Bezbednost

Penetraciono testiranje web aplikacija i servera

Tim 2, računarstvo i automatika 2014

Sadržaj

Uvod

Potrebno je sprovesti penetraciono testiranje web aplikacija i servera upotrebom sledećih alata:

1. *Nmap* (GPL-v2 licenca)
2. *Nikto* (GPL-v3 licenca)

Web aplikacije od interesa su pokrenute na sledećim portovima:

`8080`
: back-end aplikacija

`8085`
: agentska aplikacija

`8095`
: korisnička aplikacija

Poglavlje 1. *Nmap*

Nmap koristi IP pakete na kreativne načine kako bi odredio:

- Koji uređaji su dostupni na mreži
- Koje servise (naziv aplikacije i verzija) ti uređaji nude
- Koje operativne sisteme (i njihove verzije) koriste
- Koji tipovi firewall-a su u upotrebi

Iako se *Nmap* većinom koristi za potrebe provere bezbednosti, mnogi administratori ga pronalaze korisnim za rutinske poslove, kao što je monitoring uređaja i servisa.

1.1. Skeniranje servera

Pre svega, potrebno je skenirati server kako bi se otkrilo koje servise on nudi.

U te svrhe, `nmap` *se poziva u svom osnovnom obliku:*

```
nmap {target specification}
```

Zbog uštede vremena, *Nmap* podrazumevano skenira samo najčešće korišćenih 1000 portova. Da bi se skenirali i ostali portovi potrebno je dodati opciju `-p-`.

Konkretno:

```
nmap -p- localhost
```

Rezultat Nmap skeniranja:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 13:38 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000062s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65528 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
8080/tcp open  http-proxy
8085/tcp open  unknown
8095/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

Nmap je pronašao servise od interesa na portovima `8080`, `8085` i `8095`. Za sva naredna skeniranja koristićemo opciju `-p8080,8085,8095`.

1.2. Detekcija servisa i verzije

Rezultat prethodnog skeniranja je pokazao otvorene portove i pretpostavio servise koji su pokrenuti na njima. Pretpostavka je napravljena pomoću interne baze koju *Nmap* poseduje. U bazi je naveden najčešći naziv servisa koji je pokrenut na datom portu.

Može se zaključiti da takva pretpostavka nije ispravna u našem slučaju gde su servisi pokrenuti na nestandardnim portovima.

Upotrebom opcije `-A`*, Nmap pokušava da odredi:*

- Protokol kojim servis komunicira
- Naziv aplikacije
- Broj verzije
- Tip uređaja
- Operativni sistem

Konkretan `nmap` *poziv:*

```
nmap -p8080,8085,8095 -A localhost
```

1.2.1. Rezultati detekcije

Deo rezultata:

```
8095/tcp open  http           Node.js Express framework
|_http-title: Booking

Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.14
Network Distance: 0 hops

Nmap done: 1 IP address (1 host up) scanned in 27.01 seconds
```

Nmap je uspešno otkrio da korisnička aplikacija koristi *Node.js* sa *Express* bibliotekom. Takođe, otkrio je da se radi o *GNU/Linux* operativnom sistemu, međutim pogrešio je verziju kernela.

```
uname -r
```

Tačna verzija kernela:

```
4.17.2-1-ARCH
```

Drugi deo rezultata detekcije:

```
PORT     STATE SERVICE        VERSION
8080/tcp open  ssl/http-proxy
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, RTSPRequest,
SSLSessionReq:
|     HTTP/1.1 400
|     Date: Wed, 27 Jun 2018 12:33:19 GMT
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|     Pragma: no-cache
|     Expires: 0
|     Strict-Transport-Security: max-age=31536000 ; includeSubDomains
|     X-Frame-Options: SAMEORIGIN
|     Content-Type: application/json;charset=UTF-8
|     Date: Wed, 27 Jun 2018 12:33:19 GMT
|     Connection: close
|     {"timestamp":"2018-06-27T12:33:19.565+0000","status":404,"error":"Not
Found","message":"No message available","path":"/"}
|   HTTPOptions:
|     HTTP/1.1 404
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|     Pragma: no-cache
|     Expires: 0
|     Strict-Transport-Security: max-age=31536000 ; includeSubDomains
|     X-Frame-Options: SAMEORIGIN
|     Content-Type: application/json;charset=UTF-8
|     Date: Wed, 27 Jun 2018 12:33:19 GMT
|     Connection: close
|_    {"timestamp":"2018-06-27T12:33:19.771+0000","status":404,"error":"Not
Found","message":"No message available","path":"/"}
|_http-cors: HEAD GET POST PUT DELETE TRACE OPTIONS PATCH
|_http-title: Site doesn't have a title (application/json;charset=UTF-8).
| ssl-cert: Subject: commonName=server/organizationName=FTN-
Booking/stateOrProvinceName=Serbia/countryName=RS
| Not valid before: 2018-06-14T12:59:06
|_Not valid after:  2019-06-14T12:59:06
|_ssl-date: 2018-06-27T12:33:22+00:00; 0s from scanner time.
```

sličan ispis dobije se i za port 8085

Može se primetiti da Nmap nije uspeo da detektuje *Spring Boot* aplikaciju odnosno *Apache Tomcat* server.

1.3. Sprečavanje skeniranja

Da bi se skeniranje sprečilo, može se koristiti firewall.

Jedna opcija je dodatni modul za *iptables* pod nazivom *PSD*. Princip na kojem radi *PSD* je jednostavan—ukoliko je broj zahteva sa jedne adrese veći od dozvoljenog praga, tada je ta IP adresa klasifikovana kao port skener.

Poglavlje 2. *Nikto*

Nikto je skener web servera koji pronalazi potencijalne probleme kao što su:

- Pogrešna konfiguracija servera i softvera
- Podrazumevane datoteke i programi
- Nesigurne datoteke i programi
- Zastarele verzije servera i programa

Nikto se u osnovnom obliku pokreće na sledeći način:

```
nikto -host HOSTNAME -port PORT
```

Odnosno, konkretno:

```
nikto -host localhost -port 8080,8085,8095
```

Rezultat za port 8080

```
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8080
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /emailAddress=ftn.hps@gmail.com/C=RS/ST=Serbia/L=Novi
Sad/O=FTN-Booking/OU=Team2/CN=server
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /emailAddress=ftn.hps@gmail.com/C=RS/ST=Serbia/L=Novi
Sad/O=FTN-Booking/OU=Team2/CN=server
+ Start Time:         2018-06-27 15:13:12 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname 'localhost' does not match certificate's names: server ①
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS ②
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save
files on the web server. ②
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files
on the web server. ②
+ 7375 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2018-06-27 15:15:17 (GMT2) (125 seconds)
```

① Problem postoji zato što je server pokrenut na localhost-u.

② Sve HTTP metode su potrebne zato što se radi o REST servisu.

sličan ispis dobije se i za port 8085

Rezultat za port 8095

```
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8095
+ Start Time:         2018-06-27 15:15:17 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express ①
+ Server leaks inodes via ETags, header found with file /, fields: 0xW/fb7
0x16436b18afd ②
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 14886 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2018-06-27 15:15:41 (GMT2) (24 seconds)
---------------------------------------------------------------------------
```

① Potencijalni problem, zato što napadač zna koja biblioteka je korišćena

② Lažno pozitivna informacija koju *Nikto* generiše ukoliko ETag header sadrži `-`.

Problem <1> se može rešiti dodatnom konfiguracijom korisničke aplikacije.

Preciznije, potrebno je dodati:

```
app.disable('x-powered-by');
```