

Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode *Ethical Hacking*

Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods

Yusuf Muhyidin¹, M. Hafid Totohendarto², Erina Undamayanti³, Salsabilla C.N⁴

Sekolah Tinggi Teknologi Wastukancana

*yusufmuhyidin@stt-wastukancana.ac.id, hafid@stt-wastukancana.ac.id,
erinaundamayanti01@gmail.com, salsabillachoirunnisa08@gmail.com*

Corresponding author : yusufmuhyidin@stt-wastukancana.ac.id

Keamanan website perlu menjadi perhatian di tengah banyaknya kasus peretasan website dari pihak yang tidak bertanggung jawab. Keamanan website merupakan upaya untuk melindungi website dari serangan hacker yang terhubung melalui suatu jaringan. Situs website yang dapat diakses secara online dapat menciptakan kerentanan terhadap ancaman dari serangan hacker. Untuk meminimalkan kerentanan ini, perlu untuk menguji website yang lebih tinggi dan menganalisis tingkat keamanan website tersebut. Metode yang digunakan dalam penelitian ini adalah metode *Ethical Hacking* yang menitikberatkan pada teknik *footprinting* dan *vulnerability scanning*. Hasil penelitian ini telah menemukan informasi terkait dengan website target yaitu web A, B, dan C, dapat diketahui IP target, hostname target, port target, lalu jenis server yang digunakan website tersebut.

Kata kunci: *Ethical Hacking, Footprinting, Vulnerability Scanning*

Website security needs to be a concern in the midst of many cases of website hacking from irresponsible parties. Website security is an effort to protect websites from hacker attacks that are connected through a network. Websites that can be accessed online can create vulnerabilities to threats from hacker attacks. To minimize these vulnerabilities, it is necessary to test higher websites and analyze the security level of those websites. The method used in this study is the Ethical Hacking method which focuses on footprinting techniques and vulnerability scanning. The results of this study have found information related to the target website, namely A, B, and C, it can be seen the target IP, target hostname, target port, and the type of server used by the website.

Keywords: *Ethical Hacking, Foot Printing, Vulnerability Scanning*

1 Pendahuluan

Di era Perkembangan teknologi informasi saat ini perkembangan website sangatlah pesat, hal ini berdasarkan jumlah pengguna layanan internet yang semakin bertambah dari tahun ke tahun. Beberapa website yang sering dikunjungi adalah *Search Engine*, *e-commerce*, *media social*, *portal berita* dan lain-lain. Dari kemudahan yang diberikan oleh website tersebut terdapat beberapa masalah pada celah kemanan contohnya seperti *SQL Injection*, *cross-site scripting* *CSRF* dan banyak lagi. Seorang hacker dapat memanfaatkan celah kemanan yang ada untuk melakukan exploitasi pada web tersebut.

Website adalah sekumpulan script yang digunakan untuk menampilkan informasi teks, gambar, animasi, suara, dan atau gabungan dari semuanya, baik yang bersifat statis ataupun dinamis dimana membentuk suatu rangkaian yang saling berhubungan halaman satu dengan halaman lainnya. (Bekti, 2015:35)

Keamanan merupakan keadaan bebas dari bahaya. Keamanan diusahakan mempunyai unsur-unsur misal adanya proteksi, integritas, keaslian suatu data, dan mempunyai hak akses. Keamanan website merupakan sebuah upaya untuk melindungi &

menjaga website dari serangan hacker. Keamanan sebuah website sangatlah penting, mengingat akses ke internet yg terbuka dan bebas. Selain memberikan informasi diera modern saat ini website juga berkembang menjadi salah satu cara bertransaksi secara online. (Palmer, 2001)

Dari sekian banyak tahapan yang dilakukan seorang hacker untuk menyusup kedalam web atau jaringan yang pertama dilakukan adalah *vulnerability assesment* dan *information gathering*.

Tujuan dari penelitian ini adalah untuk mengetahui keamanan dari beberapa website untuk dibandingkan dan sejauh mana aplikasi nmap & nikto dapat mendeteksi kelemahan sebuah website.

Berdasarkan uraian tersebut maka peneliti mencoba melakukan penelitian untuk menganalisis tingkat keamanan website (nama website kami samarkan menjadi A,B dan C) menggunakan metode *ethical hacking* dengan membandingkan kinerja tool nmap dan nikto.

2. Kajian Pustaka

2.1 Ethical Hacking

Ethical Hacking merupakan suatu aktifitas melakukan penetrasi ke suatu sistem, jaringan, dan aplikasi dengan cara mengesploitasi kelemahan dengan maksud untuk mendapatkan hak akses atas data dan sistem, tujuannya adalah membantu perusahaan menguji keamanan system dan jaringan yang mereka miliki. Oran yang melakukan ethical hacking disebut sebagai *Ethical Hacker*. Teknik yang digunakan oleh ethical hacker dan hacker hampir sama hanya saja tujuanya berbeda.

Ethical Hacker sangat diperlukan oleh perusahaan yang ingin menguji sistem yang dimiliki untuk diekploitasi dan dicari *vulnerability* nya sehingga ditemukan resiko yang disebabkan dari *vulnerability* tersebut. (Palmer, 2001)

2.2 Vulnerability Assesement

Vulnerability assessment dilakukan untuk mengetahui celah-celah yang berpotensi masuknya serangan. Selain itu juga untuk mengetahui masa berlakunya versi sebuah software, port yang terbuka, dan aplikasi apa saja yang sedang berjalan pada sistem tersebut. *Vulnerability assessment* digunakan untuk mendeteksi kelemahan dalam jaringan. (Aboelfotoh & Haikal, 2019)

2.3 Information Gathering

Pencarian informasi (*Information Gathering*) adalah fase untuk mendapatkan informasi target serangan baik itu individu ataupun perusahaan. Meliputi pencarian informasi secara detail, Termasuk menggali untuk mendapatkan informasi yang akurat. (Palmer, 2001)

2.3.1 Reconnaissance

Reconnaissance adalah sebuah fase persiapan sebelum (*attacker*) melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Teknik ini akan menyertakan *network scanning* baik melalui jaringan internal atau external yang tentu saja tanpa mengantongi izin. (Palmer, 2001)

2.3.2 Footprinting

Footprinting adalah tahap mengumpulkan informasi sebelum melakukan penyerangan terhadap web atau system dengan cara mengumpulkan informasi target yang tujuannya adalah untuk merangkai apa yang ditemukan (blueprint dari suatu jaringan) hasilnya bisa berupa nama domain, nomor telepon email dan lain-lain. (EC-Council, 2012)

2.4 Network Scanning

Network scanning merupakan cara yang digunakan untuk melakukan *scanning* pada mesin jaringan, baik itu untuk mendapatkan IP, Port, Packet data yang keluar masuk melalui jaringan, termasuk merekam aktifitas browsing, yang tentunya terdapat *password* dan *username*. (Rohinet, Abdul Rahman, 2019)

2.5 Port Scanning

Port Scanning adalah aktivitas yang dilakukan untuk memeriksa status *port* TCP dan UDP pada sebuah mesin, tujuannya adalah untuk mengetahui kelemahan suatu sistem dari *port* yang terbuka dan OS yang digunakan. banyak aplikasi yang bisa digunakan untuk *scanning* ini salah satunya adalah Nmap. (Shidiqpu, 2009)

2.6 NMAP (Network Mapper)

Nmap atau Network Mapper adalah aplikasi terbuka yang dipakai khusus untuk eksplorasi jaringan dan audit keamanan jaringan. Fyodor Vaskovich adalah orang yang pertama kali mengembangkan Nmap pada tanggal 1 september 1997. Fyodor Vaskovich adalah salah satu pendiri Honeynet project yaitu sebuah organisasi yang melakukan riset untuk keamanan jaringan computer. (Abdullah, 2016)

a. Nmap -sS

SYN scan digunakan untuk membedakan 3 state *port* yaitu *open*, *filtered* ataupun *close*. Teknik ini dikenal sebagai *half open scanning* karena suatu koneksi penuh TCP tidak sampai terbentuk

b. Nmap -sF

Teknik ini mengirim suatu paket FIN ke *port* sasaran. Berdasarkan RFC 793, sistem sasaran akan mengirim balik suatu RST untuk setiap *port* yang tertutup

c. Nmap -A

Nmap -A adalah perintah yang memberi tahu Nmap untuk menemukan dan menampilkan informasi *Operation Sistem* tentang host/ip target. Nmap -A bisa juga disebut sebagai *agresif scanning* karena hasil dari *scanning* menggunakan perintah tersebut sangat lengkap.

d. Nmap -O

Nmap -O memungkinkan deteksi OS untuk host atau rentang host.

e. Nmap -sV

Untuk mendeteksi informasi layanan dan versi. Pengguna jahat biasanya menggunakan ini untuk memeriksa apakah host menjalankan layanan yang rentan atau tidak.

f. Nmap -sX

Teknik ini mengirimkan paket *FIN*, *URG* dan *PUSH* ke *port* sasaran. Berdasarkan RFC 739, sistem sasaran akan mengembalikan suatu *RST* untuk semua *port* yang tertutup

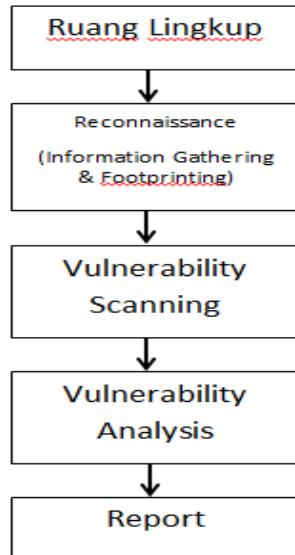
2.7 Nikto

Nikto adalah sebuah webserver dan sekaligus alat untuk penilaian aplikasi web untuk menemukan masalah keamanan dan kerentanan pada web tersebut. Nikto dapat memindai 6700 file/program yang berpotensi berbahaya.

3. Metode

Penelitian ini dilakukan menggunakan metode *Ethical Hacking*, dimana peneliti akan menekankan penelitian dalam tahapan *Footprinting* dan *Vulnerability Scanning* untuk melakukan pengujian *vulnerability*. Adapun objek (target) dalam penelitian ini yaitu website A, B, C, yang akan dilakukan pengujian *vulnerability* menggunakan tools (Nmap dan Nikto).

Berikut adalah tahapan-tahapan yang dilakukan dalam penelitian ini:



Gambar 3.1 Tahapan Pengujian

Berikut ini adalah penjelasan tahapan-tahapan yang dilakukan pada penelitian ini:

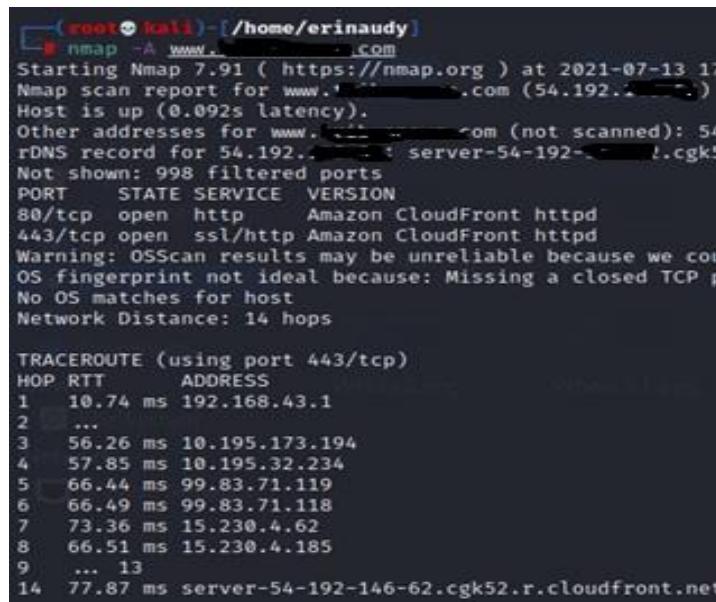
- 1) **Ruang Lingkup (Scope)**
Tahapan awal adalah menetukan batasan terhadap website yang menjadi target yaitu Web A, B, dan C. Peneliti hanya akan melakukan *vulnerability scanning* dan tidak melakukan eksplorasi terhadap website tersebut.
- 2) **Reconainsance (Footprinting dan Information Gathering)**
Tahapan ini dilakukan untuk mendapatkan informasi sebanyak-banyaknya terkait dengan perangkat apa saja yang digunakan, versi OS dan lain-lain.
- 3) **Vulnerability Scanning**
Tahapan ini melakukan *scanning* dengan memanfaatkan tools yang ada, agar mendapatkan informasi seperti daftar port yang terbuka dan lain-lain.
- 4) **Vulnerability Analysis**
Tahap ini peneliti melakukan analisis terhadap informasi yang ditemukan setelah dilakukan *scanning* terhadap website target.
- 5) **Report**
Tahapan ini adalah hasil analisa dari celah keamanan website target yang akan diberikan kepada pengelola website target untuk mengetahui apa saja kelemahan yang ada dalam website tersebut.

4 Hasil dan Pembahasan

Hasil dari pengujian perbandingan keamanan pada 3 website menggunakan nmap dan nikto yaitu sebagai berikut:

4.1 Network Scanning Menggunakan Nmap pada ketiga web

- Menggunakan Perintah Nmap -A

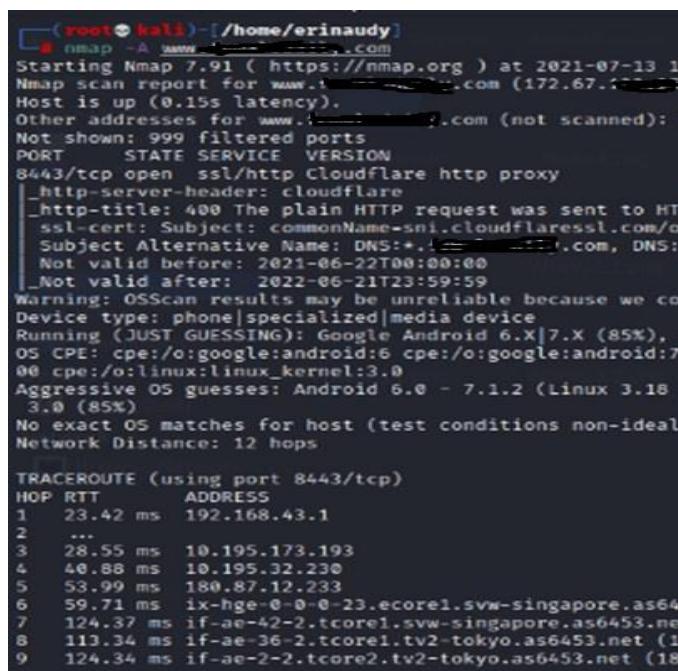


```
(root㉿kali)-[~/home/erinaudyy]
# nmap -A www. ....com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 17:17
Nmap scan report for www. ....com (54.192.1. ....)
Host is up (0.092s latency).
Other addresses for www. ....com (not scanned): 54.192.1. ....
rDNS record for 54.192.1. ....: server-54-192-1-....cgk5
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Amazon CloudFront httpd
443/tcp   open  ssl/http Amazon CloudFront httpd
Warning: OSScan results may be unreliable because we could not
OS fingerprint not ideal because: Missing a closed TCP port
No OS matches for host
Network Distance: 14 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  10.74 ms  192.168.43.1
2  ...
3  56.26 ms  10.195.173.194
4  57.85 ms  10.195.32.234
5  66.44 ms  99.83.71.119
6  66.49 ms  99.83.71.118
7  73.36 ms  15.230.4.62
8  66.51 ms  15.230.4.185
9  ...
14 77.87 ms  server-54-192-146-62.cgk52.r.cloudfront.net
```

Gambar 1. nmap -A web “A”

Dari proses *network scanning* nmap pada website “A” yang telah dilakukan, dapat diketahui version dari *port* yang terbuka (*open*), contohnya pada *port* 80/tcp, statusnya *open*, service yang dipakai adalah http, dan versionnya adalah *Amazon CloudFront httpd*. Selain itu, pada *network distance* muncul *output* 14 hops, artinya ada 14 gerbang untuk menuju ke internet.



```
(root㉿kali)-[~/home/erinaudyy]
# nmap -A www. ....com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 17:17
Nmap scan report for www. ....com (172.67.1. ....)
Host is up (0.15s latency).
Other addresses for www. ....com (not scanned): 172.67.1. ....
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
8443/tcp  open  ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=sni.cloudflaressl.com/or...
|   Subject Alternative Name: DNS:*.....com, DNS:*.....com
| Not valid before: 2021-06-22T00:00:00
|_Not valid after: 2022-06-21T23:59:59
Warning: OSScan results may be unreliable because we could not
Device type: phone|specialized|media device
Running (JUST GUESSING): Google Android 6.X|7.X (85%), ...
OS CPE: cpe:/o:google:android:6 cpe:/o:google:android:7
|_cpe:/o:linux:linux_kernel:3.0
Aggressive OS guesses: Android 6.0 - 7.1.2 (Linux 3.18 - 3.0 (85%)
No exact OS matches for host (test conditions non-ideal)
Network Distance: 12 hops

TRACEROUTE (using port 8443/tcp)
HOP RTT      ADDRESS
1  23.42 ms  192.168.43.1
2  ...
3  28.55 ms  10.195.173.193
4  40.88 ms  10.195.32.230
5  53.99 ms  180.87.12.233
6  59.71 ms  ix-hge-0-0-0-23.ecore1.svw-singapore.as6453.net
7  124.37 ms  if-ae-42-2.tcore1.svw-singapore.as6453.net
8  113.34 ms  if-ae-36-2.tcore1.tv2-tokyo.as6453.net (128.113.34.8)
9  124.34 ms  if-ae-2-2.tcore2.tv2-tokyo.as6453.net (128.124.34.9)
```

Gambar 2. nmap -A web “B”

Dari proses *network scanning* Nmap -A pada website “B” yang telah di lakukan, dapat diketahui version dari *port* yang terbuka (*open*), contohnya pada *port* 8443/tcp, statusnya *open*, service yang dipakai adalah ssl/http, dan versionnya adalah Cloudflare http proxy. Selain itu, pada *network distance* muncul *output* 12 hops, artinya ada 12 gerbang untuk menuju ke internet.

```

root@kali:~/home/erinaudy]# nmap -A www.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-1
Nmap scan report for www.nmap.org (172.16.4.1)
Host is up (0.16s latency).
Other addresses for www.nmap.org (not scanned):
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Cloudflare http proxy
|_http-title: Did not follow redirect to https://www.
443/tcp   open  ssl/http Cloudflare http proxy
|_http-title: 403 Forbidden
8080/tcp  open  http   Cloudflare http proxy
|_http-title: 521 Origin Down
8443/tcp  open  ssl/http Cloudflare http proxy
|_http-title: Site doesn't have a title.
|_ssl-cert: Subject: commonName=sni.cloudflaressl.co
Subject Alternative Name: DNS:sni.cloudflaressl.co
Not valid before: 2021-01-22T00:00:00
Not valid after:  2022-01-21T23:59:59
Warning: OSScan results may be unreliable because we
Device type: phone|specialized|media device
Running (JUST GUESSING): Google Android 7.X (85%), L
OS CPE: cpe:/o:google:android:7.0 cpe:/o:linux:linux
Aggressive OS guesses: Android 7.0 (Linux 3.18) (85%
No exact OS matches for host (test conditions non-id
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  9.20 ms   192.168.4.1
2  ...
3  84.81 ms  10.195.173.193
4  86.15 ms  10.195.32.202
5  86.19 ms  180.87.12.233
6  84.87 ms  ix-hge-0-0-0-23.ecore1.svw-singapore.a

```

Gambar 3. Nmap -A web “C”

Dari proses *network scanning* Nmap -A pada website “C” yang telah di lakukan, dapat diketahui version dari *port* yang terbuka (*open*), contohnya pada *port* 80/tcp, statusnya *open*, service yang dipakai adalah http, dan versionnya adalah Cloudflare http proxy. Selain itu, pada *network distance* muncul *output* 12 hops, artinya ada 12 gerbang untuk menuju ke internet.

b. Menggunakan Perintah Nmap –O

Pada website “A” yang telah dilakukan, dapat diketahui bahwa prediksi dari operation system yang digunakan website tersebut diantaranya OneAccess 1641 router (86%), AVtech Room Alert 26w environmental monitor (85%)

Pada website “B” yang telah kami lakukan, dapat diketahui bahwa prediksi dari operation system pada website ini tidak terdeteksi, hanya terdapat *port* yang terbuka saja.

Pada website “C” yang telah kami lakukan, dapat diketahui bahwa prediksi dari operation system pada website ini tidak diketahui, hanya terdapat *port* yang terbuka saja.

c. Menggunakan Perintah Nmap –sV

Pada website “A” yang telah kami lakukan, dapat diketahui semua *ports* (1000 *ports*) pada website ini adalah filtered yang artinya *port* tersebut tidak bisa ditentukan statusnya apakah *open* atau *close*, bisa juga menunjukkan bahwa *port* tersebut dilindungi atau ditolak oleh *firewall*.

Pada website “B” yang telah kami lakukan, dapat diketahui *service* dan *version* dari *port* yang terbuka (*open*). Di sini ada satu *port* yang terbuka yaitu *port* 8443/tcp, statusnya

open, service yang dipakai adalah https-alt, namun versionnya tidak diketahui. Selain itu, 999 *ports* lainnya pada website ini adalah filtered yang artinya *port* tersebut tidak bisa ditentukan statusnya apakah *open* atau *close*, bisa juga menunjukkan bahwa *port* tersebut dilindungi atau ditolak oleh *firewall*.

Pada website “C” yang telah kami lakukan, dapat diketahui service dan version dari *port* yang terbuka (*open*). Di sini ada 4 *port* yang terbuka yaitu 80/tcp dengan service http dan version Cloudflare http proxy, 443/tcp dengan service https dan version Cloudflare http proxy, 8080/tcp dengan service http-proxy dan version Cloudflare http proxy, 8443/tcp dengan service http-alt. dan version Cloudflare http proxy. Selain itu, 996 *ports* lainnya pada website ini adalah filtered yang artinya *port* tersebut tidak bisa ditentukan statusnya apakah *open* atau *close*, bisa juga menunjukkan bahwa *port* tersebut dilindungi atau ditolak oleh *firewall*.

d. Menggunakan Perintah Nmap -sX

Pada website “A” yang telah kami lakukan, dapat diketahui teknik ini mengirimkan paket FIN, URG dan PUSH ke *port* sasaran. Dan semua *port* (1000 *ports*) pada web “A” adalah *open|filtered* yang artinya *port* tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

Pada “B” yang telah kami lakukan, dapat diketahui bahwa semua *port* (1000 *ports*) pada web “B” adalah *open|filtered* yang artinya *port* tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

Pada website “C” yang telah kami lakukan, dapat diketahui bahwa semua *port* (1000 *ports*) pada web “C” adalah *open|filtered* yang artinya *port* tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

4.2 Port Scanning Menggunakan Nmap

a. Menngunakan Perintah Nmap -sS

```
(root㉿kali)-[~/Documents]
└─# nmap -sS www.[REDACTED].com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 16:45
Failed to resolve "www.[REDACTED].com".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.12s
```

Gambar 4. Nmap -sS web “A”

Dari proses *port scanning* Nmap -sS pada website “A” yang telah kami lakukan, dapat diketahui bahwa website ini tidak mengizinkan kita untuk mengambil informasi lebih dalam, sehingga tertera “failed to resolve” artinya kita gagal dalam men-scan website ini.

```
(root㉿kali)-[~/Documents]
└─# nmap -sS www.[REDACTED].com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 16:45
Failed to resolve "www.[REDACTED].com".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.12s
```

Gambar 5. Nmap -sS web “B”

Dari proses *port scanning* Nmap -sS pada website “B” yang telah kami lakukan, dapat diketahui bahwa website ini tidak mengizinkan kita untuk mengambil informasi lebih dalam, sehingga terdapat “failed to resolve” artinya kita gagal dalam men-scan website ini.

```
(root㉿kali)-[~/home/erinaud]
$ nmap -sS www.████████.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-13 16:13:39
Nmap scan report for www.████████.com (████████.com)
Host is up (0.10s latency).
Other addresses for www.████████.com (████████.com):
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
```

Gambar 6. Nmap -sS web “C”

Dari proses *port scanning* Nmap -sS pada website “C” yang telah kami lakukan, dapat diketahui bahwa terdapat 4 port yang aktif yaitu pada 80/tcp dengan service http, 443/tcp dengan service https, 8080/tcp dengan service http-proxy, 8443/tcp dengan service http-alt.

b. Menggunakan Perintah Nmap –sF

Pada website “A” yang telah kami lakukan, dapat diketahui bahwa semua port (1000 ports) pada web “A” adalah open|filtered yang artinya port tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

Pada website “B” yang telah kami lakukan, dapat diketahui bahwa perintah ini mengirim satu paket FIN ke website target, tapi hasilnya adalah nihil. Dapat diketahui, semua port (1000 ports) pada web “B” adalah open|filtered yang artinya port tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

Pada website “C” yang telah kami lakukan, dapat diketahui bahwa perintah ini mengirim satu paket FIN ke website target, tapi hasilnya adalah nihil. Dapat diketahui, semua port (1000 ports) pada web “C” adalah open|filtered yang artinya port tersebut mungkin dilindungi *firewall* atau mungkin terbuka sehingga statusnya tidak dapat ditentukan.

4.3 Pengujian Menggunakan Nikto di Kali Linux

```
(erinaud@kali)-[~]
$ sudo su
[sudo] password for erinaud:
(root㉿kali)-[~/home/erinaud]
# nikto -h www.████████.com
- Nikto v2.1.6

+ Target IP:          54.192.████.████
+ Target Hostname:    www.████████.com
+ Target Port:         80
+ Message:             Multiple IP addresses found:
+ Start Time:        2021-07-13 16:13:39 (GMT-4)
```

Gambar 7. Nikto-h web “A”

```
(erinaudy㉿kali)-[~]
$ sudo su
[sudo] password for erinaudy:
(eroot㉿kali)-[/home/erinaudy]
# nikto -h www.104.21.129.129.com
- Nikto v2.1.6

+ Target IP:          104.21.129.129
+ Target Hostname:    www.104.21.129.129.com
+ Target Port:         80
+ Message:            Multiple IP addresses found!
+ Start Time:         2021-07-13 16:14:38 (GMT-4)
```

Gambar 8. Nikto-h web “B”

```
(root㉿kali)-[/home/erinaudy]
# nikto -h www.172.67.1.11.com
- Nikto v2.1.6

+ Target IP:          172.67.1.11
+ Target Hostname:    www.172.67.1.11.com
+ Target Port:         80
+ Message:            Multiple IP addresses found!
+ Start Time:         2021-07-13 16:11:11 (GMT-4)
```

Gambar 9. Nikto-h web “C”

Dari pengujian *vulnerability assessment* menggunakan nikto pada 3 website tersebut, hanya dapat diketahui IP target, hostname target, port target, lalu jenis server yang digunakan website tersebut.

4.3 Hasil Analisis

Dari pengujian *network* dan *port scanning* pada tool nmap yang telah peneliti lakukan, dapat disimpulkan bahwa website yang memiliki keamanan paling tinggi adalah website “A” karena dari beberapa perintah *scanning*, website tersebut hanya merespon satu perintah saja yaitu nmap -A. Sedangkan website yang memiliki keamanan yang paling rendah adalah website “C” karena website ini selalu merespon perintah-perintah *scanning* yang peneliti lakukan.

5. Kesimpulan

Dari pengujian tingkat keamanan wesbsite yang telah dilakukan, peneliti menyimpulkan bahwa website yang memiliki tingkat keamanan paling tinggi adalah website “A” karena dari beberapa perintah *scanning*, website tersebut hanya merespon satu perintah saja yaitu nmap -A. Sedangkan website yang memiliki tingkat keamanan yang paling rendah adalah website “C” karena website ini selalu merespon perintah-perintah *scanning* yang kami lakukan. Selain itu, dilihat dari metode *information gathering* menggunakan tool *whois*, website “A” hanya menampilkan informasi yang umum dan tidak detail termasuk tidak memberi tahu nama admin, lokasi server, dan lain-lain.

Dari pengujian yang dilakukan maka dapat disimpulkan bahwa tool nmap mampu melakukan *vulnerability assessment* dengan baik karena lebih lengkap dalam memberikan informasi disbanding nikto.

Referensi

- Abdullah. 2016. Kung-fu *Hacking* dengan Nmap. Yogyakarta: ANDI
- Aboelfotoh. S. F, & N. A. Hikal. A. 2020. Review of Cyber-Security Measuring and Assessment Methods for Modern Enterprise. International Journal on Informatics Visualization. vol.3.no.2. 2019. E-ISSN: 2549-9904. ISSN: 2549-9610
- Alwi, E. I., Herdianti, H., & Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. INFORMAL: Informatics Journal, 5(2), 43. <https://doi.org/10.19184/isj.v5i2.18941>
- Bekti, H.B. 2015. Mahir Membuat Website dengan Adobe Dreamweaver CS6, CS5 dan Jquery. Yogyakarta: C.V Andi Offset
- EC-Council. 2012. Certified Ethical Hacker v8: Module 02 Footprinting and Reconnaissance. Amerika: EC-Council
- Palmer, C. C. (2001). Ethical hacking. IBM Systems Journal, 40(3), 769–780. <https://doi.org/10.1147/sj.403.0769>
- Rohinet, Abdul Rahman, 2019. Pengertian Network Scanning. <https://abdurrahmanrohitnet.blogspot.com/2019/10/pengertian-network-scanning-network.html>.
- Shidiqpu, 2009. Port Scanning. <http://shidiqpu.blogspot.com/2009/01/port-scanning.html>.