LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

PERTEMUAN 12

WEB DYNAMIC PENTEST

DISUSUN OLEH

Nama	: Fariansyah Permata Surya
NIM	: 21/473155/SV/18810
Hari, Tanggal	: Senin, 05/06/2023
Kelas	: RI4AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. Dasar Teori

Nessus adalah sebuah perangkat lunak keamanan jaringan yang digunakan untuk melakukan pemindaian kelemahan dan audit keamanan pada sistem komputer. Nessus awalnya dikembangkan oleh Renaud Deraison pada tahun 1998 dan saat ini diproduksi oleh perusahaan Tenable Network Security.

Nessus berfungsi dengan melakukan pemindaian pada jaringan atau host yang ditentukan untuk mencari kerentanan yang mungkin dieksploitasi oleh penyerang. Perangkat lunak ini menggunakan berbagai teknik pemindaian yang meliputi pemindaian port, pemindaian protokol, pemindaian kerentanan, dan pemindaian keamanan lainnya. Hasil pemindaian ini kemudian dianalisis untuk mengidentifikasi potensi kerentanan dan memberikan laporan yang detail kepada pengguna.

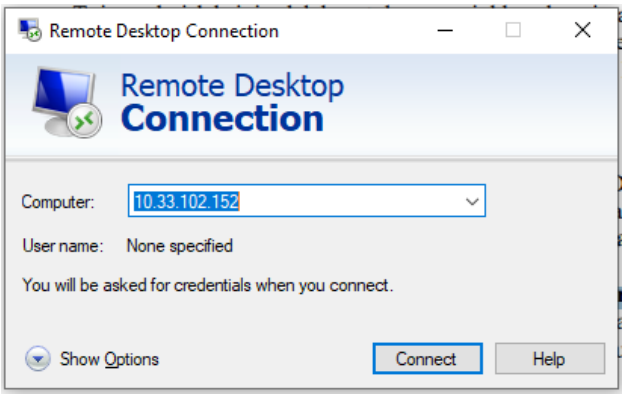
Nessus juga menyediakan database yang terus diperbarui dengan informasi mengenai kerentanan yang ditemukan dalam perangkat lunak dan sistem operasi yang berbeda. Hal ini memungkinkan pengguna untuk melacak dan memperbaiki kerentanan yang ada dalam sistem mereka.

B. Alat dan Bahan

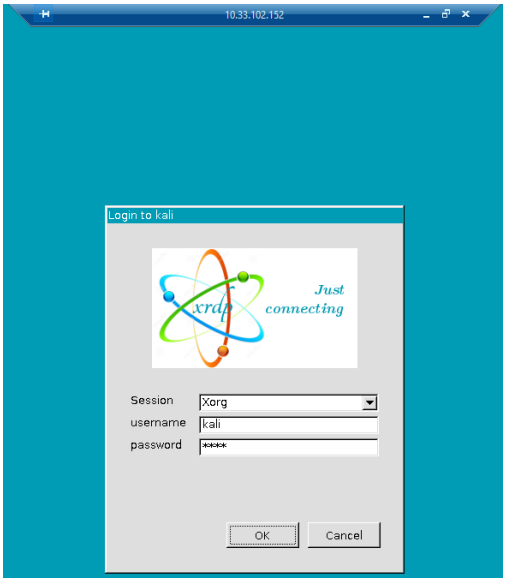
1. PC Host
2. Koneksi Internet
3. Kali Linux

C. Tugas dan Penyelesaian

1. Jalankan mesin Kali Linux dengan Remote Dekstop Connection di PC windows. Masukkan masing-masing IP yang sudah di sediakan.



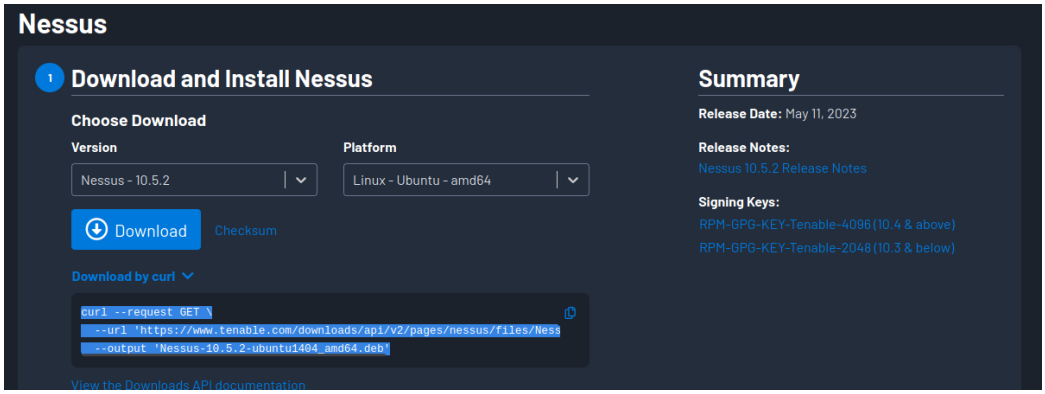
2. Masukkan password kali pilih username kali.



3. Kemudian lakukan penginstalan nessus. Pertama jalankan perintah “sudo apt update && sudo apt install curl” pada terminal.

```
┌──(root💀kali)-[/home/kali]
└─# sudo apt update && sudo apt install curl
Hit:1 https://mirror.primelink.net.id/kali kali-rolling InRelease
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
1805 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following package was automatically installed and is no longer required:
  php7.4-mysql
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libcurl4 libgmp-dev libgmp10 libgmpxx4ldbl libgnutls30 libldap-2.5-0 libldap-common libnettle8 libsasl2-2 libsasl2-modules-db
Suggested packages:
  gmp-doc libgmp10-doc libmpfr-dev gnutls-bin
Recommended packages:
  libsasl2-modules
The following NEW packages will be installed:
  libldap-2.5-0 libldap-common
The following packages will be upgraded:
  curl libcurl4 libgmp-dev libgmp10 libgmpxx4ldbl libgnutls30 libnettle8 libsasl2-2 libsasl2-modules-db
9 upgraded, 2 newly installed, 0 to remove and 1796 not upgraded.
Need to get 4,225 kB of archives.
After this operation, 1,030 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libgmp-dev amd64 2:6.2.1+dfsg1-1.1 [641 kB]
Get:2 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libgmpxx4ldbl amd64 2:6.2.1+dfsg1-1.1 [338 kB]
Get:3 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libgmp10 amd64 2:6.2.1+dfsg1-1.1 [563 kB]
Get:4 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libnettle8 amd64 3.8.1-2 [288 kB]
Get:5 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libgnutls30 amd64 3.7.9-2 [1,403 kB]
Get:6 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libsasl2-modules-db amd64 2.1.28+dfsg-10 [20.3 kB]
Get:7 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libsasl2-2 amd64 2.1.28+dfsg-10 [59.7 kB]
Get:8 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libldap-2.5-0 amd64 2.5.13+dfsg-5 [183 kB]
Get:9 https://mirror.primelink.net.id/kali kali-rolling/main amd64 curl amd64 7.88.1-9 [314 kB]
Get:10 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libcurl4 amd64 7.88.1-9 [386 kB]
Get:11 https://mirror.primelink.net.id/kali kali-rolling/main amd64 libldap-common all 2.5.13+dfsg-5 [29.3 kB]
Fetched 4,225 kB in 43s (97.8 kB/s)
(Reading database ... 273083 files and directories currently installed.)
Preparing to unpack .../libgmp-dev_2%3a6.2.1+dfsg1-1.1_amd64.deb ...
Unpacking libgmp-dev:amd64 (2:6.2.1+dfsg1-1.1) over (2:6.2.1+dfsg-1) ...
Preparing to unpack .../libgmpxx4ldbl_2%3a6.2.1+dfsg1-1.1_amd64.deb ...
Unpacking libgmpxx4ldbl:amd64 (2:6.2.1+dfsg1-1.1) over (2:6.2.1+dfsg-1) ...
Preparing to unpack .../libgmp10_2%3a6.2.1+dfsg1-1.1_amd64.deb ...
Unpacking libgmp10:amd64 (2:6.2.1+dfsg1-1.1) over (2:6.2.1+dfsg-1) ...
Setting up libgmp10:amd64 (2:6.2.1+dfsg1-1.1) ...
(Reading database ... 273083 files and directories currently installed.)
```

4. Buka browser dan gunakan kata kunci download nessus. Ubah beberapa hal seperti gambar dibawah dan kemudian copy command seperti gambar dibawah.



5. Paste command sebelumnya pada terminal.

```
┌──(root💀kali)-[/home/kali]
└─# curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.5.2-ubuntu1404_amd64.deb' \
  --output 'Nessus-10.5.2-ubuntu1404_amd64.deb'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 62.2M    0 62.2M    0     0  5737k      0 --:--:--  0:00:11 --:--:-- 7335k
```

6. Cek file Nessus dan Install Nessus.

```
┌──(root💀kali)-[/home/kali]
└─# file Nessus-10.5.2-ubuntu1404_amd64.deb
Nessus-10.5.2-ubuntu1404_amd64.deb: Debian binary package (format 2.0), with control.tar.gz, data compression gz

┌──(root💀kali)-[/home/kali]
└─# sudo apt install -f ./Nessus-10.5.2-ubuntu1404_amd64.deb
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'nessus' instead of './Nessus-10.5.2-ubuntu1404_amd64.deb'
The following package was automatically installed and is no longer required:
  php7.4-mysql
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 1796 not upgraded.
Need to get 0 B/65.2 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/kali/Nessus-10.5.2-ubuntu1404_amd64.deb nessus amd64 10.5.2 [65.2 MB]
Selecting previously unselected package nessus.
(Reading database ... 273098 files and directories currently installed.)
Preparing to unpack .../Nessus-10.5.2-ubuntu1404_amd64.deb ...
Unpacking nessus (10.5.2) ...
Setting up nessus (10.5.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
```

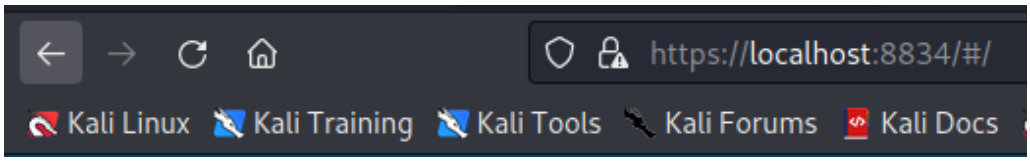
7. Jalankan Nessus.

```
┌──(root💀kali)-[/home/kali]
└─# sudo systemctl enable nessusd
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

┌──(root💀kali)-[/home/kali]
└─# sudo systemctl start nessusd
```

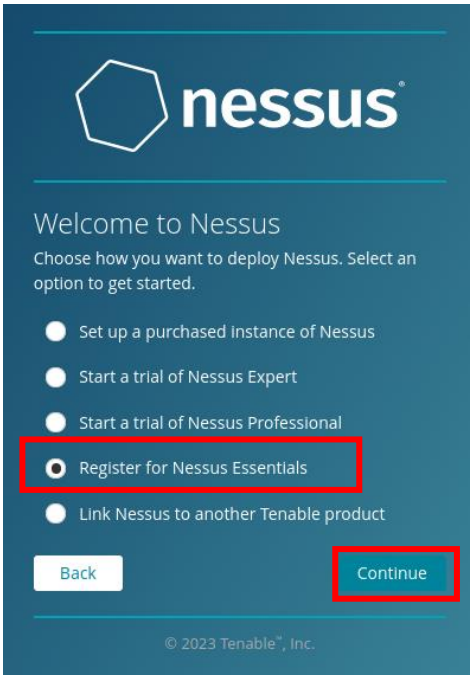
8. Cek status Nessus.

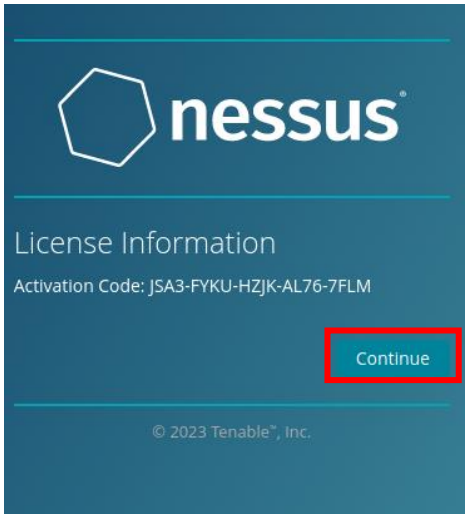
```
┌──(root💀kali)-[/home/kali]
└─# systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: disabled)
     Active: active (running) since Mon 2023-05-29 20:57:24 CDT; 51s ago
   Main PID: 323533 (nessus-service)
      Tasks: 14 (limit: 4635)
     Memory: 136.7M
        CPU: 34.815s
     CGroup: /system.slice/nessusd.service
             ├─323533 /opt/nessus/sbin/nessus-service -q
             └─323534 nessusd -q

May 29 20:57:24 kali systemd[1]: Started The Nessus Vulnerability Scanner.
May 29 20:57:25 kali nessus-service[323534]: Cached 0 plugin libs in 0msec
May 29 20:57:25 kali nessus-service[323534]: Cached 0 plugin libs in 0msec

┌──(root💀kali)-[/home/kali]
└─# sudo  ss -ant | grep 8834
LISTEN    0      1024                 0.0.0.0:8834             0.0.0.0:*
LISTEN    0      1024                    [::]:8834                [::]:*

┌──(root💀kali)-[/home/kali]
└─#
```

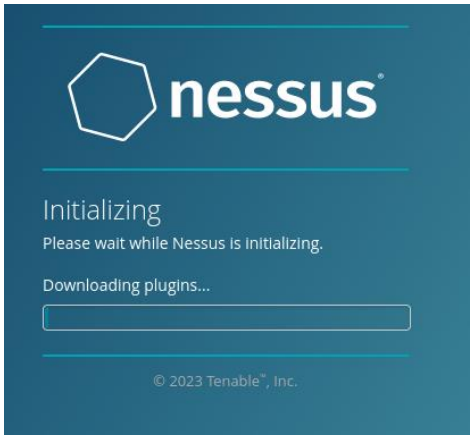
9. Kunjungi antarmuka web Nessus di IP server atau port nama host 8834 untuk menyelesaikan instalasi dan aktivasi Nessus.



10. Kemudian lakukan pendafataran akun Nessus seperti gambar dibawah

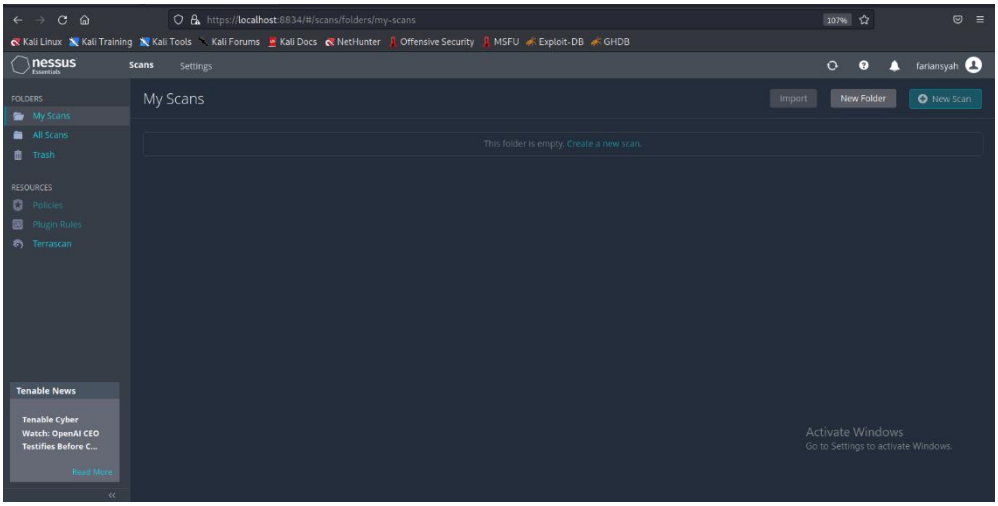




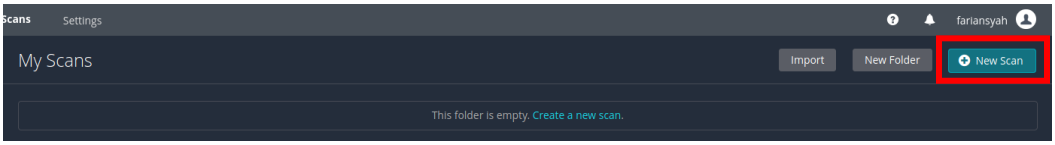


Tunggu hingga selesai

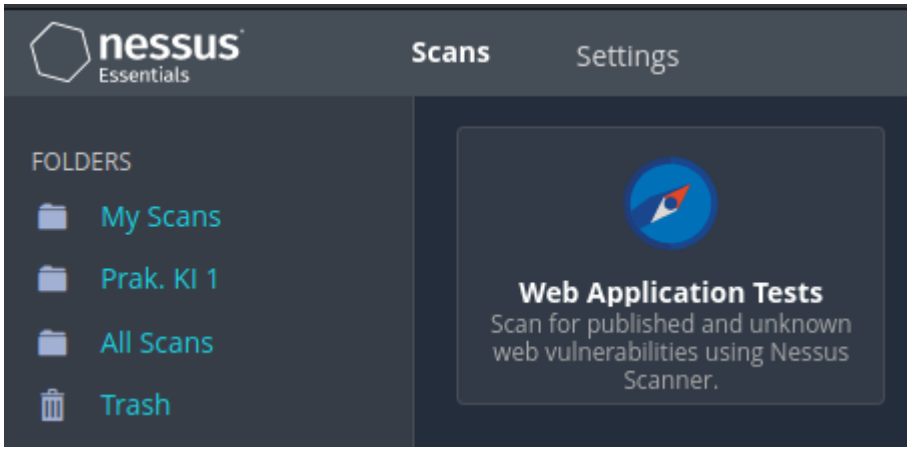
11. Tampilan awal web Nessus dan tunggu compile file selesai.



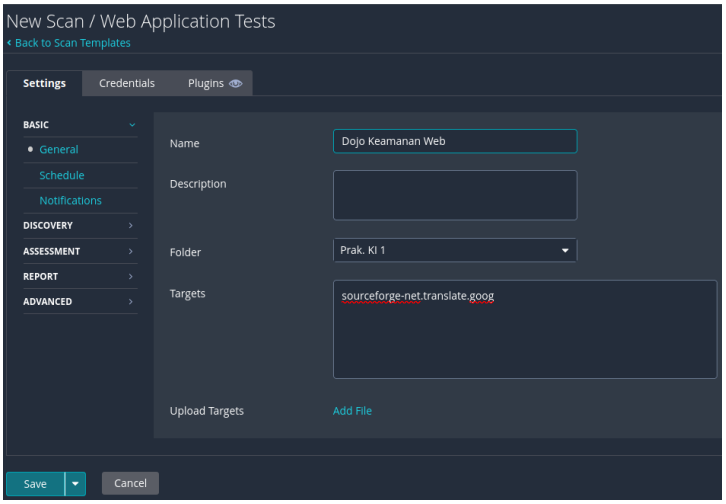
12. Pilih New Scan.



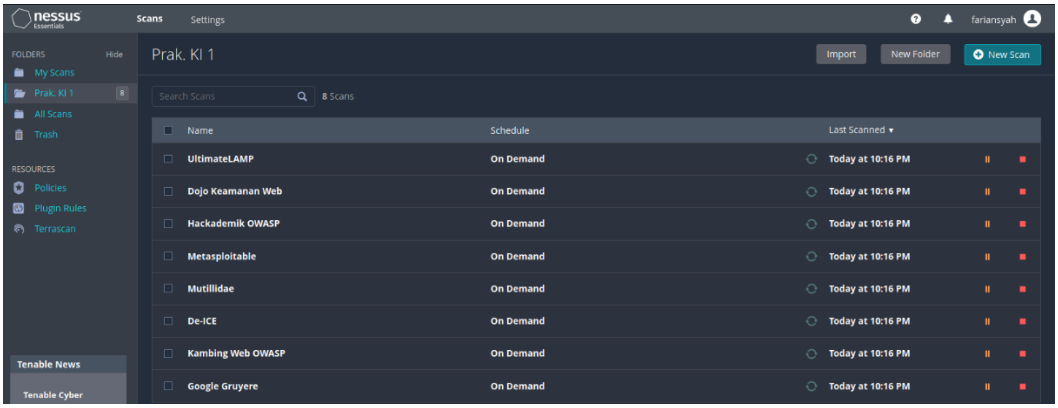
13. Klik Web Application Test.



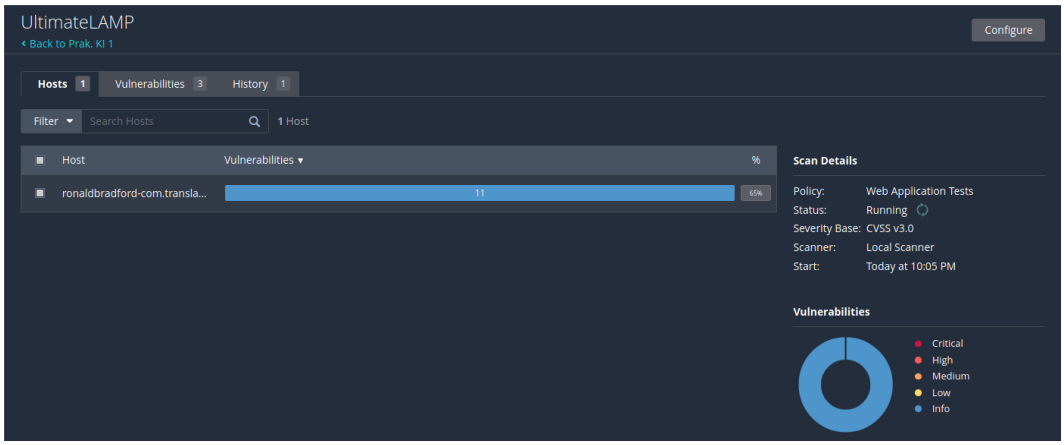
14. Isikan Name bebas dengan saja, kemudian pilih folder untuk menyimpan dan pada Targets isi dengan alamt website yang akan dilakukan ujicoba dan klik save.

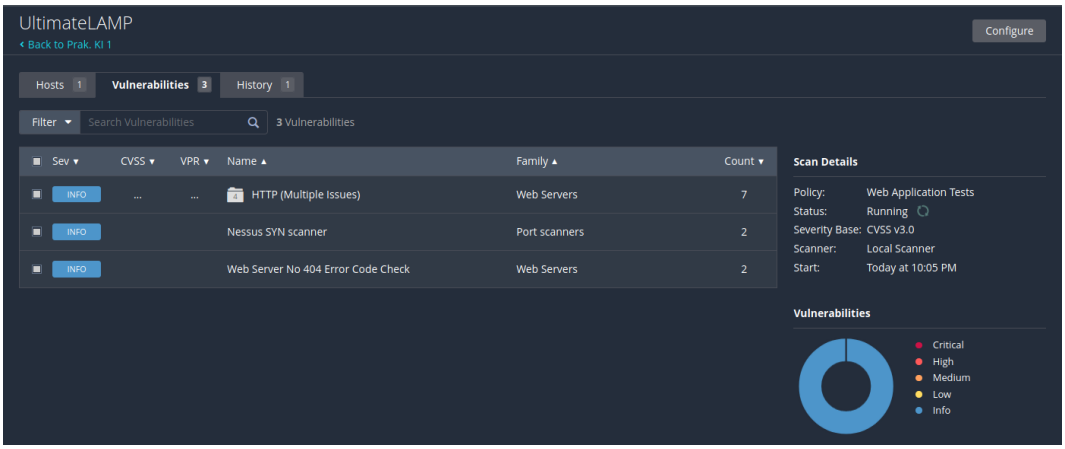


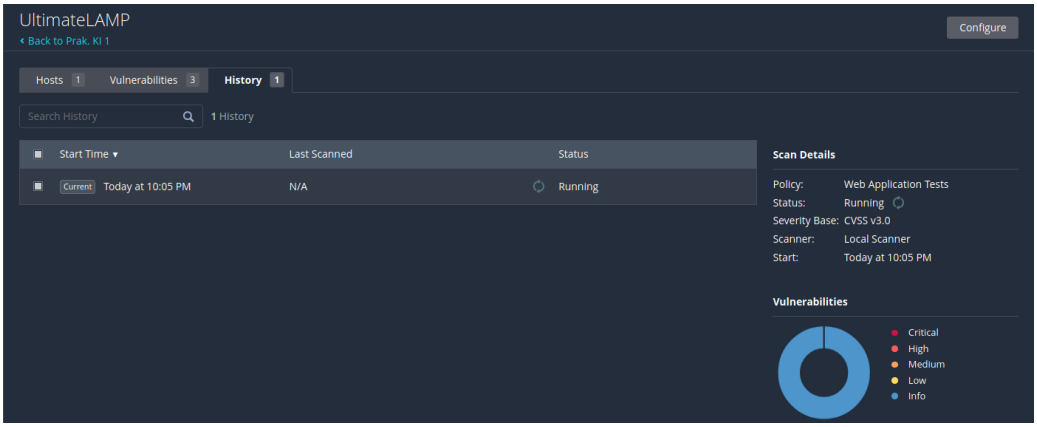
15. Beberapa website yang dijadikan target dan juga tunggu proses running kurang lebih 5 hingga 10 menit hingga pemindaian 100% selesai.



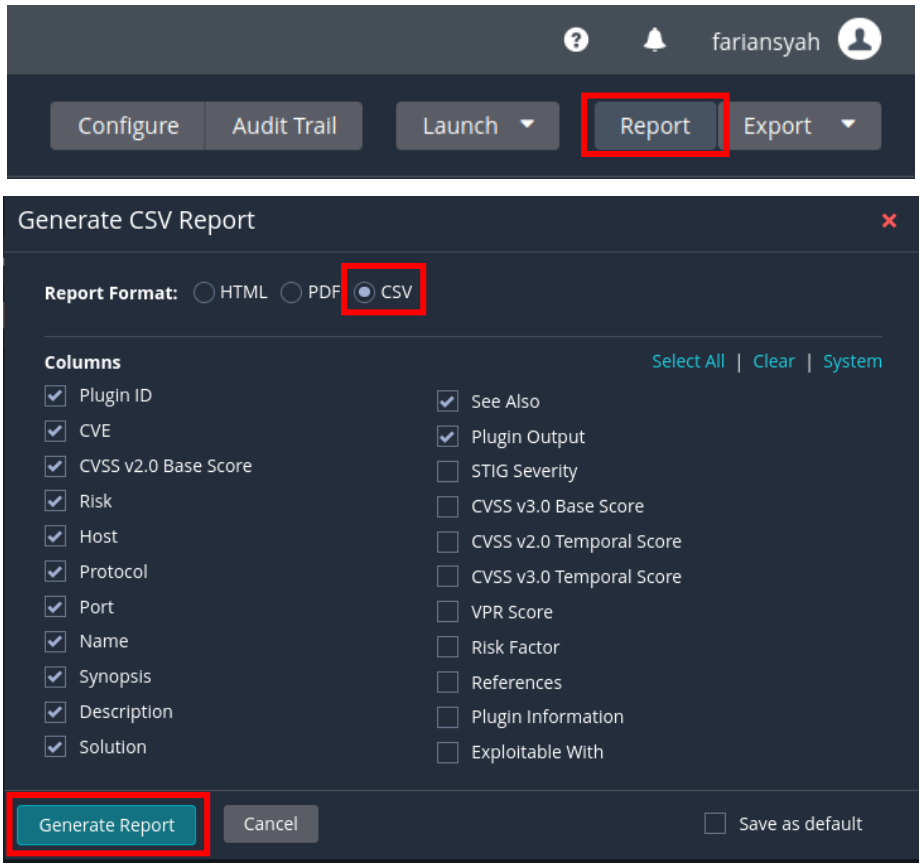
16. Klik salah satu file. File tersebut terdapat 3 menu yaitu host, vulnerabilities dan history.



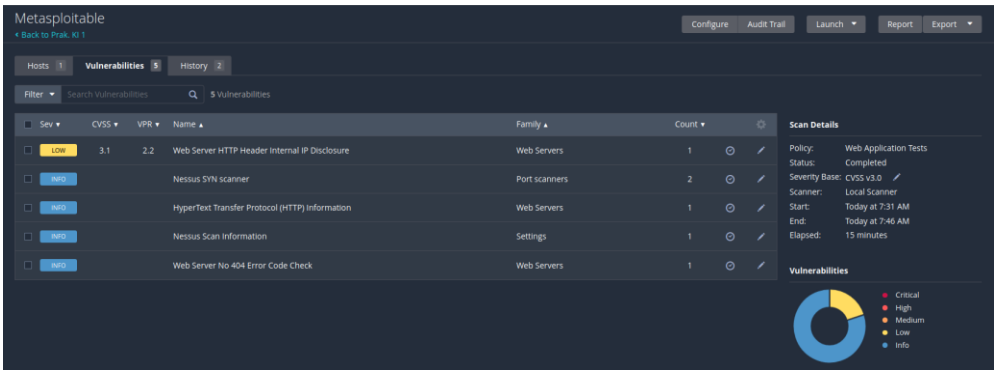




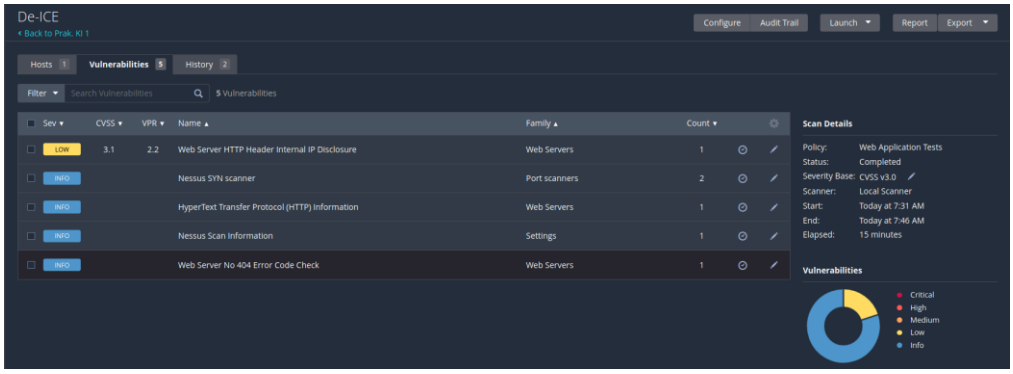
17. Setelah proses selesai lakukan eksport file menjadi .csv.



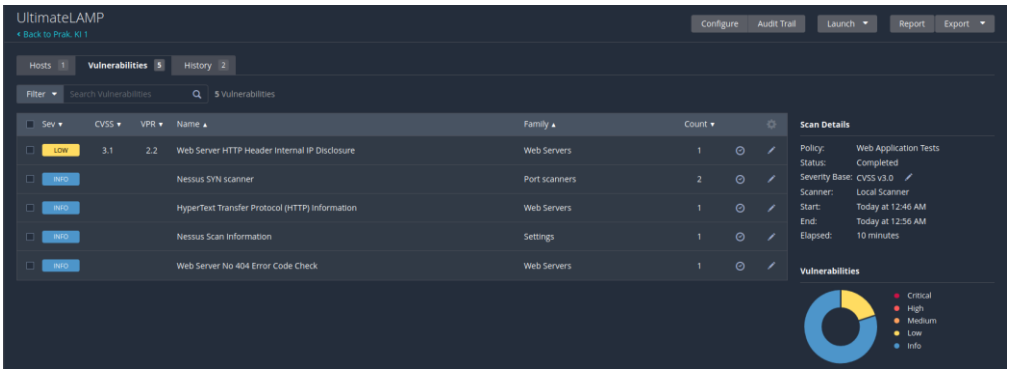
18. Hasil yang didapat pada web Nessus.



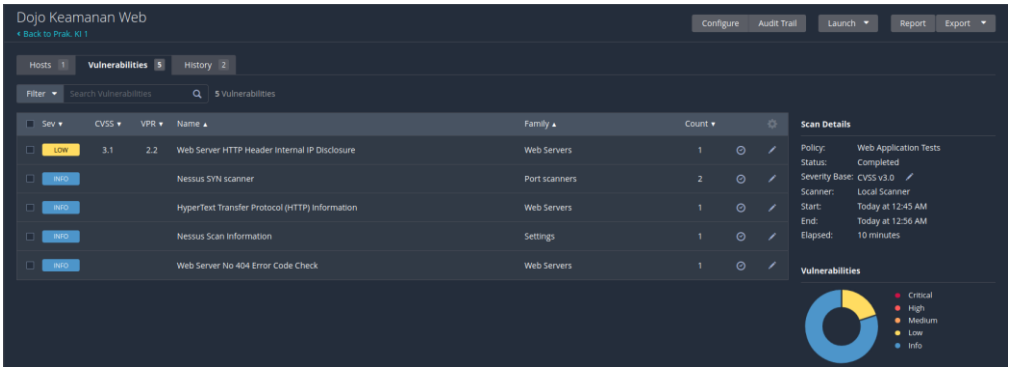
Information.rapid7.com



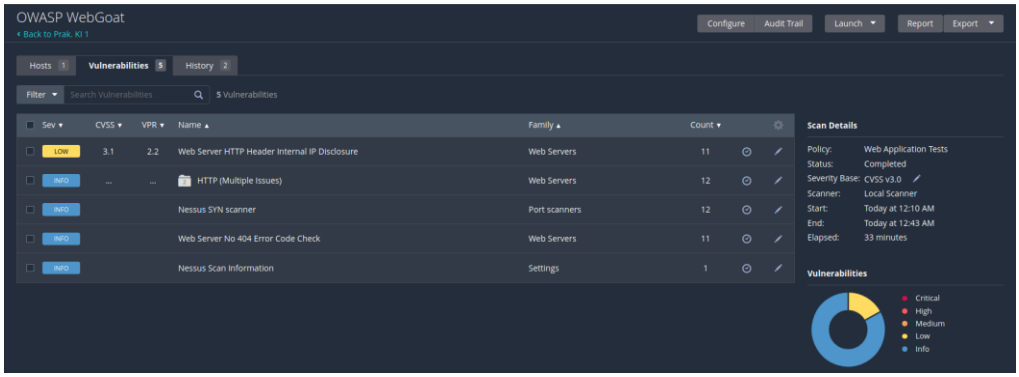
www.vulnhub.com



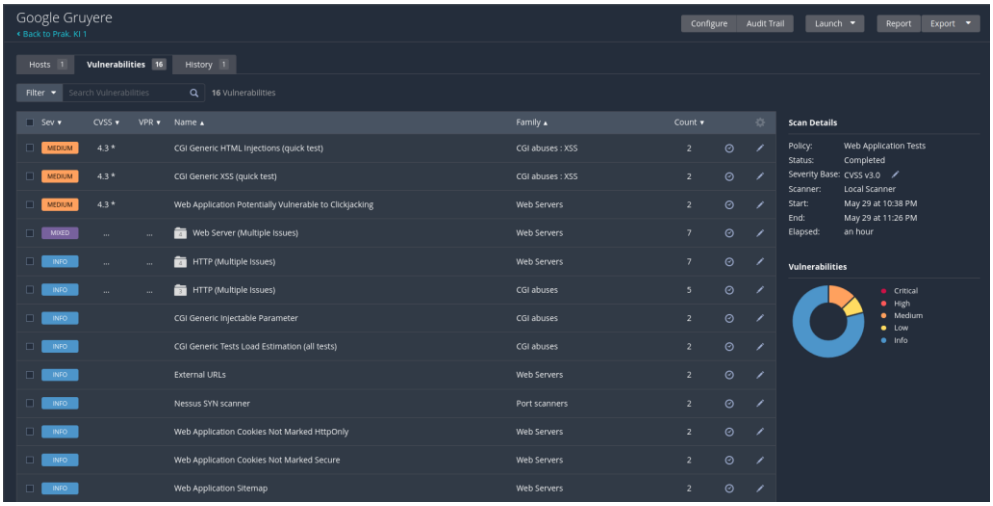
Ronaldbradford.com



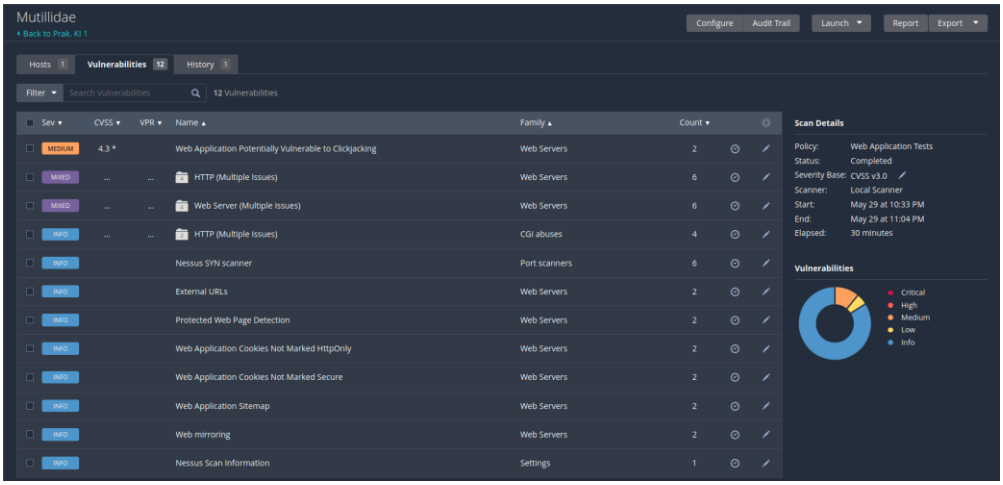
Sourceforge.net



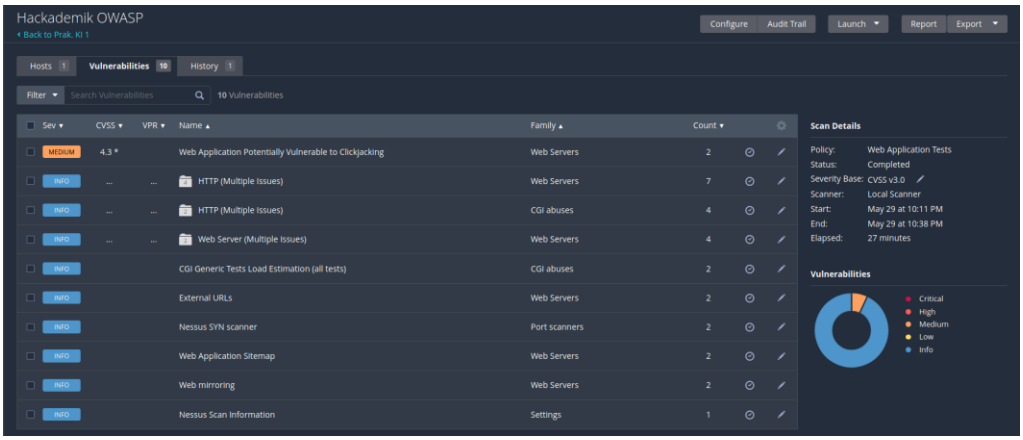
www.project.webgoat



Google.gruyere.appspot.com



www.irongeek.com



Code.google.com

D. Analisis

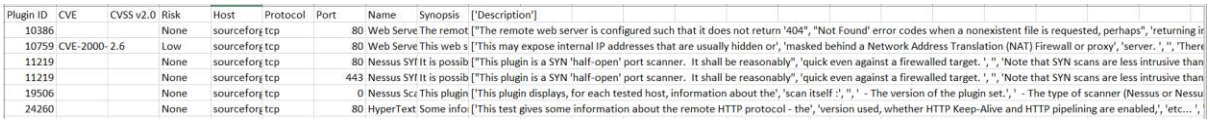
Pada praktikum Pertemuan 11 membahas tentang Web Dynamic Pentest (pengujian penetrasi web dinamis) adalah proses mengidentifikasi dan mengeksploitasi kerentanan keamanan dalam aplikasi web yang memiliki komponen dinamis atau interaktif. Dalam pengujian penetrasi web dinamis, tujuannya adalah untuk menemukan celah keamanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses yang tidak sah, mencuri data sensitif, atau merusak sistem.

Pengujian penetrasi web dinamis melibatkan penggunaan alat dan teknik yang dirancang khusus untuk memeriksa keamanan aplikasi web. Beberapa langkah umum dalam proses pengujian ini meliputi:

1. Pemetaan: Menganalisis aplikasi web untuk mengidentifikasi semua komponen dan fungsionalitasnya, termasuk halaman web, formulir, fitur interaktif, basis data, dan API yang mungkin terlibat.
2. Identifikasi Kerentanan: Mencari kerentanan keamanan seperti injeksi SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), kerentanan file upload, dan kerentanan terkait akses dan otorisasi.
3. Pemindaian Kerentanan: Melakukan pemindaian otomatis menggunakan alat-alat seperti Nessus, Burp Suite, atau OWASP ZAP untuk mengidentifikasi kerentanan yang mungkin ada dalam aplikasi web.
4. Eksploitasi: Setelah kerentanan ditemukan, melakukan serangan aktif untuk menguji apakah kerentanan tersebut dapat dieksploitasi dan memberikan akses yang tidak sah.
5. Pencatatan Hasil: Merekam semua temuan dan eksploitasi dalam laporan yang rinci, termasuk langkah-langkah mitigasi yang disarankan untuk memperbaiki kerentanan yang ditemukan.

Saat melakukan praktikum Web Dynamic Pentest ini menggunakan tool bernama Nessus dimana Nessus adalah sebuah perangkat lunak komputer yang digunakan untuk melakukan pemindaian keamanan jaringan. Perangkat lunak ini dikembangkan oleh perusahaan Tenable, dan telah menjadi salah satu alat penting dalam industri keamanan informasi. Nessus dapat digunakan untuk mengidentifikasi beberapa kerentanan yang mungkin terkait dengan aplikasi web, alat ini tidak secara khusus dirancang untuk melakukan pengujian penetrasi web dinamis.

Langkah awal pada praktikum ini adalah menginstall nesus pada VM Kali Linux setelah itu melakukan pendaftaran akun Nessus pada web Nessus. Setelah selesai melakukan pendaftaran, web Nessus akan melakukan compile file terlebih dahulu sebelum melakukan Web Dynamic Pentest. Setealh itu dilakukan Web Dynamic Pentest pada beberapa web tujuan yang telah ditentukan. Proses memindai sebuah web cukup memakan waktu yang lama, setelah selesai memindai 100% hasil yang didapat akan ditampilkan pada web Nessus dan juga dapat di eksport menjadi file csv. Hasil pada menu Vulnerabilities web Nessus dibagi menjadi beberapa kategori Risk seperti merah berarti Critical, merah muda berarti High, orange berarti Medium, kuning berarti Low, dan biru berarti Info. Sedangkan pada hasil dengan file csv terdapat beberapa kolom label seperti gambar dibawah.



Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	['Description']
10386			None	sourceforg	tcp	80	Web Serve	The remot	["The remote web server is configured such that it does not return '404', "Not Found' error codes when a nonexistent file is requested, perhaps", 'returning ir
10759	CVE-2000-	2.6	Low	sourceforg	tcp	80	Web Serve	This web s	["This may expose internal IP addresses that are usually hidden or', 'masked behind a Network Address Translation (NAT) Firewall or proxy', 'server. ', '', 'There
11219			None	sourceforg	tcp	80	Nessus SYI	It is possib	["This plugin is a SYN 'half-open' port scanner. It shall be reasonably", 'quick even against a firewalled target. ', '', 'Note that SYN scans are less intrusive than
11219			None	sourceforg	tcp	443	Nessus SYI	It is possib	["This plugin is a SYN 'half-open' port scanner. It shall be reasonably", 'quick even against a firewalled target. ', '', 'Note that SYN scans are less intrusive than
19506			None	sourceforg	tcp	0	Nessus Sc	This plugin	['This plugin displays, for each tested host, information about the', 'scan itself :', '', ' - The version of the plugin set.', ' - The type of scanner (Nessus or Nessu
24260			None	sourceforg	tcp	80	HyperText	Some info	['This test gives some information about the remote HTTP protocol - the', 'version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,', 'etc... ',

Label Risk sama seperti pada web Nessus dan pada hasil file csv terdapat host yang terdapat Risk beserta Port, Protocol, Nama dari Protocol, Synopsis serta Description vulnerabilities tersebut. Hasil dari beberapa web yang di pindai, web dengan Risk dengan kategori Medium ada 3 yaitu Mutillidae (www.irongeek.com), Hackademik OWASP (code.google.com) dan Google Gruyere (google.gruyere.appspot.com). Ketiga web tersebut juga terdapat banyak sekali Vulnerabilities yang ter scan walaupun dengan Risk hanya berupa Info dan Low.

E. Kesimpulan

Adapun kesimpulan yang dapat diambil setelah melakukan praktikum kali ini adalah

1. Nessus dapat digunakan oleh administrator jaringan dan profesional keamanan untuk melakukan pemindaian keamanan secara rutin, mengidentifikasi dan memperbaiki kerentanan sebelum mereka dieksploitasi oleh penyerang. Hal ini membantu meningkatkan keamanan sistem dan jaringan, serta melindungi data sensitif dari ancaman keamanan.
2. Web Dynamic Pentest penting untuk mengidentifikasi dan memperbaiki kerentanan keamanan dalam aplikasi web yang kompleks. Dengan melakukan pengujian ini, organisasi dapat memperkuat keamanan sistem mereka, melindungi data sensitif dan menjaga kepercayaan pengguna dalam menggunakan aplikasi web mereka.

3. Dalam pengujian penetrasi web dinamis, alat-alat seperti Burp Suite, OWASP ZAP, atau Acunetix dapat digunakan bersama dengan Nessus untuk melengkapi pengujian dan mencakup aspek aplikasi web yang lebih dinamis dan interaktif.

F. Daftar Pustaka

1. (DOCX) Nessus Adalah Scanner Keamanan Jaringan Yang Harus Digunakan Oleh Administrator System. (n.d.). Dokumen.tips. Retrieved June 5, 2023, from https://dokumen.tips/documents/nessus-adalah-scanner-keamanan-jaringan-yang-harus-digunakan-oleh-administrator.html?page=18