max number of packets per second for a port scan*: 50

4.1.7.2. Opcija *Ping*

Naredba `ping`, koja odašilje *echo-request* zahtjeve, koristi se za određivanje dostupnosti računala i njihovih priključaka. Ukoliko se, primjerice, uključe i ICMP ping i TCP ping, poslužitelj će ispitati postojanje računala odnosno otvorenih priključaka korištenjem oba protokola.

4.1.7.3. Opcija *Services*

Ovdje se nalaze postavke vezane uz raspoznavanje vrste usluge koja se nalazi iza odgovarajućeg priključka na pregledavanom računalu. Njihovim pravilnim postavljanjem umanjuje se opasnost od simultanog pregleda pisača ili sličnih uređaja/usluga koje ne podržavaju više otvorenih priključaka istovremeno.

4.1.7.4. Opcija *Credentials*

SMB (eng. *Server Message Block*) je usluga koja omogućava dijeljenje zajedničkih resursa između više računala s različitim operacijskim sustavima. Ova opcija sadrži postavke vezane uz SMB korisničke račune poput korisničkog imena, zaporke i domene. Ostale SMB postavke se preporuča ostaviti na podrazumijevanim vrijednostima ukoliko korisnik nije stručnjak za to područje.

4.1.7.5. Opcija *Web*

Omogućuje izmjenu postavki vezanih uz poslužitelje koji su pokrenuti na računalima nad kojima se obavlja pregled ranjivosti. Ukoliko se nekoj usluzi na pregledavanom računalu može pristupiti i sa i bez korištenja korisničkih podataka (korisničko ime i zaporka), tada se savjetuje njihovo postavljanje kako bi se proveo pregled i u slučaju s povećanim ovlastima. Dobar primjer je korištenje Apache web poslužitelja čije se ranjivosti ne mogu provjeriti bez upisivanja korisničkih podataka u ovu karticu. Iako se tako pronađene ranjivosti mogu iskoristiti jedino od strane autenticiranih korisnika, one i dalje predstavljaju potencijalnu opasnost te ih je poželjno uočiti i ispraviti.

4.1.7.6. Opcija *Compliance*

Omogućava učitavanje datoteka s pravilima kako bi se provjerilo zadovoljava li sustav određene sigurnosne standarde. Provjera se može obaviti za pet Windows i pet Unix/Linux sigurnosnih pravila. Ova usluga je omogućena samo za korisnike s *Direct Feed* vrstom pretplate.

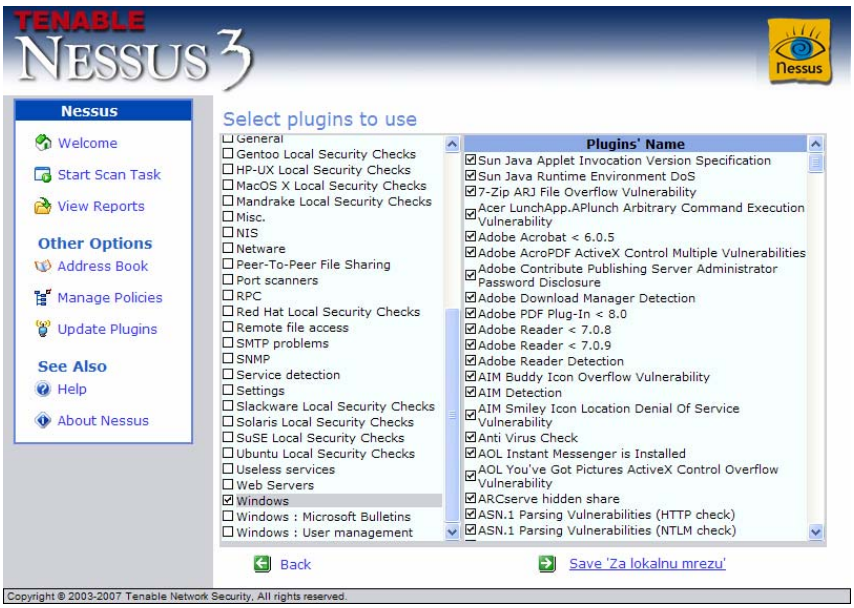
4.1.7.7. Opcija *Others*

Ovdje se nalazi čitav niz različitih mogućnosti. Nekoliko ih je vezano uz provjeru poslužitelja elektroničke pošte i tzv. *news* poslužitelja. Provjera elektroničke pošte radi se pokušajem njenog

neovlaštenog slanja. Ukoliko se pošta uspije poslati, ranjivost je uočena budući da na taj način poštu mogu slati i generatori neželjenih (eng. *spam*) poruka.

4.1.8. Odabir modula

Moduli su podijeljeni u skupine prema zajedničkim karakteristikama. Iz bogatog sadržaja moguće je odabrati proizvoljan broj modula s ranjivostima koja je potrebno provjeriti. Sljedeći prikaz ilustrira opisano:



Slika 5: Popis modula

4.1.9. Izvješća

Odabirom poveznice *View Reports* pristupa se izvješćima koja mogu biti u različitim formatima. Nessus inicijalno sva izvješća sprema u XML formatu. Ona se mogu pregledavati prema različitim kriterijima koji utječu na preglednost danih podataka:

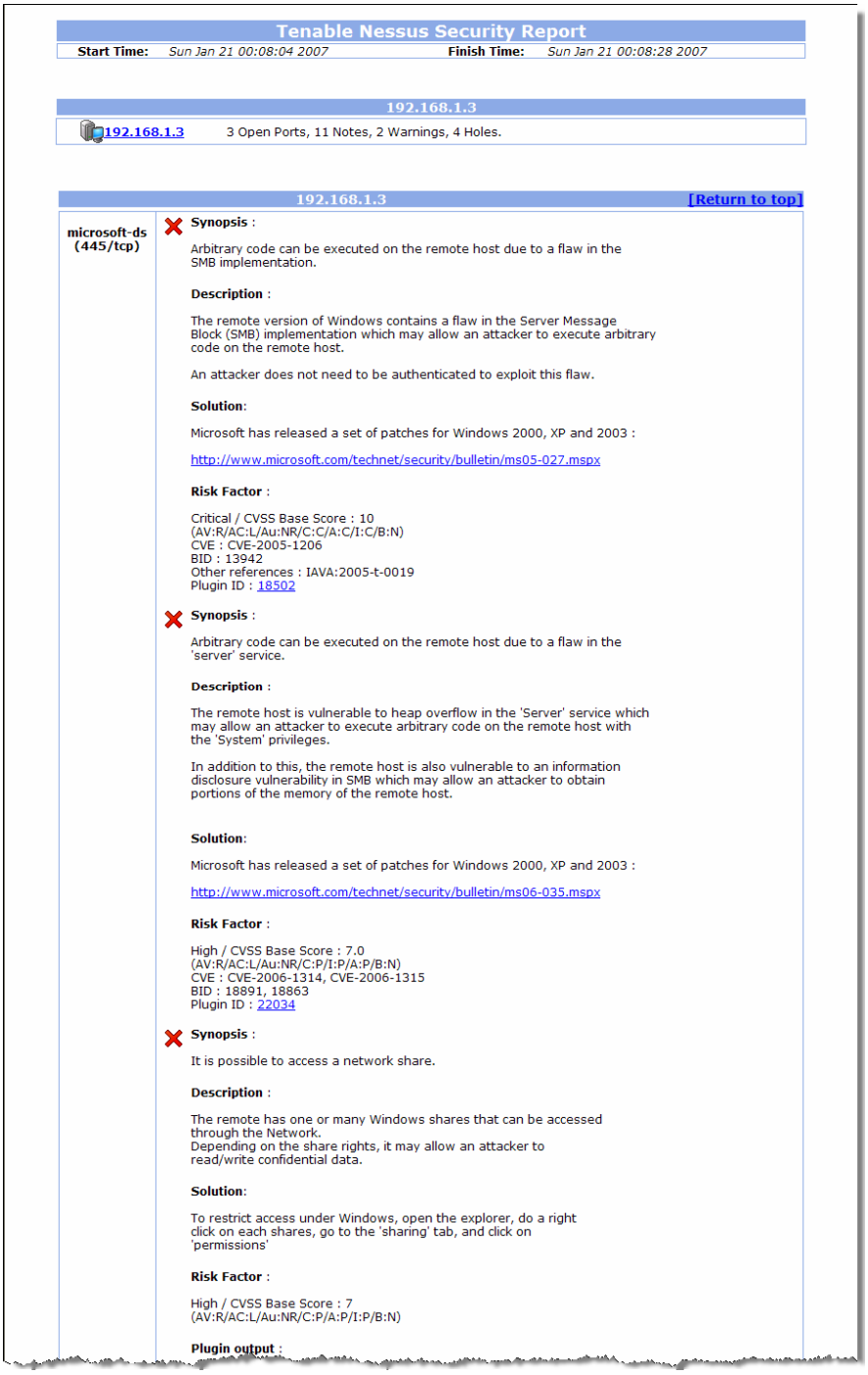
- *View by Host* – prema pregledanom računalu,
- *View by Port* – prema pregledanim priključcima,
- *View by Vulnerability* – prema ranjivostima,
- *Plain XML* – pregled čistih XML podataka i
- *Plain Text (NSR)* – pregled u obliku neobrađenog teksta.

Nessus može generirati izvješća razlika između dva pregleda. Ova je mogućnost izuzetno korisna za određivanje razlika kod pregleda iste mreže u različitim trenucima te na taj način daje obavijesti o ispravljenim propustima kao i o uočenim novim ranjivostima.
Slijedi izbor njenih triju mogućnosti:

- *Only compare with plugin ID* – ukoliko je uključena tada se radi usporedba prema jedinstvenom broju propusta, a u protivnome prema cijelom tekstu propusta.
- *Ignore "host is dead" message* – ukoliko se želi dobiti na kompaktnosti izvješća, preporuka je uključiti ovu mogućnost, posebno korisno kod pregledavanja mrežnih segmenata velikog raspona s malo aktivnih računala.
- *Only compare hosts which show up in both of the reports* – uspoređuju se samo računala čiji se opisi nalaze u oba izvješća.

Izvješća se mogu zasebno oblikovati korištenjem XSL odnosno tzv. *style sheet* mehanizma te kao takva prikazivati u nekom HTML pregledniku.
Nadalje, izvješća se mogu i dijeliti s ostalim korisnicima za što postoji nekoliko tehnika:

- Web arhive – spremanje u Microsoft Web Archive (*.mht) format omogućuje jednostavno dijeljenje arhiva i njihovo pregledavanje korištenjem Microsoft Internet Explorer programskog paketa.
- Čisti HTML – spremanje stranica u obliku HTML datoteka i pripadnih mapa sa slikovnim datotekama.
- Ispis u PDF dokument – nije izvorno podržano aplikacijom Nessus, ali se radi o spremanju izvješća u PDF dokument korištenjem odgovarajuće programske podrške.
- XML izlaz – svako Nessus izvješće se može spremiti u XML formatu te dalje proslijediti na obradu, primjerice, u Microsoft Office 2003 Excel paket.



Tenable Nessus Security Report

Start Time: Sun Jan 21 00:08:04 2007 Finish Time: Sun Jan 21 00:08:28 2007

192.168.1.3

192.168.1.3 3 Open Ports, 11 Notes, 2 Warnings, 4 Holes.

192.168.1.3 [Return to top]

microsoft-ds (445/tcp)

Synopsis :

Arbitrary code can be executed on the remote host due to a flaw in the SMB implementation.

Description :

The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation which may allow an attacker to execute arbitrary code on the remote host.

An attacker does not need to be authenticated to exploit this flaw.

Solution:

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

http://www.microsoft.com/technet/security/bulletin/ms05-027.mspx

Risk Factor :

Critical / CVSS Base Score : 10
(AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N)
CVE : CVE-2005-1206
BID : 13942
Other references : IAVA:2005-t-0019
Plugin ID : 18502

Synopsis :

Arbitrary code can be executed on the remote host due to a flaw in the 'server' service.

Description :

The remote host is vulnerable to heap overflow in the 'Server' service which may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

In addition to this, the remote host is also vulnerable to an information disclosure vulnerability in SMB which may allow an attacker to obtain portions of the memory of the remote host.

Solution:

Microsoft has released a set of patches for Windows 2000, XP and 2003 :

http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx

Risk Factor :

High / CVSS Base Score : 7.0
(AV:R/AC:L/Au:NR/C:P/I:P/A:P/B:N)
CVE : CVE-2006-1314, CVE-2006-1315
BID : 18891, 18863
Plugin ID : 22034

Synopsis :

It is possible to access a network share.

Description :

The remote has one or many Windows shares that can be accessed through the Network.
Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution:

To restrict access under Windows, open the explorer, do a right click on each shares, go to the 'sharing' tab, and click on 'permissions'

Risk Factor :

High / CVSS Base Score : 7
(AV:R/AC:L/Au:NR/C:P/A:P/I:P/B:N)

Plugin output :

Slika 6: Pregled izvješća

4.1.10. Nessus iz naredbenog retka

Pokretanjem `NessusCmd.exe` izvršne datoteke iz `C:\Program Files\Tenable\Nessus` (odnosno mape u koju je spremljen program za vrijeme instalacije) omogućuje se korištenje klijenta iz naredbenog retka. Za uspješan rad, Nessus servis mora biti prethodno pokrenut.

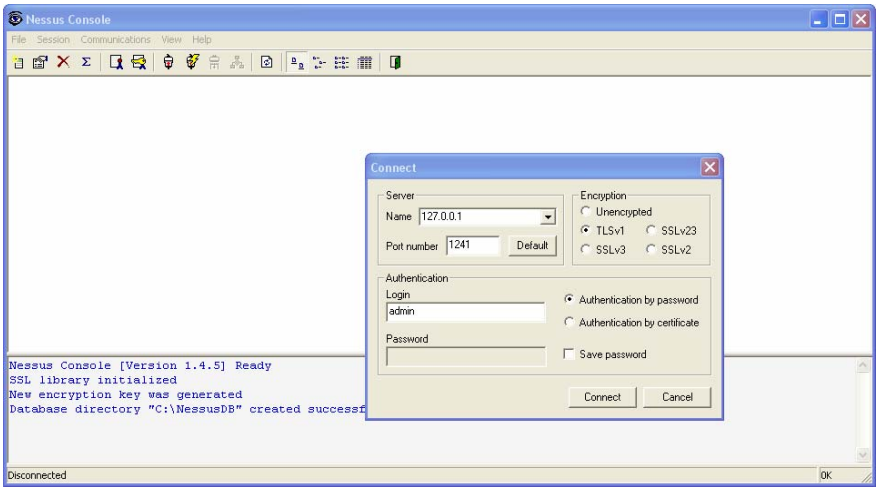
4.2. NessusWX

Radi se o klijent aplikaciji čiji je autor Victor Kirhenshtein, a nadogradnje i održavanje radi Tenable tim. Aplikacija podržava nezaštićenu, ali i zaštićenu (SSL) komunikaciju s poslužiteljem te autentikaciju korisnika zaporkom ili sigurnosnom potvrdom (X.509 certifikat). Mogu se uspostaviti i dvije ili više sjednica (eng. *session*), pri čemu svaka može imati zasebne postavke. Razvijen je i relativno jednostavan model baze podataka u kojem se čuvaju svi važni podaci. Izvješće se generira kao običan tekst, u PDF formatu i HTML formatu, a podržano je i generiranje (eng. *export*) u nekoliko različitih formata datoteka kao i uvođenje (eng. *import*) nekih formata. Izvješća se mogu i međusobno uspoređivati.

Instalacija NessusWX paketa je jednostavna budući da dolazi unutar ZIP arhive koju je potrebno raspakirati. Nadogradnja se obavlja na jednak način: preuzima se najnovija inačica paketa u obliku arhive (npr. nessuswx-1.4.5d.zip) te se raspakira u istu mapu u kojoj je paket prvotno bio instaliran.

Prvim pokretanjem izvršne datoteke pojavljuje se prozor s postavkama vezanim uz direktorij u koji će klijent spremati različite datoteke tijekom svojeg izvođenja. Preporuča se odabir podrazumijevane vrijednosti.

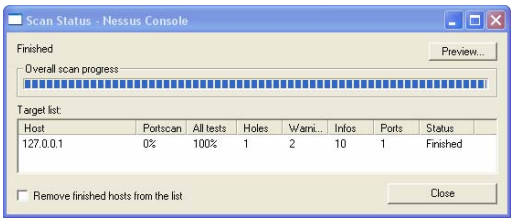
Za spajanje na poslužitelj potrebno je uvesti stvorenu datoteku sa sigurnosnom potvrdom odabirom izbornika *File* te odabirom *Client certificate* opcije. Odabirom *Communications* padajućeg izbornika omogućuje se odabir *Connect* opcije koja se koristi prilikom spajanja na poslužitelj. Potrebno je unijeti valjane korisničke podatke za autentikaciju. Ukoliko je korisnik klijenta prethodno dodao sigurnosnu potvrdu, ona bi se trebala vidjeti u padajućem izborniku ukoliko se uključi opcija *Authentication by certificate*.



Slika 7: NessusWX klijent

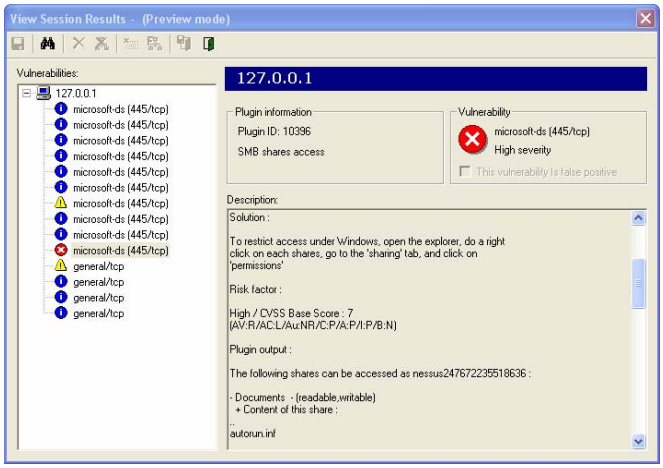
Slijedi preuzimanje podataka o instaliranim modulima za provjeru ranjivosti.

Pregled se inicijalno pokreće odabirom padajućeg izbornika *Session* i odabirom opcije *New* te prihvaćanjem ponuđenog naziva ili unosom željenog. Pod karticom *Targets* treba odabrati opciju *Add* i unijeti IP računala nad kojim se želi izvesti provjera. Opcija *Options* nudi *Safe checks* mogućnost koju ne treba zanemariti budući da njezino isključivanje može uzrokovati DoS stanje kod računala nad kojim se provjera izvodi. Desnim klikom miša na stvorenu ikonu i odabirom *Execute* opcije pokreće se sigurnosna provjera.



Slika 8: Indikator količine obavljenog posla

Izgled prozora s podacima o dovršenom pregledu dan je na sljedećem prikazu.

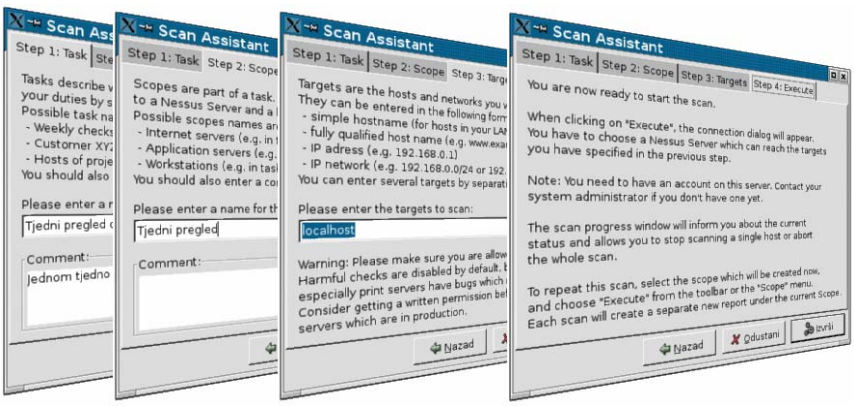


Slika 9: Izvješće u NessusWX aplikaciji

Dodatne postavke pojedine sjednice mijenjaju se desnim klikom miša te odabirom opcije *Properties* i vrlo su slične onima već pojašnjenima za Nessus3 klijent aplikaciju pa ih se ovdje neće zasebno navoditi.

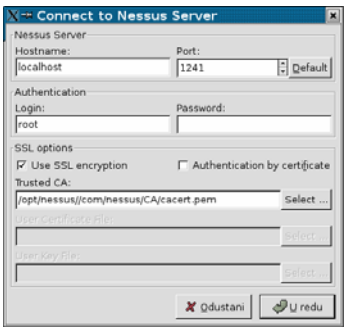
4.3. Linux klijent - NessusClient

NessusClient ime je Nessus klijentske aplikacije koja je namijenjena izvođenju pod X11/GTK grafičkim korisničkim sustavom, a temeljena je na izvornom Nessus klijentu. Aplikaciju održava Tenable tim, a uz njihovu pomoć Inteviation GmbH je u jesen 2005. prenijela klijent i na Windows platforme.
Mogućnosti ovog klijenta su vrlo velike. Podrška za *Scopes* i *Tasks* omogućuje preglednije praćenje svih podataka o provedenim sigurnosnim provjerama te postavkama vezanim uz module. NessusClient može izvoditi više pregleda istovremeno. Izvješća se mogu izvesti u PDF, HTML, XML i još neke formate. Pored svega navedenog, klijent sadrži i značajku *Scan Assistant* kojom se korisnika vodi kroz proces stvaranja novih pregleda korak po korak, a ilustrativno je prikazan na slijedećoj slici.



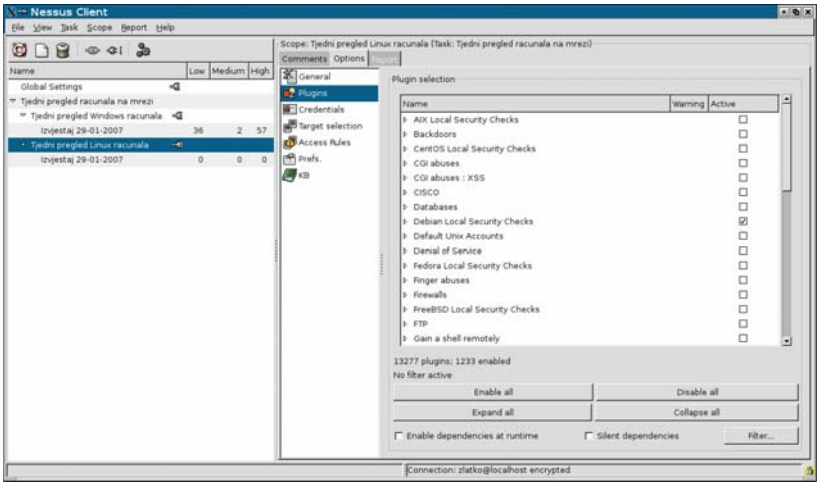
Slika 10: *Scan Assistant* – četiri koraka

Spajanje na poslužitelj se obavlja upisivanjem korisničkih podataka za Nessus poslužitelj ili odabirom odgovarajuće datoteke sa certifikatom.



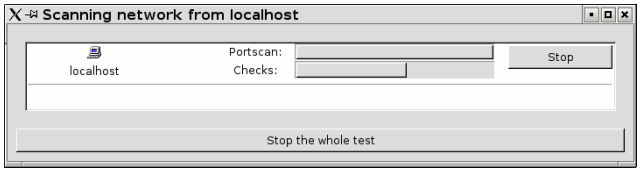
Slika 11: Spajanje na poslužitelj

Važno je razumjeti hijerarhijsku organizaciju koju omogućuje NessusClient. Opća grupa *Task*, može se shvatiti kao direktorij, podržava *Scope*, što se može shvatiti kao poddirektorij, unutar kojeg se spremaju izvješća (shvatiti ih kao datoteke). Svaki se entitet može spojiti na zaseban poslužitelj, a preglede je moguće provoditi istovremeno.



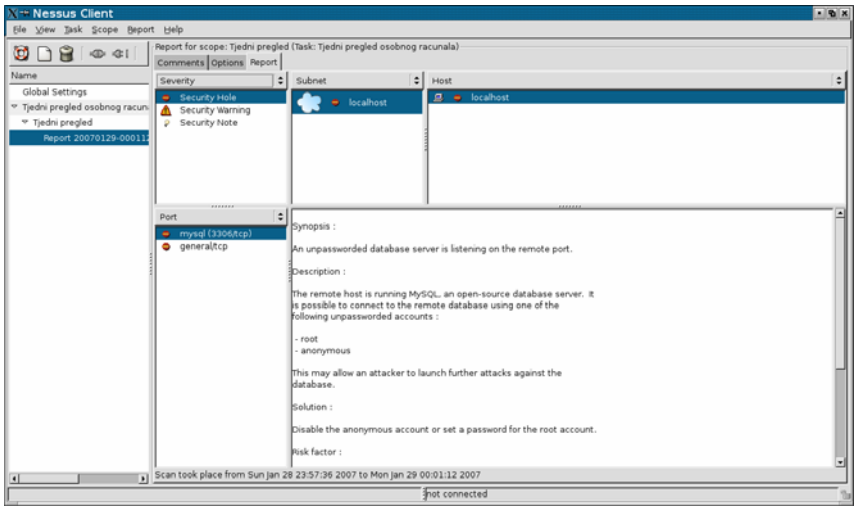
Slika 12: Potpuni prikaz NessusClient aplikacije

Postavke su vrlo slične onima na klijentu za Windows sustave pa ovdje neće biti posebno pojašnjene. Pregled ranjivosti se obavlja odabirom željenog zadatka ili dosega (*task*, *scope*) te odabirom opcije *Execute*. Pojavljuje se prozor s indikatorom preostale količine posla.



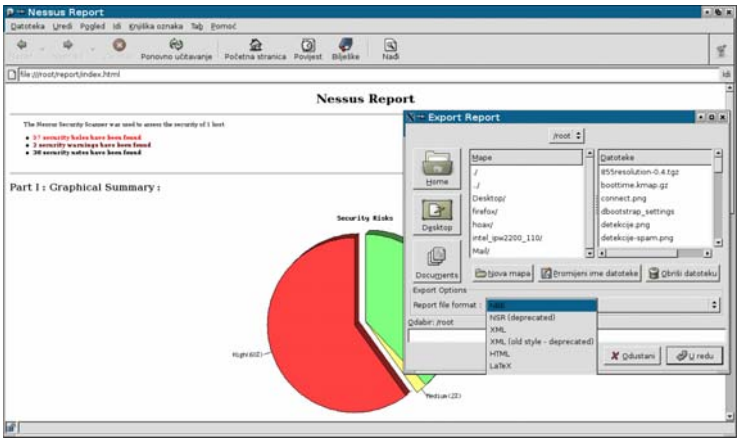
Slika 13: Indikator obavljenog posla

Nakon provjere ranjivosti slijedi prikaz rezultata koji je nešto drukčiji od prikaza kod ostalih klijenata. NessusClient ima ugrađen vrlo dobar i koncizan, a istovremeno i potpun preglednik rezultata sigurnosnih provjera. Većim brojem manjih izbornika omogućena je pretraga prema više karakteristika istovremeno, što daje vrlo veliku jasnoću rezultata.



Slika 14: Pregled rezultata sigurnosne provjere

Vrlo korisna značajka ovog klijenta je i već spomenuta bogata ponuda formata za izradu izvješća. Na sljedećem prikazu vidljiv je dijalog generiranja izvješća te jedan primjer grafičkih rezultata u obliku web stranice.



Slika 15: Dijalog za izvoz izvješća i jedan primjer HTML izvješća

Odabir NessusClient aplikacije je vrlo dobar, a možda i najbolji, izbor klijentske Nessus aplikacije za Unix i Linux operacijske sustave.

4.4. Linux/Unix naredbeni redak i Nessus

Od korisnika se ne zahtijeva isključivo korištenje klijentskih aplikacija za povezivanje na Nessus poslužitelj i provođenje sigurnosnih pregleda. Može se koristiti i naredbeni redak za pokretanje provjere, ali se tada provjera pokreće u tzv. *batch* modu. Naredba izgleda ovako:

```
# /opt/nessus/bin/nessus -q [-pPS] <host> <port> <user> <password>
<targets-file> <result-file>
```

Slijedi opis parametara:

- `-p` – dohvaća popis instaliranih modula za pregled ranjivosti,
- `-P` – dohvaćanje popisa poslužitelja i postavki modula,
- `-S` – ispis prethodna dva parametra u SQL formatu,
- `<host>` – računalo na komu je pokrenut poslužitelj,
- `<port>` – priključak na kojemu poslužitelj čeka uspostavu veze,
- `<user>` – korisničko ime za pristup poslužitelju,

- `<password>` – korisnička zaporka,
- `<targets>` – ime datoteke koja sadrži popis računala nad kojima će se pregled obaviti,
- `<results>` – ime datoteke u koju se spremaju rezultati pregleda.

Istu se aplikaciju može koristiti i za pretvorbu izvješća u različite formate, a sintaksa joj glasi:

```
# /opt/nessus/bin/nessus -i in.[nsr|nbe] -o out.[xml|nsr|nbe|txt]
```

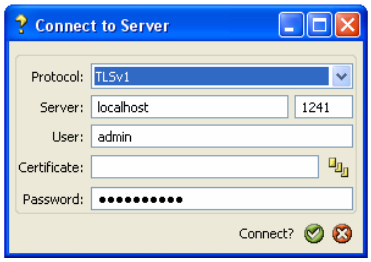
Opcija '`-i`' određuje izvorno izvješće koje može biti u NSR ili NBE formatu dok '`-o`' označava ime izlazne datoteke iza koje se navodi željeni format.

4.5. Klijent aplikacija Nessj

Nessj je višeplatformska aplikacija za Nessus i Nessus kompatibilne poslužitelje, koja je prije bila poznata pod imenom Reason. Osim što je grafičko korisničko sučelje vrlo napredno i vizualno ugodno, i broj ostalih mogućnosti je velik. Pritom je potrebno izdvojiti mogućnost uređivanja sjedničkih podataka, izrade obrazaca, grafova i izvješća korištenjem XSLT jezika za "vizualnu doradu" XML dokumenata. Klijent je dostupan za Linux, Mac OS X i Windows operacijske sustave, a napisan je Java programskim jezikom uz korištenje SWT alata za izradu grafičkog sučelja. Važna značajka je i otvorenost koda (eng. *open source*).

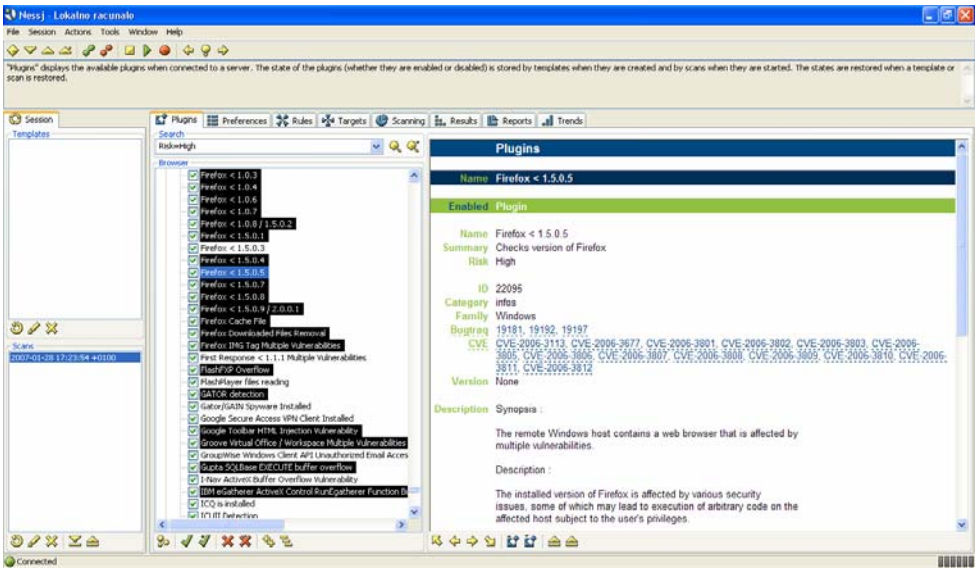
Sve postavke pojašnjene u opisu Windows klijenta Nessus3 postoje i ovdje pa neće biti ponovno opisivane.

Prilikom korištenja prvi je korak povezivanje na željeni poslužitelj. U prikazanom slučaju riječ je o poslužitelju na lokalnom računalu:



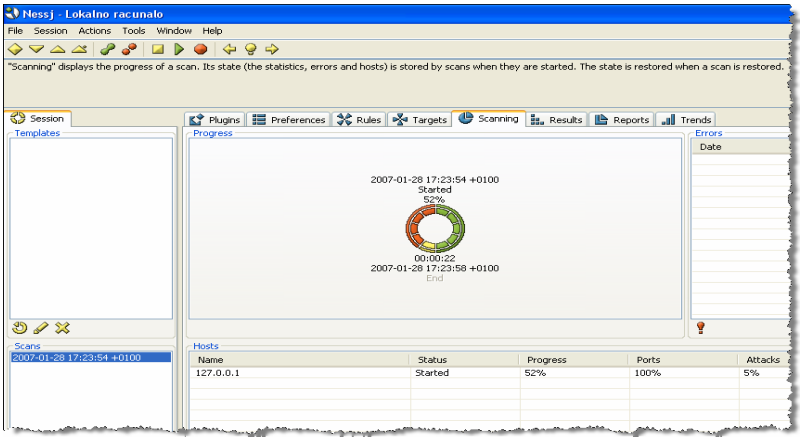
Slika 16: Spajanje na poslužitelj

Vrlo korisna značajka je i pretraživanje modula. Primjerice, uz postavljanje upita pretrage na "*Risk=High*" odabrati će se svi moduli za testiranje ranjivosti s visokim stupnjem opasnosti.



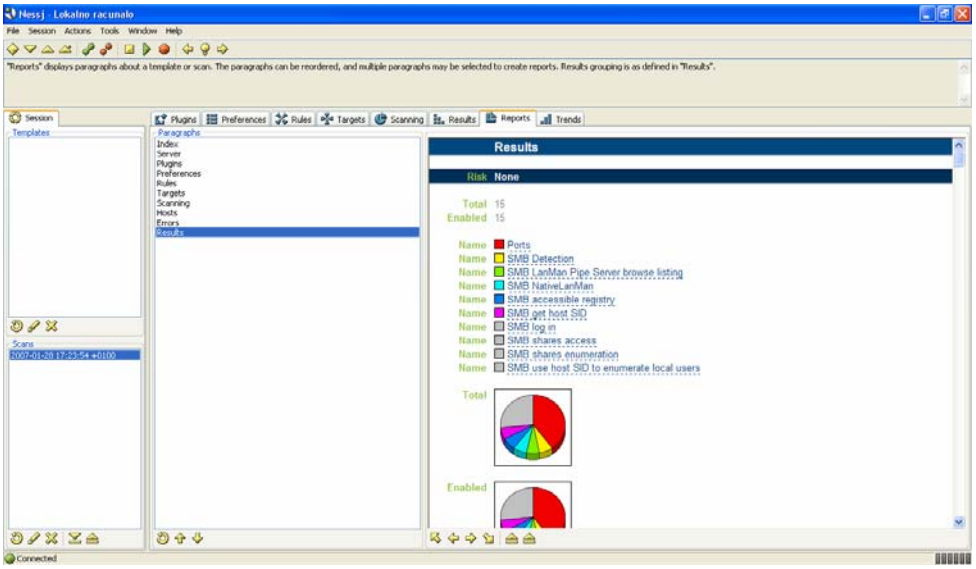
Slika 17: Pretraživanje modula

Pokretanje provjere ranjivosti obavlja se odabirom padajućeg izbornika *Actions* te zatim opcije *Start scan*. Nakon kraće inicijalizacije indikator počinje prikazivati napredak u ukupnoj količini obavljenog posla.



Slika 18: Klijent tijekom izvođenja provjere

Konačno, prikaz rezultata također je grafički dotjeran, a omogućeno je i određivanje vrste grafova, boja i sličnih karakteristika. Slični se izvještaji generiraju i kod ostalih klijenata, ali se prikazuju u web preglednicima. Nessj ne koristi vanjski preglednik za prikaz izvješća nego ima svoj.



Slika 19: Grafički prikaz rezultata

5. NASL skriptni jezik

Skriptni jezik NASL (eng. *Nessus Attack Scripting Language*) razvijen je za potrebe stvaranja modula za provjeru ranjivosti korištenjem Nessus programskog paketa. Temeljna ideja bila je razvoj jednostavnog i razumljivog skriptnog jezika koji će biti prilagođen razvoju Nessus modula te omogućiti transparentnost operacijskih sustava na kojima je Nessus poslužitelj pokrenut. Ovakvom rješenju pribjeglo se zbog niza nedostataka u slučaju korištenja nekih drugih skriptnih jezika kao što su Python, Ruby, Perl i sl. Prva manjkavost ovakvih rješenja je potreba za instaliranjem podrške za jezik te dodatnih biblioteka koje omogućuju razvoj programa u kontekstu računalnih mreža. Kompatibilnost operacijskih sustava još je jedan nedostatak koji u velikoj mjeri može utjecati na jednostavnost korištenja Nessus paketa. Nadalje, korištenje odnosno razvoj skripti korištenjem drugih skriptnih jezika može otvoriti potencijalne sigurnosne probleme na računalu s kojeg se provjera

obavlja te uzrokovati veću potrebu za resursima nego bi to bilo u slučaju jezika usmjerenog na konkretnu problematiku.
Prednosti jezika NASL u odnosu na ostale skriptne jezike su:

- jednostavno učenje zbog sličnosti sa C jezikom s kojim je većina naprednijih korisnika upoznata,
- jednostavna instalacija paketa,
- za razvoj različitih modula nisu potrebni dodatni paketi,
- brza i jednostavna izrada modula,
- u pogledu sigurnosti NASL osigurava da tijekom izvođenja skripte neće doći do izvođenja naredbi na lokalnom računalu te da neće doći do slanja paketa niti jednom drugom računalu osim onoga nad kojim se obavlja provjera sigurnosti.

Svakako, sve prednosti u jednom kontekstu u drugome mogu biti i mane pa tako i NASL ima nedostataka odnosno ograničenja u odnosu na druge skriptne jezike:

- podržani su samo jednostavni tipovi podataka,
- broj mogućnosti i ugrađenih funkcija znatno je manji u odnosu na ostale skriptne jezike,
- brzina izvođenja i raspolaganje memorijom nisu optimalni,
- nepostojanje alata za traženje pogrešaka (eng. *debug*) u NASL skriptama.

Zbog ovih ograničenja NASL skriptni jezik nije pogodan za razvoj aplikacije neke druge namjene, ali zbog svih navedenih prednosti ovaj jezik prednjači u kontekstu razvoja Nessus modula za provjeru ranjivosti.

6. Zaključak

Treća generacija Nessus programskog paketa dostupna je za velik broj današnjih operacijskih sustava, a u sprezi s jednostavnošću korištenja te besplatnom distribucijom ovaj alat vodeći je među alatima slične namjene. Usprkos činjenici da nije komercijalan proizvod, na tržištu je više prihvaćen od velikog broja komercijalnih rješenja. Na http://sectools.org/ web stranicama koje obrađuju temu sigurnosti na Internetu, Nessus je odabran kao prvi paket između stotinu paketa s područja mrežne sigurnosti u 2006. godini, što dovoljno govori o njegovoj kvaliteti.

NASL skriptni jezik, koji omogućava jednostavan i brz razvoj modula za provjeru ranjivosti, dodatno povećava vjerodostojnost opisanog proizvoda, a veliki broj aktivnih suradnika koji razvijaju nove module osiguravaju korisnicima rad s trajno ažurnim definicijama sigurnosnih propusta.

Dijelovi aplikacije namijenjeni radu s izvješćima koja se stvaraju nakon svake provjere ranjivosti sadrže velik broj mogućnosti te pružaju odlične mogućnosti oblikovanja u skladu sa svojim potrebama i zahtjevima korisnika.

Naprednijim korisnicima se preporuča pregled NASL datoteka u kojima se mogu pronaći uzroci eventualno krivo prepoznatih propusta. Osim toga, njihovom je izmjenom moguće dodatno provjeriti proizvoljne ranjivosti.

Što se tiče programskih paketa, poslužitelji inačica 2.x i dalje će se nadograđivati pa postojeći korisnici ne moraju nužno prijeći na najnoviju inačicu. Međutim, to se preporuča zbog noviteta u brzini i ostalim segmentima izvođenja sigurnosnih provjera.

7. Reference

[1.] Nessus Vulnerability Scanner, http://www.nessus.org, siječanj 2007.

[2.] Introduction to Nessus, http://www.securityfocus.com/infocus/1741, siječanj 2007.

[3.] Introduction to Nessus Tutorial, http://www.securitydocs.com/library/2730, siječanj 2007.

[4.] Nessus Security Scanner, http://www.cramsession.com/articles/get-article.asp?aid=336, siječanj 2007.

[5.] Nessj, http://reason.idealogica.com/, siječanj 2007.

[6.] CARNet CERT & LSS, NASL – Nessus Attack Scripting Language, CCERT-PUBDOC-2005-03-114, ožujak 2005.

[7.] CARNet CERT & LSS, Analiza alata NeWT, CCERT-PUBDOC-2004-08-85, kolovoz 2004.

[8.] Nessus 3.0 Advanced User Guide, http://www.nessus.org/documentation/nessus_3.0_advanced_user_guide.pdf, kolovoz 2006.

[9.] Nessus 3.0 Client Guide, http://www.nessus.org/documentation/nessus_3.0_client_guide.pdf, prosinac 2006.

[10.] Nessus 3.0 Installation Guide, http://www.nessus.org/documentation/nessus_3.0_installation_guide.pdf, siječanj 2007.

[11.] Nessj, http://sourceforge.net/docman/display_doc.php?docid=33221&group_id=157279, siječanj 2007.