HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Nikto CGI skenera

CCERT-PUBDOC-2003-04-18

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

Nikto je alat za pregledavanje Web poslužitelja u potrazi za potencijalno opasnim CGI skriptama i ostalim sigurnosnim propustima. CGI pregledavanje umanjuje rizik od ranjivosti Web poslužitelja uzrokovanih nesigurnim CGI skriptama i nehotičnim pogreškama u konfiguraciji poslužitelja. Budući da se nesigurnosti u CGI skriptama otkrivaju gotovo svakodnevno, ovakvo pregledavanje predstavlja jednostavan način održavanja visoke razine sigurnosti Web poslužitelja.
Ovaj alat je u mogućnosti provoditi opsežna pregledavanja koja obuhvaćaju identifikaciju više od dvije tisuće potencijalno opasnih CGI skripti i ostalih sigurnosnih problema koji su najčešće posljedica loše konfiguracije. Pretraživanjem je podržano oko dvije stotine inačica Web poslužitelja.

2. Instalacija

Nikto je skup skripti pisanih u Perl programskom jeziku, koje nije potrebno instalirati ali za njihov ispravan rad na sustavu mora postojati Perl interpreter. Program je platformski neovisan i može raditi na Windows i Linux operacijskim sustavima. Ipak, ovaj paket je ovisan o još nekoliko programskih paketa, koji su obavezni za njegov ispravan rad.
Cjelokupna podloga rada Nikto-a temelji se na Perl modulu pod nazivom libwhisker. Namjena ovog modula je pronalaženje CGI skripti na Web poslužiteljima, koje se realizira direktnim upitima i pretraživanjem poslužitelja. Libwhisker modul je standardno uključen u Nikto programski paket (`./plugins/LW.pm`), ali poželjno ga je redovito osvježavati novijim inačicama. Modul se može pronaći na adresi http://www.wiretrip.net/rfp/7/index.asp.

3. Konfiguracija i pokretanje

U program je ugrađena i mogućnost korištenja eksternog alata za pregledavanje portova u potrazi za Web poslužiteljima. Kao eksterni alat koristi se nmap (http://www.insecure.org/nmap/), koji drastično ubrzava proces pregledavanja portova u odnosu na pretraživanje pomoću Nikto-a. Da bi se omogućilo korištenje eksternog programa za pregledavanje portova, u `config.txt` datoteci potrebno je vrijednost parametra NMAP podesiti tako da pokazuje put do nmap programa koji je instaliran na sustavu. Npr.:

```
NMAP=/usr/bin/nmap
```

U datoteci `config.txt` nalazi se pohranjen set konfiguracijskih opcija pomoću kojega se može modificirati ponašanje Nikto alata.
Moguće je podešavati sljedeće parametre:

- `CGIDIRS` – imena cgi direktorija koji će se pretraživati na udaljenom računalu,
- `CLIOPTS` – ovaj parametar definira opcije iz naredbenog retka koje se obavezno uključuju prilikom pokretanja Nikto-a (bez obzira da li ih korisnik navede),
- `SKIPPORTS` – ovdje se navode portovi udaljenog računala koji se iz određenih razloga ne žele pregledavati; ova opcija se najčešće koristi kada se želi izbjeći ometanje rada određenih servisa,
- `PROXYHOST` – proxy poslužitelj koji će se koristiti za pregledavanje,
- `PROXYPORT` – port na proxy poslužitelju koji se koristi za tuneliranje prometa,
- `PROXYUSER` – korisničko ime za prijavljivanje na proxy poslužitelj (ukoliko je potrebno),
- `PROXYPASS` – zaporka za prijavljivanje na proxy poslužitelj; ukoliko je zaporka potrebna, a nije navedena na ovom mjestu, program će zatražiti da ju korisnik upiše u naredbenom retku,
- `DEFAULTHTTPVER` – definira inačicu HTTP protokola koji će koristiti za spajanje na udaljeni poslužitelj; u slučaju da spajanje ne uspije, program će automatski pokušati pronaći ispravan protokol,
- `PLUGINDIR` – specificira punu stazu do direktorija s *plugin* datotekama; ova opcija koristi se u slučaju da program iz nekog razloga nije u stanju automatski pronaći *pluginove*,

- `MUTATEDIRS` – put do dodatnih direktorija koji će se koristiti u *mutate* načinu rada,
- `MUTATEFILES` – dodatne datoteke koje se koriste u *mutate* načinu rada,
- `GOOGLERS` – ukoliko se program pokreće s `-google` opcijom, pretraživanje će se izvršiti sa opcijama navedenima ovdje,
- `STATIC-COOKIE` – postavlja vrijednost kolačića (engl. *Cookie*) koji će biti poslan uz svaki zahtjev upućen udaljenom poslužitelju.

Potrebno je napomenuti kako niti jedna od opisanih opcija nije obavezna za ispravan rad programa.
Osim opcija u konfiguracijskoj datoteci, Nikto podržava i niz opcija u naredbenom retku. Od sljedećih opcija koje će biti opisane, obavezna je jedino `-host` opcija koja označava ime (ili IP adresu) računala koje će se pregledavati.

- `-allcgi` – uključuje pregledavanje svih cgi direktorija definiranih parametrom `CGIDIRS` u konfiguracijskoj datoteci; pregledavanje će se izvršiti bez obzira da li spomenuti direktoriji postoje ili ne,
- `-cookies` – ispisuje imena i vrijednosti svih kolačića koji su primljeni prilikom pregledavanja,
- `-evasion` – uključuje metode izbjegavanja IDS sustava, koje su detaljnije opisane u poglavlju 4.1,
- `-generic` – uključuje kompletno pregledavanje, koje obuhvaća sve tipove Web poslužitelja i njihove sigurnosne propuste, tj. zanemaruje se identifikacijski "Server:" niz koji je primljen od strane poslužitelja; ova opcija je vrlo korisna u slučajevima namjerno izmijenjenih "Server:" nizova, koji pokazuju lažne inačice poslužitelja,
- `-findonly` – pregledava portove na udaljenom računalu u potrazi za Web poslužiteljima ali ne izvršava nikakvu daljnju provjeru u slučaju da je poslužitelj pronađen,
- `-host` – definira ime ili IP adresu računala koje će se pregledavati,
- `-id` – korisničko ime i zaporka (u formatu korisničko ime:zaporka) koje će Nikto koristiti u slučaju da pretraživani Web poslužitelj zahtijeva autorizaciju,
- `-mutate` – uključuje *mutate* način rada u kojem alat izvodi kombinirano pretraživanje svih direktorija navedenih u .db datotekama; *Mutate* načina rada opširnije je opisan u poglavlju 4.3.,
- `-nolookup` – isključuje potragu za DNS imenom pregledavanog računala,
- `-output` – definira datoteku u koju će se u tekstualnom formatu upisati rezultati pregledavanja,
- `-port` – definira port udaljenog računala na kojemu se nalazu poslužitelja koji se pregledava; u slučaju da opcija nije navedena koristiti će se uobičajeni port 80,
- `-root` – definira direktorij koji će se upotrijebiti ako prefiks svim zahtjevima upućenima prema testiranom računalu,
- `-ssl` – uključuje SSL način pregledavanja na portovima koji su navedeni ovom opcijom,
- `-timeout` – definira vrijeme čekanja na odgovor za postavljene upite; vrijeme čekanja inicijalno je podešeno na 10 sekundi,
- `-useproxy` – uključuje *proxy* način pregledavanja, koristeći *proxy* poslužitelj naveden opcijom `PROXYHOST` u konfiguracijskoj datoteci,
- `-vhost` – definiran imena virtualnih poslužitelja (ako postoje na testiranom računalu),
- `-webformat` – zapisuje rezultate pretraživanja, u navedenu datoteku, koristeći HTML oblik zapisa.

Sve navedene opcije mogu se koristiti u skraćenom obliku. To znači da je npr. u naredbenom retku umjesto `-generic` opcije moguće upisati samo `-g`.
Osim gore opisanih opcija, Nikto podržava i još nekoliko rjeđe korištenih opcija:

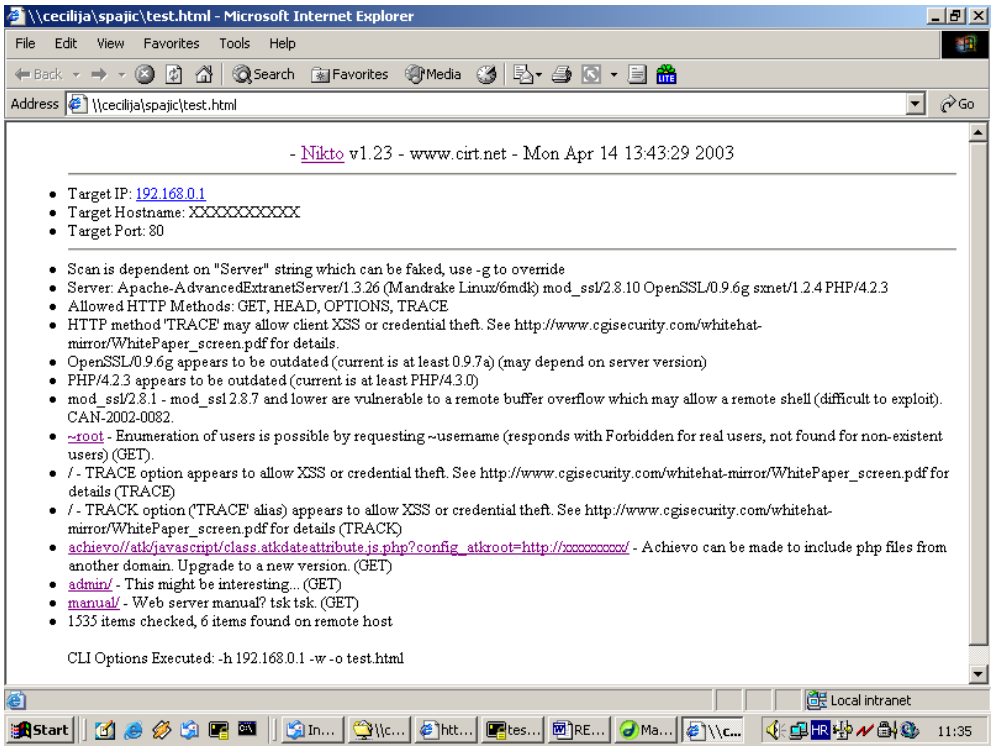
- `-dbcheck` – ukoliko se pokrene s ovom opcijom, Nikto će provjeriti ispravnost definicija za pretraživanje u `scan_database.db` i `user_scan_database.db` datotekama; preporučuje se izvršavanje ovakvih provjera prilikom svake izmjene navedenih datoteka,
- `-debug` – uključuje detaljan ispis podataka tijekom pregledavanja udaljenog računala; zbog vrlo velike količine podataka koja se generira, korištenje ove opcije preporučuje se isključivo prilikom problema u radu programa,

- `-google` – poziva Google Web pretraživač i pronalazi sve podatke vezane uz zadani poslužitelj, koristeći ključne izraze zapisane u `GOOGLERS` parametru u konfiguracijskoj datoteci; ukoliko u konfiguracijskoj datoteci ne postoje ključne riječi, program će koristiti inicijalni set ključnih riječi kao `password`, `passwd` itd.,
- `-update` – ovom opcijom podržano je automatsko osvježavanje baza podataka sa ranjivostima i *plugin* datoteka,
- `-verbose` – uključuje mogućnost opširnijeg ispisa tijeka i rezultata pregledavanja. Ova opcija je korisna u slučaju analize neuspjelih pregledavanja ili onih koja su prouzročila prekid rada testiranog poslužitelja.

Tipičan izlazni rezultat pregledavanja Nikto alatom je sljedeći:

```
test@testing nikto-1.23]$ ./nikto.pl -h 192.168.0.1
---------------------------------------------------------------------------
- Nikto v1.23  - www.cirt.net - Tue Apr 15 11:31:08 2003
---------------------------------------------------------------------------
+ Target IP:       192.168.0.1
+ Target Hostname: XXXXXXXXXXXX
+ Target Port:     80
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to
override
+ Server: Apache-AdvancedExtranetServer/1.3.26 (Mandrake Linux/6mdk)
mod_ssl/2.8.10 OpenSSL/0.9.6g sxnet/1.2.4 PHP/4.2.3
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ HTTP method 'TRACE' may allow client XSS or credential theft. See
http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for
details.
+ OpenSSL/0.9.6g appears to be outdated (current is at least 0.9.7a) (may
depend on server version)
+ PHP/4.2.3 appears to be outdated (current is at least PHP/4.3.0)
+ mod_ssl/2.8.1 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer
overflow which may allow a remote shell (difficult to exploit). CAN-2002-
0082.
+ /~root - Enumeration of users is possible by requesting ~username
(responds with Forbidden for real users, not found for non-existent users)
(GET).
+ / - TRACE option appears to allow XSS or credential theft. See
http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details
(TRACE)
+ / - TRACK option ('TRACE' alias) appears to allow XSS or credential theft.
See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for
details (TRACK)
+
/achievo//atk/javascript/class.atkdateattribute.js.php?config_atkroot=http:/
/xxxxxxxxxx/ - Achievo can be made to include php files from another domain.
Upgrade to a new version. (GET)
+ /admin/ - This might be interesting... (GET)
+ /manual/ - Web server manual? tsk tsk. (GET)
- 1535 items checked, 6 items found on remote host
```

Poželjno je korištenje opcije `-webformat` koja će rezultate pregledavanja pohraniti u datoteku u HTML formatu, što znatno olakšava pregledavanje rezultata.



Slika 1: Rezultati pregledavanja u HTML formatu

4. Mogućnosti programa

4.1. Izbjegavanje IDS sustava

Zbog velikog broja log poruka koje će se na poslužitelju generirati kao posljedica pregledavanja Nikto alatom, vrlo je lako uočiti ove aktivnosti. Međutim, Nikto je sposoban prikriti svoje aktivnosti kako bi se izbjegla detekcija od strane sustava za detekciju neovlaštenih aktivnosti na mreži (engl. *Intrusion Detection System*). Korištenjem opcije `-evasion` prilikom pokretanja programa moguće je primijeniti neke od sljedećih metoda za izbjegavanje IDS sustava:

1. slučajno URI kodiranje,
2. dodavanje znakova "/./" unutar URL adrese,
3. prerano završavanje URL adresa,
4. dodavanje dugačkih slučajnih znakovnih nizova HTTP zahtjevima,
5. pridjeljivanje lažnih parametara datotekama,
6. korištenje TAB umjesto SPACE znaka,
7. slučajna promjena velikih i malih slova unutar URL adrese,
8. korištenje znaka "\" umjesto "/" kod navođenja URL adresa,
9. isprepletanje sjednica.

Ukoliko se želi kombinirati više metoda istovremeno navode se redom njihovi brojevi. Tako će npr. opcija `-evasion 246` primijeniti metode pod rednim brojevima 2, 4 i 6 istovremeno.

```
[test@testing nikto-1.23]$ ./nikto.pl -evasion 246 -h 192.168.0.1
---------------------------------------------------------------------------
- Nikto v1.23  - www.cirt.net - Tue Apr 15 10:41:36 2003
---------------------------------------------------------------------------
+ Target IP:       192.168.0.1
+ Target Hostname: XXXXXXXXXXXXXX
+ Target Port:     80
+ Using IDS Evasion:    Directory self-reference (/./)
+ Using IDS Evasion:    Prepend long random string
```

```
+ Using IDS Evasion:    TAB as request spacer
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to
override
+ Server: Apache/1.3.27 (Unix) mod_ssl/2.8.11 OpenSSL/0.9.6g PHP/4.2.3
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, CONNECT, OPTIONS,
PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK, UNLOCK, TRACE
+ HTTP method 'PUT' method may allow clients to save files on the web
server.
+ HTTP method 'CONNECT' may allow server to proxy client requests.
+ HTTP method 'DELETE' may allow clients to remove files on the web server.
+ HTTP method 'PROPFIND' may indicate DAV/WebDAV is installed. This may
allow DAV
.
.
.
```

Opcija izbjegavanja IDS sustava preuzeta je iz LibWhisker paketa koji čini osnovu rada Nikto alata. Potrebno je napomenuti da se pregledavanje tuđih računalnih mreža smatra nedopuštenom aktivnošću, te da je ovu opciju poželjno koristiti isključivo za izbjegavanje IDS sustava na vlastitoj mreži.

4.2. Pregledavanje portova

Nikto ima mogućnost pregledavanja portova udaljenog računala u potrazi za Web poslužiteljima. Ukoliko pronađe otvoren port na udaljenom računalu, program se pokušava spojiti slanjem HTTP zahtijeva. U slučaju da HTTP zahtjevi ne uspiju, automatski će se pokušati i spajanje HTTPS protokolom.

```
[test@testing nikto-1.23]$ ./nikto.pl -findonly -h 192.168.0.1
---------------------------------------------------------------------------
- Nikto v1.23  - www.cirt.net - Tue Apr 15 10:37:58 2003
+ Server: http://192.168.0.1:80 Apache/1.3.26 mod_ssl/2.8.10 OpenSSL/0.9.6g
sxnet/1.2.4 PHP/4.2.3
[spajic@testing nikto-1.23]$
```

Ovom metodom moguće je pregledavati proizvoljna računala na mreži kako bi se ustanovilo da li imaju pokrenute Web poslužitelje na nestandardnim portovima.
Kako bi se ubrzalo pregledavanje portova, ostavljena je mogućnost korištenja nmap alata. Put do izvršne datoteke nmap-a podešava se parametrom `NMAP` u konfiguracijskoj datoteci. Pregledavanje portova nmap-om trebalo bi biti značajno brže od onog Niktom.

4.3. *Mutate* način rada

U *mutate* načinu rada Nikto pregledava udaljeni poslužitelj tražeći sve ranjive datoteke navedene u bazi ranjivosti u svim poznatim direktorijima. Na taj način moguće je pronaći ranjive CGI datoteke koje su premještene u nestandardne direktorije. Osim kombiniranja datoteka i direktorija, Nikto je u mogućnosti pronaći broj korisnika na Apache poslužiteljima pomoću `/~user` zahtijeva ili pronaći datoteke koje sadrže zaporke.
Mutate način rada omogućuje se navođenjem `–mutate` opcije prilikom pokretanja. Uz `–mutate` opciju potrebno je navesti i jedan od tipova pretrage:

1. kombiniranje imena CGI datoteka i poznatih direktorija,
2. pokušaj pogađanja datoteke s zaporkama,
3. pokušaj pronalaženja korisnika na Apache Web poslužiteljima.

Tako na primjer drugi tip pretrage rezultira sljedećim ispisom:

```
[test@testing nikto-1.23]$ ./nikto.pl -mutate 3  -h 192.168.0.1
```

```
---------------------------------------------------------------------------
- Nikto v1.23  - www.cirt.net - Tue Apr 15 11:06:08 2003
---------------------------------------------------------------------------
+ Target IP:       192.168.0.1
.
.
.
+ /~root - Enumeration of users is possible by requesting ~username
(responds with Forbidden for real users, not found for non-existent users)
(GET).
+ /~bond - Is a valid user on the system.
+ /~hoax - Is a valid user on the system.
.
.
.
```

Potrebno je napomenuti da korištenje *mutate* opcije može generirati vrlo veliku količinu prometa na lokalnoj mreži, a samim time i preopterećenje testiranog poslužitelja, što može uzrokovati nasilnim prekidanjem njegova rada (engl. *Crash*).

4.4. Korisničko definiranje pretrage

Osim standardnih pretraga definiranih u datoteci `scan_database.db`, koja se nalazi u direktoriju `plugins`, korisnicima je ostavljena mogućnost definiranja vlastitih pretraga koje se smještaju u datoteku `user_scan_database.db` (također u `plugins` direktoriju).
Na taj način administratori mogu podesiti pravila koja su specifična za određene poslužitelje na njihovoj mreži i time olakšati redovite provjere sigurnosti poslužitelja. Pravila dodana u `user_scan_database.db` datoteku neće se brisati prilikom osvježavanja `-update` opcijom.

4.5. Osvježavanje paketa

Plugin moduli koji se isporučuju alatom pisani su u Perl programskom jeziku i osvježavaju se pokretanjem programa sa `-update` opcijom. Navedena opcija pokrenuti će skidanje posljednjih inačica plugin modula sa Web stranice cirt.net. Preuzete module poželjno je prije pokretanja programa provjeriti, kako ne bi došlo do neželjenih posljedica zbog ubacivanja malicioznog programskog koda.

5. Zaključak

Nikto se pokazao kao vrlo koristan alat za provjeru sigurnosti Web poslužitelja s mogućnošću izvršavanja vrlo brzih provjera. Prilikom provjere treba imati na umu da ovaj program generira vrlo velik broj HTTP zahtijeva prema poslužiteljima, te stoga može uzrokovati probleme u radu poslužitelja i lokalne mreže. U određenim načinima rada moguć je promet od oko 70,000 zahtijeva prema poslužitelju.
Iz navedenih razloga očito je da se ovaj alat treba koristiti s oprezom i isključivo na računalima sa vlastite računalne mreže. Korištenje ovog alata na tuđim računalnim mrežama tretira se kao maliciozna aktivnost.
Kako bi pregledavanja Nikto alatom bila precizna i pouzdana potrebno je obavljati redovito osvježavanje baze ranjivosti.