Održavanje sigurnosne razine mrežnih servisa računalnog sustava programskim paketom NMAP

Pavelić, Krešimir; Bauer, Denis; Jažić, Ivica

Source / Izvornik: **OTO 2018 : zbornik radova, 2018, 135 - 140**

Conference paper / Rad u zborniku

Publication status / Verzija rada: **Published version / Objavljena verzija rada (izdavačev PDF)**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:133:855672

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

GRAĐEVINSKI I ARHITEKTONSKI FAKULTET OSIJEK
Faculty of Civil Engineering and Architecture Osijek

Repository / Repozitorij:

Repository GrAFOS - Repository of Faculty of Civil Engineering and Architecture Osijek

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Održavanje sigurnosne razine mrežnih servisa računalnog sustava programskim paketom NMAP

Professional paper

Krešimir Pavelić
Sveučilište Josipa Jurja Strossmayera
Građevinski fakultet Osijek
Vladimir Preloga 3, 31000 Osijek, Hrvatska
kreso@gfos.hr

Denis Bauer
Prvo plinarsko društvo
Kardinala Alojzija Stepinca 27, 32000 Vukovar
denosk@gmail.com

Ivica Jažić
HEP Plin d.o.o.
Cara Hadrijana 7, 31000 Osijek, Hrvatska
ivica.jazic@hep.hr

Sažetak – *Članak opisuje rad sa programskim paketom NMAP kao i načine detekcije portova na ciljanim računalima u mreži. Opisane su vrste provjere stanja portova i aplikacija na njima, te načini održavanja trenutnog nivoa sigurnosti. Prikazani su i neki od primjera kako zlonamjerni napadači mogu koristiti isti programski paket radi iskorištavanja nedostataka i prikupljanja podataka o sustavu s ciljem planiranja napada na računala ili sustav u cjelini.*
Ključne riječi – *NMAP, računalni sustav, održavanje, sigurnost, port*

Maintaining the level of security of network services with the computer system package NMAP

Abstract – *The article describes how to work with the NMAP program as well as how to detect ports on target computers in the network. Port and application statuses are described, and ways to maintain the current level of network security. There are also some ways that malicious attackers can use the same program suite to exploit the disadvantages and gather information about the system to target attacks on computers or the system as a whole.*
Keywords – *NMAP, computer system, maintenance, security, port*

1. UVOD

Pod pojmom sigurnosti mrežnih (informatičkih) sustava podrazumijevamo bilo koju aktivnost usmjerenu zaštiti samog mrežnog sustava u cjelini kao i njegovih podataka. Dva su osnovna načina zaštite: programski (software) i fizička zaštita opreme koja je sastavni element sustava (hardware).

Najčešći problemi koji se javljaju prilikom održavanja sigurnosti mrežnih sustava su detekcija i otklanjanje zlonamjernih programa koji mogu dovesti do krađe poslovnih i osobnih podataka te identiteta zaposlenih i time uzrokovati poslovni i financijski gubitak korisnika štićenog mrežnog sustava. Također, treba obratiti pozornost i na korisnike samog sustava (zaposlenike) koji svojom namjerom ili nenamjerom mogu dovesti do narušavanja sigurnosti mrežnog sustava.

U ovom radu opisujemo rad sa programskim paketom NMAP, odnosno jedan njegov osnovni dio koji služi za početnu detekciju otvorenih portova koji mogu služiti neovlaštenom napadaču za ulaz u štićeni sustav, te vrste zaštite i održavanja tražene sigurnosne razine mrežnih servisa. Nmap (Network Mapper) je program otvorenog koda (open source) čija je namjena istraživanje računalne mreže i računalnog sustava.

U svojoj pretrazi otkriva računala koja su dostupna na mreži, verzije operativnih sustava koje se na njima nalaze, portove koji su na njima otvoreni, pokrenute servise i otkrivene nedostatke bitne za administriranje i otkrivanje sigurnosnih propusta radi održavanja ili povećanja sigurnosti samog sustava.

Nakon pokretanja pretrage, izvještaj sadrži podatke o ciljanom računalu, stanju portova i operativnom sustavu.

2. PRIMJER SKENIRANJA CILJANOG RAČUNALA

U primjeru na slici 1., zatraženo je skeniranje (pretraga) računala koje se nalazi na adresi 161.53.203.179 pomoću naredbe:

nmap -A 161.53.203.179

Prekidač A nam omogućuje da saznamo verziju operativnog sistema na ciljanom računalu uz vrstu i broj otvorenih portova.

Iz izvještaja se mogu saznati slijedeći podatci:

1. Nmap je otkrio 997 zatvorenih portova te dva porta koji su otvoreni i koji su nam time zanimljivi za analizu.

Stanje portova može biti izraženo kroz četiri tipa: otvoreni, zatvoreni, filtrirani, nefiltrirani.

Otvoreni - označava da na određenom portu postoji program (aplikacija) koja sluša stanje i prima/šalje informacije preko tog porta.

Zatvoreni - nema aplikacije na tim portovima.

Filtrirani - oznaka porta kojega brani ili vatrozid, paket filter ili nešto drugo, te NMAP ne može odrediti da li je taj port otvoren ili zatvoren.

Nefiltrirani - Nmap dobija odgovor od tog porta ali nije u stanju decidirano odrediti da li je taj port otvoren ili zatvoren.

2. Jedina dva porta koja su otvorena na skeniranom računalu su 80/tcp i 22/tcp.

Port 80 - *HTTP Hyper Tekst Transfer Protocol* - protokol koji se koristi za prijenos datoteka i općenito resursa na internetu te omogućuje objavljivanje i prezentaciju internet www stranica.

Port 22 - *ssh (Secure shell)* - mrežni protokol koji služi za uspostavljanje sigurnog komunikacijskog kanala između dva računala u računalnoj mreži.

3. Otkrivena je vrsta operativnog sustava i programa koji se koristi na računalu:

- Linux 3.19, Ubuntu verzija

- web server Apache 2.4.18.

- open SSH 7.2p2

Rezultati pretrage, kao i otvoreni portovi sa programskim paketima koji ih koriste su vidljivi na slici 1.

```
root@vijece:~# nmap -A 161.53.203.15

Starting Nmap 7.01 ( https://nmap.org ) at 2018-02-08 08:45 CET
Nmap scan report for gfosweb.gfos.hr (161.53.203.15)
Host is up (0.00026s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
80/tcp  open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
222/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 06:5b:dc:a9:71:58:a1:fe:f7:c4:0b:70:5f:72:48:0d (DSA)
|   2048 f3:bd:22:38:ec:e7:4f:50:8b:70:fc:31:eb:79:6f:4a (RSA)
|_  256 4d:29:82:47:39:f7:ad:55:1e:b0:9e:fa:dd:80:6a:1e (ECDSA)
MAC Address: 00:15:17:27:F5:F4 (Intel Corporate)
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 3.2 - 4.0
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.26 ms gfosweb.gfos.hr (161.53.203.15)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

Sl. 1. Primjer provjere ciljanog računala na adresi 161.53.203.179

3. OTKRIVANJE SIGURNOSNIH NEDOSTATAKA I MOGUĆNOSTI ZAŠTITE

Slijedeći korak je pokušati saznati informacije o verzijama programa koji koriste otvorene portove, te saznati postoje li sigurnosni nedostatci koji mogu zlonamjernom napadaču pružiti priliku da preko tih portova i aplikacija izvrše neovlašteni ulaz u zaštićeni sustav.

Na Internet stranici www.cvedetails.com provjeravamo sigurnosne nedostatke za web server Apache inačica 2.4.18., kao i za SSH verzije 7.2.p2. Rezultati su vidljivi na slikama 2 i 3.

Nakon toga, potrebno je upoznati se sa mogućnostima primjene pojedinih programskih nadogradnji ili postupaka koji su opisani u uputama izdanim uz svaki tip sigurnosnih propusta koji su do sada otkriveni.

Također treba primijeniti postupke opisane za pojedine sigurnosne nedostatke.

Internet stranice, kao i općenito izvori informacija koji služe za objašnjenja sigurnosnih nadogradnji ovise o samim sistem administratorima. U radu smo se bazirali na nekoliko nama prihvatljivih izvora, no to je subjektivan odabir onoga tko je zadužen za održavanje sigurnosti samih računala kao i mrežnog računalnog sustava u cjelini.

Na istoj Internet stranici na kojoj smo tražili opise sigurnosnih nedostataka nalaze se primjeri, rješenja i poveznice sa novim verzijama aplikacija u kojima su primjećeni nedostatci možebitno ispravljeni.

Slike 2 i 3 nam pokazuju primjer kako se za određene sigurnosne nedostatke mogu pronaći i njihove oznake, datum kada su otkriveni nedostatci, opise istih te načine i mjere koje treba poduzeti kako bi se održala razina sigurnosti u samom sustavu.

Što je veća ocjena sigurnosnog nedostatka to je njemu pridata veća važnost (opasniji je). Ukoliko u sustavu postoji više nedostataka, prvo se rješavaju oni sa većom ocjenom a nakon toga oni s manjom ocjenom.

Openbsd » Openssh » 7.2 P2 : Security Vulnerabilities

Cpe Name:*cpe:/a:openbsd:openssh:7.2:p2*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

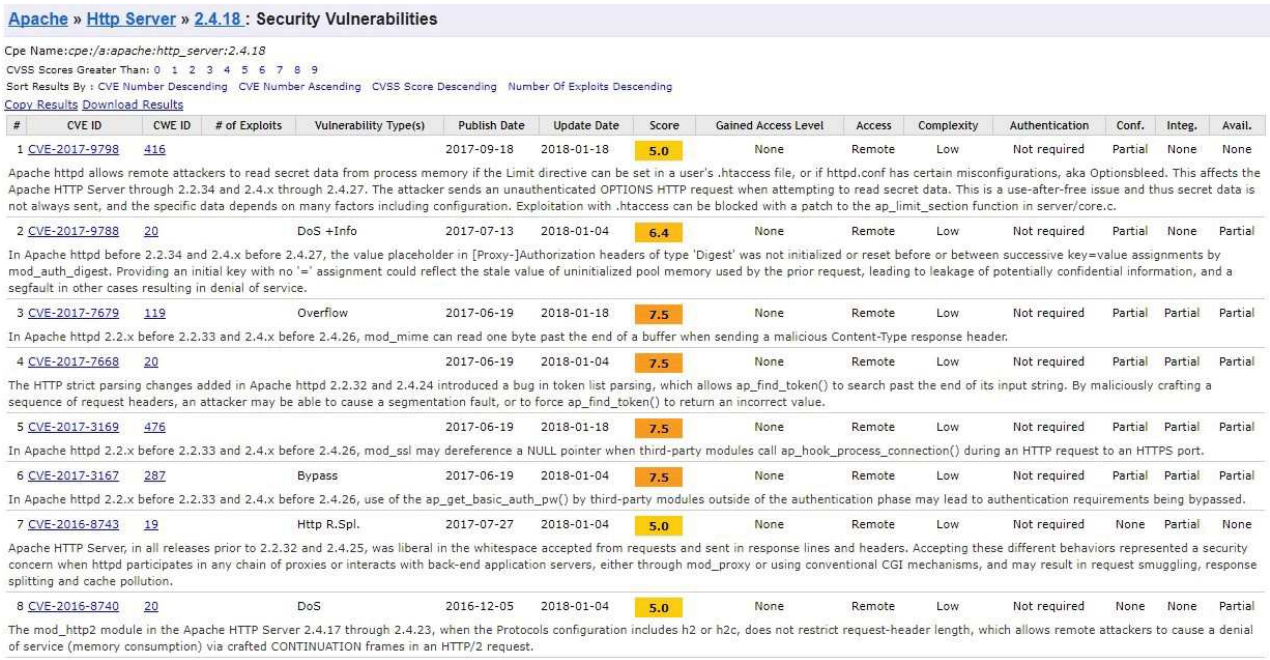
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-15906	275			2017-10-25	2018-01-31	5.0	None	Remote	Low	Not required	None	Partial	None
The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.														
2	CVE-2016-8858	399		DoS	2016-12-09	2018-02-03	7.8	None	Remote	Low	Not required	None	None	Complete
** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue."														
3	CVE-2016-6515	20		DoS	2016-08-07	2018-01-04	7.8	None	Remote	Low	Not required	None	None	Complete
The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.														
4	CVE-2016-6210	200		+Info	2017-02-13	2018-01-04	4.3	None	Remote	Medium	Not required	Partial	None	None
sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.														
5	CVE-2015-8325	264		+Priv	2016-04-30	2018-01-04	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.														

Total number of vulnerabilities : 5 Page : 1 (This Page)

Sl. 2. Primjer otkrivanja sigurnosnih nedostataka za programski paket SSH, verzije 7.2.P2



Apache » Http Server » 2.4.18 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.4.18*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2017-9798	416			2017-09-18	2018-01-18	5.0	None	Remote	Low	Not required	Partial	None	None
	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.													
2	CVE-2017-9788	20		DoS +Info	2017-07-13	2018-01-04	6.4	None	Remote	Low	Not required	Partial	None	Partial
	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.													
3	CVE-2017-7679	119		Overflow	2017-06-19	2018-01-18	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.													
4	CVE-2017-7668	20			2017-06-19	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.													
5	CVE-2017-3169	476			2017-06-19	2018-01-18	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.													
6	CVE-2017-3167	287		Bypass	2017-06-19	2018-01-04	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.													
7	CVE-2016-8743	19		Http R.Spl.	2017-07-27	2018-01-04	5.0	None	Remote	Low	Not required	None	Partial	None
	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.													
8	CVE-2016-8740	20		DoS	2016-12-05	2018-01-04	5.0	None	Remote	Low	Not required	None	None	Partial
	The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.													

Sl. 3. Primjer otkrivanja sigurnosnih nedostataka za web server Apache, verzije 2.4.18

U primjeru prikazanom na slici 4. naveden je primjer sigurnosnog nedostataka Apache poslužitelja oznake CVE-2017-3167.

Koristeći ovaj nedostatak, potencijalni napadač može zaobići postupak autentifikacije. Također je moguća izmjena određenih sistemskih datoteka.

Jedan od načina rješavanja problema je nadogradnja Apache web servera na noviju verziju u kojoj je ispravljen taj nedostatak.



Vulnerability Details : CVE-2017-3167

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
Publish Date : 2017-06-19 Last Update Date : 2018-01-04

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	287

Sl. 4. Opis sigurnosnog nedostatka Apache (web server) poslužitelja

Slika 5. prikazuje Nmap pretragu računala internetskih stranica Građevinskog Fakulteta u Osijeku.

Za razliku od prethodnog računala, ovdje je otkriven i port 21 koji služi za *FTP (File Transfer Protocol)* komunikaciju.

Također pretragom je otkriveno da su izrazito stare verzije Apache web servera 2.4.7. za razliku od 2.4.18 trenutne verzije, te SSH 6.6 a trenutna je verzija 7.2.

Običnim slijedom naredbi *sudo apt-get update/upgrade* potrebno je nadograditi pakete na aktualne verzije te provjerama sigurnosnih nedostataka obaviti podešavanje konfiguracijskih datoteka ukoliko to bude potrebno.

```
root@vijece:~# nmap -A 161.53.203.15

Starting Nmap 7.01 ( https://nmap.org ) at 2018-02-08 08:45 CET
Nmap scan report for gfosweb.gfos.hr (161.53.203.15)
Host is up (0.00026s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
80/tcp  open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
222/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 06:5b:dc:a9:71:58:a1:fe:f7:c4:0b:70:5f:72:48:0d (DSA)
|   2048 f3:bd:22:38:ec:e7:4f:50:8b:70:fc:31:eb:79:6f:4a (RSA)
|_  256 4d:29:82:47:39:f7:ad:55:1e:b0:9e:fa:dd:80:6a:1e (ECDSA)
MAC Address: 00:15:17:27:F5:F4 (Intel Corporate)
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 3.2 - 4.0
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.26 ms gfosweb.gfos.hr (161.53.203.15)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.27 seconds
```

Sl. 5. Primjer pretrage starih internetskih stranica Građevinskog fakulteta Osijek

4. MOGUĆNOSTI ZLOUPORABE OD STRANE NAPADAČA

Bitno je napomenuti da osim sistemskih i mrežnih administratora, Nmap za prikupljanje informacija koriste i napadači (hakeri). Informacije prikupljene ovim programom koriste za planiranje napada na računala ili mrežu. Prikupljanje informacija je najkritičniji korak u čitavoj fazi napada, jer krive ili nepotpune informacije rezultiraju neuspješnim napadom. Napadači također, kao i administratori, pokreću Nmap i analiziraju izvještaj. Za prepoznate operacijske sustave, aplikacije ili servise, pronalaze ranjivosti i napadaju računalo ili mrežu preko tih ranjivosti. Osim već pronađenih i dokumentiranih ranjivosti, sposobniji napadači su u stanju pronaći i nove, nedokumentirane.

Dosadašnja sigurnosna preporuka je određivala da u mreži postoji sustav koji detektira skeniranje ili pokušaje napada (IDS - Intrusion Detection System). Ti sustavi dolaze sa setovima previla koji detektiraju skeniranje računala i upozoravaju administratora. Na žalost, Nmap je moguće konfigurirati na raznolike načine što otežava IDS-u prepoznavanje skeniranja.

4.1 Prikriveno skeniranje (Stealth scan)

Ova opcija pokreće skeniranje u kojem se ne završava proces uspostave TCP konekcije. Takvo skeniranje najčešće prolazi neopaženo jer je uspostava konekcije prekinuta prije završetka.

Skeniranje se vrši na slijedeći način: Napadač šalje serveru zahtjev za povezivanje s specijalni dijelom TCP paketa, takozvanim SYN bitom koji je postavljen na 1. Ciljano računalo zaprimi zahtjev i šalje segment kojim odobrava uspostavu veze s napadačem u kojem se

nalaze oznake SYN bita=yes (1) te ACK (acknowledge). Napadač prima te pakete te ne vraća potvrdu ciljanom računalo o dobijanju segmenta odobravanja veze, čime veza nije uspostavljena.

Primjer:

nmap 192.168.0.34 -sS

4.2 Vremensko podešavanje (Timing)

Nmap automatski podešava vremenske periode između slanja signala ovisno o brzini mreže i vremenu odziva računala. Napadač može koristiti vremensko podešavanje koje mu najviše odgovara. Vremensko podešavanje omogućava napadaču da ili završi skeniranje brže ili da skeniranje bolje sakrije od IDS-a.

Primjer:

nmap 192.168.0.34 -T0

Između slanja svakog paketa mora proći barem 5 minuta. Takvo skeniranje je izuzetno teško identificirati jer su zapisi toliko vremenski razmaknuti da ih je u analizi teško povezati.

nmap 192.168.0.34 -T5

Skeniranje će biti izvršeno u što kraćem roku i može rezultirati gubitkom informacija. Što je veći broj iza prekidača T skeniranje je brže

4.3 Mamci (Decoys)

Pomoću ove opcije, napadač može pokrenuti skeniranje koje će izgledati da dolazi sa više različitih računala. Ne sakriva adresu napadača, ali je teško odrediti izvor skeniranja.

Primjer:

nmap 192.168.0.34 -D 192.168.0.101,192.168.0.102,192.168.0.103

Osim navedenih opcija skeniranja, postoje i naprednije koje se rjeđe koriste. Te naprednije tehnike često ne daju rezultate jer predugo traju (Idle skeniranje) ili se koristi moderna oprema koja je imuna na takvo skeniranje (Fragmentiranje).

Zbog svoje svestranosti i dostupnosti Nmap je vrlo popularan kod mrežnih stručnjaka i napadača. Logično je korištenje takvog programa u obadvije svrhe jer informacije dobivene ovakvim programom ukazuju na ranjivosti mrežnih servisa. Mrežni administratori moraju znati ranjivosti da bi ih otklonili ili dodatno osigurali, a napadači koriste ranjivosti za nedozvoljen ulaz u sustav.

5. ZAKLJUČAK

Zaštita računala i sustava se u grubo može podijeliti na hardversku i softversku. Računalni i mrežni administratori zaduženi za sigurnost računalnog sustava, u svom radu se koriste čitavom paletom programskih rješenja.

Nerijetko su i sami primorani koristeći svoja znanja prepravljati kodove i izmišljati načine zaštite.

Operativni sustavi koji se koriste na računalima unutar samog štićenog mrežnog sustava (Windows, Linux, MAC OS), često nakon instalacije ostavljaju veliki broj portova (vrata) otvorenima.

Zadatak mrežnih administratora je provjera svakog aktivnog dijela opreme (računala, usmjerivači, mrežni prilagodnici, pisači itd.) te ukoliko je potrebno izvršavanje skupa naredbi i/ili podešavanje dodatnih programskih paketa s ciljem povećanja ili održavanja zadatog nivoa mrežne sigurnosti.

Programski paket NMAP im omogućuje i olakšava pretragu za sigurnosnim nedostatcima u samom sustavu te pomaže da se nivo sigurnosti samog sustava održi na željenom nivou. NMAP ima daleko više mogućnosti nego što je opisano u ovome članku, pa se administratori sustava ukoliko ga žele koristiti trebaju podrobnije upoznati s njim.

Načini na koje se može spriječiti NMAP pretraga sa vanjskih računala, svode se na korištenje alata poput programskog paketa HIDS (Host based intrusion detection system) koji omogućava administratorima da primjete takav pokušaj i reagiraju u skladu s naputcima vezanim za isti ili sa vatrozidovima koji će na isti način pokušati blokirati i/ili dojaviti pojavu pretrage portova.

6. LITERATURA

[1] https://sysportal.carnet.hr/node/2 NMAP 4.0 Carnet Sys portal.

[2] https://nmap.org/man/hr/index.html Nmap vodič (upute).

[3] https://www.cvedetails.com, list of Vulnerabilities for Apache and SSH.

[4] A.J. Bennieston, "NMAP - A stealth Port Scanner", http://nmap.org/bennieston-tutorial/

[5] Primjeri pretrage, izvori: Građevinski fakultet Osijek, https://www.tecmint.com/nmap-command-examples