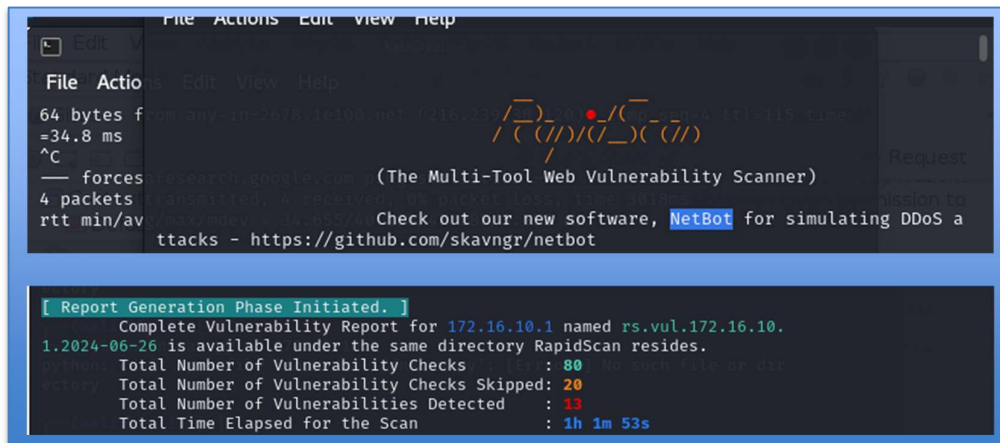


BAB 4

HASIL DAN PEMBAHASAN

4.1. Identifikasi Kerentanan

Teknik pemindaian cepat digunakan dalam penelitian ini untuk menilai tingkat kerentanan pada server web dengan domain server 172.16.10.1. Hasil dari pemindaian cepat adalah sebagai berikut::



```
File Actions Edit View Help
64 bytes f
=34.8 ms
^C
— forces
4 packets
rtt min/av

RapidScan
(The Multi-Tool Web Vulnerability Scanner)
Check out our new software, NetBot for simulating DDoS a
ttacks - https://github.com/skavngr/netbot

[ Report Generation Phase Initiated. ]
Complete Vulnerability Report for 172.16.10.1 named rs.vul.172.16.10.
1.2024-06-26 is available under the same directory RapidScan resides.
Total Number of Vulnerability Checks : 80
Total Number of Vulnerability Checks Skipped: 20
Total Number of Vulnerabilities Detected : 13
Total Time Elapsed for the Scan : 1h 1m 53s
```

Gambar 4. 1 Identifikasi Kerentanan

Dari hasil scanning pada domain server 172.16.10.1 dengan menggunakan tools rapid scan terdapat 80 pemeriksaan kerentanan di mna kerentanan dilewati sebanyak 20 dan kerentanan terdeteksi 13 dapat lihat pada tabel 4.1.1

Tabel 4. 1 Hasil Identifikasi Kerentz

NO	Nama	Jumlah Kerentanan
1	<i>Vulnerability check</i>	80
2	<i>Vulnerability check skipped</i>	20
3	<i>Vulnerability detected</i>	13

4.1.1. Vulnerability Threat Level



Gambar 4. 2 Vulnerability Threat Level

Vulnerability Threat Level pada Kali Linux merujuk pada tingkat keparahan dan potensi bahaya dari sebuah kerentanan (vulnerability) yang ada dalam sistem atau perangkat lunak tertentu. Kali Linux, sebagai distribusi Linux yang terkenal dalam bidang pengujian penetrasi dan keamanan informasi, memiliki pendekatan untuk mengklasifikasikan tingkat keparahan kerentanan berdasarkan pada sejumlah faktor.

Critical (Kritis): Kerentanan ini memiliki potensi yang sangat tinggi untuk dieksploitasi dan dapat menyebabkan kerusakan yang serius pada sistem atau data. Contohnya adalah kerentanan yang memungkinkan penyerang untuk mendapatkan akses penuh ke sistem tanpa otorisasi.

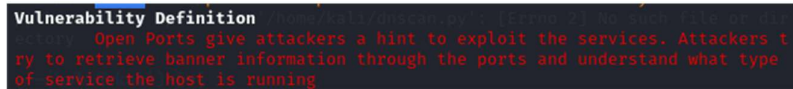
High (Tinggi): Kerentanan ini memiliki potensi tinggi untuk dieksploitasi, meskipun tidak seberat kerentanan kritis. Contohnya adalah kerentanan yang memungkinkan untuk menjalankan kode berbahaya atau memperoleh akses yang lebih tinggi dari yang seharusnya.

Medium (Sedang): Kerentanan ini memiliki potensi yang signifikan untuk dimanfaatkan oleh penyerang, tetapi sering kali memerlukan kondisi tertentu atau serangan yang lebih rumit untuk dieksploitasi.

Low (Rendah): Kerentanan ini memiliki dampak yang relatif kecil atau hanya mempengaruhi fungsi-fungsi yang terbatas. Contohnya mungkin adalah kerentanan yang memungkinkan pengungkapan informasi sensitif, tetapi tidak langsung mengancam integritas sistem secara keseluruhan.

Info (Informasi): Informasi ini biasanya bukan sebuah kerentanan yang bisa dieksploitasi secara langsung, tetapi memberikan informasi penting kepada peneliti keamanan tentang konfigurasi atau keadaan sistem.

4.1.2. Vulnerability definition



Gambar 4. 3 Vulnerability Definition

"vulnerability" (kerentanan) mengacu pada kelemahan atau celah dalam suatu sistem, perangkat lunak, atau jaringan dieksploitasi untuk mendapatkan kesempatan, menyebabkan kerusakan, dapat mengganggu operasi normal dari sistem tersebut. Secara lebih teknis, vulnerability dapat diartikan sebagai kondisi di mana ada celah atau kelemahan dalam desain, implementasi, operasi, atau pengaturan sistem yang memungkinkan penyerang untuk mengeksploitasi sistem tersebut.

Dalam konteks Kali Linux, distribusi ini dikenal sebagai alat utama untuk pengujian penetrasi (penetration testing) dan pengujian keamanan. Oleh karena itu, pengertian vulnerability dalam konteks Kali Linux:

Identifikasi Kerentanan: Proses mencari, mengidentifikasi, dan mengevaluasi kerentanan dalam sistem atau perangkat lunak yang sedang diuji. Alat-alat di Kali Linux seperti scanner kerentanan (vulnerability scanners) membantu dalam menemukan celah-celah keamanan yang ada.

Eksplorasi: Setelah kerentanan teridentifikasi, peneliti keamanan atau praktisi pengujian penetrasi dapat menggunakan Kali Linux untuk mencoba mengeksploitasi kerentanan tersebut. Ini membantu untuk memahami potensi serangan yang dapat dilakukan oleh penyerang dan mengambil tindakan pencegahan yang sesuai.

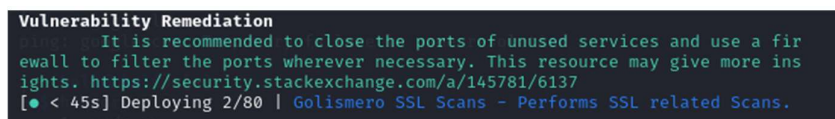
Pemetaan Risiko: Setelah identifikasi dan eksploitasi, Kali Linux dapat digunakan untuk memetakan risiko dari kerentanan yang ditemukan. Ini termasuk menilai potensi dampak, keparahan, dan kemungkinan eksploitasi oleh penyerang.

Pengujian Keamanan: Kali Linux digunakan secara luas untuk melakukan pengujian keamanan secara menyeluruh terhadap sistem dan perangkat lunak guna memastikan bahwa

mereka memiliki lapisan keamanan yang memadai dan mampu menanggulangi potensi serangan.

Dengan demikian, vulnerability definition pada Kali Linux tidak hanya mencakup identifikasi kelemahan, tetapi juga proses eksploitasi dan pengujian keamanan yang komprehensif. Hal ini penting untuk membantu meningkatkan keamanan sistem, mencegah insiden keamanan, dan menjaga integritas data.

4.1.3. Vulnerability Remediation



Gambar 4. 4 Vulnerability Remediation

Vulnerability remediation pada Kali Linux mengacu pada proses memperbaiki atau mengurangi risiko yang disebabkan oleh kerentanan yang ditemukan dalam sistem atau perangkat lunak. Ini adalah langkah-langkah yang diambil setelah kerentanan diidentifikasi melalui pengujian penetrasi atau penilaian keamanan menggunakan Kali Linux atau alat-alat lainnya. Berikut adalah beberapa tahapan utama dalam vulnerability remediation:

Pemahaman Kerentanan: Langkah pertama adalah memahami dengan jelas tentang kerentanan apa yang telah ditemukan. Ini meliputi pemahaman mendalam tentang bagaimana kerentanan dapat dieksploitasi, potensi dampaknya terhadap sistem atau data, dan kondisi yang diperlukan untuk mengeksploitasi kerentanan tersebut.

Penilaian Risiko: Setelah pemahaman awal tentang kerentanan, langkah berikutnya adalah menilai risiko yang terkait. Ini melibatkan penilaian tentang seberapa serius kerentanan tersebut dapat dieksploitasi, potensi dampaknya terhadap operasi bisnis atau layanan yang disediakan oleh sistem, dan seberapa mudah atau sulit untuk mengeksploitasi kerentanan tersebut.

Verifikasi: Setelah perbaikan atau mitigasi diterapkan, penting untuk memverifikasi efektivitasnya. Ini melibatkan pengujian ulang menggunakan alat-alat Kali Linux atau skenario

simulasi serangan untuk memastikan bahwa kerentanan telah ditangani dengan efektif dan tidak ada celah keamanan yang tersisa.

Monitoring dan Pemeliharaan: Kerentanan dan ancaman keamanan untuk melakukan pemantauan terus-menerus terhadap sistem dari perangkat lunak, serta menjaga keamanan dengan memperbarui patch dan konfigurasi keamanan secara berkala.

4.1.4. Port Manual

```
Vulnerability Threat Level
Low Some ports are open. Perform a full-scan manually.
Vulnerability Definition
Open Ports give attackers a hint to exploit the services. Attackers t
ry to retrieve banner information through the ports and understand what type
of service the host is running
Vulnerability Remediation
It is recommended to close the ports of unused services and use a fir
ewall to filter the ports wherever necessary. This resource may give more ins
ights. https://security.stackexchange.com/a/145781/6137
[● < 45s] Deploying 2/80 | Golismero SSL Scans - Performs SSL related Scans.

Scanning Tool Unavailable. Skipping Test ...

[● > 75m] Deploying 3/80 | Nmap - Performs a Full UDP Port Scan

Scan Interrupted in 20m 31s
Test Skipped. Performing Next. Press Ctrl+Z to Quit RapidScan.

[● < 45s] Deploying 4/80 | Golismero - BruteForces for certain files on the D
omain.

Scanning Tool Unavailable. Skipping Test ...

[● < 4m] Deploying 5/80 | Golismero Nikto Scans - Uses Nikto Plugin to detec
t vulnerabilities.

Scanning Tool Unavailable. Skipping Test ...

[● < 35s] Deploying 6/80 | Nikto - Performs SSL Checks.
```

Gambar 4. 5 Port Manual

Membuka port secara manual pada proses masuk ke suatu port tertentu pada sebuah perangkat atau server. Ini penting untuk aplikasi atau layanan tertentu yang perlu diakses.

Identifikasi Port yang dibuka: port 10 untuk HTTP, port 172 untuk HTTPS, atau port tertentu dibutuhkan oleh aplikasi atau layanan khusus.

Akses Konfigurasi Firewall: Jika menggunakan firewall di Linux atau Windows Firewall di Windows, akses konfigurasi firewall. Ini biasanya dapat dilakukan melalui terminal atau command promp.

Menyimpan dan Mengaktifkan Perubahan: Setelah aturan firewall ditambahkan, pastikan untuk menyimpan konfigurasi (tergantung pada sistem operasi dan alat manajemen firewall yang Anda gunakan).

Verifikasi Koneksi: Setelah port dibuka, koneksi dari luar jaringan untuk memastikan bahwa port telah terbuka dan dapat diakses.

Pemantauan dan Keamanan: Setelah membuka port, penting untuk memantau yang masuk ke port tersebut dan memastikan bahwa hanya yang diizinkan yang diterima. Pastikan juga untuk mempertimbangkan keamanan dengan menggunakan enkripsi jika diperlukan, atau mengatur akses berdasarkan alamat IP.

4.1.5. Subdomain

```
Vulnerability Threat Level
  medium Subdomains discovered with DMitry.
Vulnerability Definition
  Attackers may gather more information from subdomains relating to the
  parent domain. Attackers may even find other services from the subdomains and
  try to learn the architecture of the target. There are even chances for the
  attacker to find vulnerabilities as the attack surface gets larger with more
  subdomains discovered.
Vulnerability Remediation
  It is sometimes wise to block sub domains like development, staging t
  o the outside world, as it gives more information to the attacker about the t
  ech stack. Complex naming practices also help in reducing the attack surface
  as attackers find hard to perform subdomain bruteforcing through dictionaries
  and wordlists.
[● < 30s] Deploying 27/80 | Golismero Zone Transfer - Attempts Zone Transfer.
Scanning Tool Unavailable. Skipping Test ...
[● < 2m] Deploying 28/80 | Uniscan - Brutes for Filenames on the Domain.
Scanning Tool Unavailable. Skipping Test ...
[● < 30s] Deploying 29/80 | WebDAV - Checks if WEBDAV enabled on Home directo
ry.
Scan Completed in 1s
[● < 35s] Deploying 30/80 | Nmap [OpenSSL CCS Injection] - Checks only for CC
S Injection.
```

Gambar 4. 6 Subdomain

Subdomain pada dasarnya adalah bagian dari domain yang berada di bawah domain utama. Dalam konteks Kali Linux, subdomain dapat berarti beberapa hal tergantung pada konteksnya:

Eksploitasi dan Pemantauan: Setelah subdomain ditemukan, peneliti keamanan dapat menggunakan informasi ini untuk mengidentifikasi dan mengeksploitasi potensi celah keamanan. Misalnya, subdomain yang tidak terlindungi dengan baik atau tidak diperbarui dapat menjadi titik masuk untuk serangan.

Pengujian Web dan Aplikasi: Subdomain juga sering kali digunakan untuk mengarahkan ke aplikasi atau layanan khusus dalam pengujian web. Dalam pengujian penetrasi web, Kali Linux dapat digunakan untuk melakukan serangan terhadap subdomain yang mungkin memiliki kelemahan keamanan.

4.1.6. HTTP(Hypertext Transfer Protocol)

```
Vulnerability Threat Level
low Some issues found with HTTP Options.
Vulnerability Definition
There are chances for an attacker to manipulate files on the webservice.
Vulnerability Remediation
It is recommended to disable the HTTP PUT and DEL methods incase if you don't use any REST API Services. Following resources helps you how to disable these methods. http://www.techstacks.com/howto/disable-http-methods-in-to-mcat.html https://docs.oracle.com/cd/E19857-01/820-5627/gghwc/index.html https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/
[• < 45s] Deploying 53/80 | DNSEnum - Attempts Zone Transfer.
Scan Completed in 3m 46s
[• < 35s] Deploying 54/80 | Nikto - Checks if Server is Outdated.
Scan Completed in 1s
```

Gambar 4. 7 HTTP(Hypertext Transfer Protocol)

Pada Kali Linux, HTTP (Hypertext Transfer Protocol) digunakan secara luas dalam berbagai konteks, terutama dalam keamanan siber dan pengujian penetrasi. Berikut adalah beberapa aspek penting tentang HTTP dalam konteks Kali Linux:

Penggunaan HTTP di Kali Linux: Pengujian Penetrasi Web: Kali Linux dilengkapi dengan banyak alat untuk pengujian keamanan web yang berhubungan dengan HTTP, seperti Burp Suite, OWASP ZAP, Nikto, dan lainnya.

Eksploitasi dan Pemindaian: Alat-alat seperti Metasploit Framework menggunakan HTTP untuk melakukan eksploitasi dan pemindaian terhadap target.

Analisis Lalu Lintas HTTP: Kali Linux memiliki alat seperti Wireshark dan tcpdump yang dapat digunakan untuk menganalisis HTTP.

Alat-Alat HTTP di Kali Linux: Burp Suite: Sebuah platform untuk melakukan pengujian keamanan aplikasi web. Ini memungkinkan pengguna untuk menganalisis, memodifikasi, dan mengulang permintaan HTTP.

OWASP ZAP (Zed Attack Proxy): Alat untuk menemukan kerentanan dalam aplikasi web. Ini menyediakan fitur untuk menganalisis dan mengintersepsi lalu lintas HTTP.

Nikto: Scanner server web yang memeriksa server HTTP untuk menemukan berbagai jenis masalah keamanan.

Metasploit Framework: Platform untuk pengembangan dan pelaksanaan exploit. Ini sering digunakan untuk menguji kerentanan yang terkait dengan layanan HTTP.

4.1.7. Webserver

```
Vulnerability Threat Level
  high Webserver is Outdated.
Vulnerability Definition
  Any outdated web server may contain multiple vulnerabilities as their
  support would've been ended. An attacker may make use of such an opportunity
  to leverage attacks.
Vulnerability Remediation
  It is highly recommended to upgrade the web server to the available l
  atest version.
[• < 30s] Deploying 55/80 | SSLyze - Checks for ZLib Deflate Compression.
Scan Completed in 1s
[• < 3m] Deploying 56/80 | The Harvester - Scans for emails using Google's p
  assive search.
Scan Completed in 1s
[• < 30s] Deploying 57/80 | Joomla Checker - Checks for Joomla Installation.
Scan Completed in 1s
[• < 30s] Deploying 58/80 | Nmap - Checks for SNMP Service
Scan Completed in 14s
[• < 15s] Deploying 59/80 | Host - Checks for existence of IPV6 address.
Scan Completed in 11s
```

Gambar 4. 8 Webserver

Perangkat lunak server web bertugas merespons permintaan HTTP dengan tepat dari klien (seperti browser web), biasanya dalam bentuk halaman web atau data lainnya. Sehubungan dengan Kali Linux, web server sering digunakan untuk berbagai tujuan, termasuk pengujian penetrasi, pengembangan aplikasi web, dan simulasi serangan. Pengujian Penetrasi: Pengujian kerentanan aplikasi web dengan menggunakan server web sebagai target uji. Pengembangan dan Simulasi: Mengembangkan dan menguji aplikasi web lokal sebelum di-deploy ke lingkungan produksi. Simulasi Serangan: Menjalankan server web untuk mensimulasikan skenario serangan terhadap aplikasi web.

4.1.8. Ipv6(Internet Protocol version)

```
Vulnerability Threat Level
  info Does not have an IPv6 Address. It is good to have one.
Vulnerability Definition
  Not a vulnerability, just an informational alert. The host does not h
ave IPv6 support. IPv6 provides more security as IPSec (responsible for CIA -
Confidentiality, Integrity and Availablity) is incorporated into this model.
  So it is good to have IPv6 Support.
Vulnerability Remediation
  It is recommended to implement IPv6. More information on how to imple
ment IPv6 can be found from this resource. https://www.cisco.com/c/en/us/solu
tions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation_CS.html
[● < 30s] Deploying 60/80 | Dmitry - Passively Harvests Emails from the Domai
n.
Scan Completed in 11s
```

Gambar 4. 9 Ipv6 (Internet Protocol Version)

(Protokol Internet versi 6), iterasi terbaru dari protokol yang dimaksudkan untuk menggantikan IPv4.

Alamat 32-bit digunakan dalam IPv4, sehingga menghasilkan sekitar 4,3 miliar alamat berbeda. Ketika jumlah perangkat yang terhubung ke Internet meningkat, alamat IPv4 semakin sulit didapat. Karena alamat 128-bit digunakan dengan IPv6, ada sekitar 340 undecillion ($3,4 \times 10^{38}$) alamat unik yang mungkin. memadai untuk kebutuhan sekarang dan masa depan.

IPv6 solusi untuk keterbatasan alamat IPv4, menawarkan ruang alamat yang lebih besar dan fitur-fitur tambahan untuk meningkatkan efisiensi dan keamanan jaringan. Dengan adopsi yang terus meningkat, IPv6 menjadi penting bagi infrastruktur Internet masa depan.

4.1.9. Email Address

```
Vulnerability Threat Level
low Email Addresses discovered with DMitry. [1] No such file or dir
Vulnerability Definition
Chances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform brute-force attacks on not just email servers, but also on other legitimate panels like SSH, CMS, etc with a password list as they have a legitimate name. This is however a shoot in the dark scenario, the attacker may or may not be successful depending on the level of interest
Vulnerability Remediation
Since the chances of exploitation is feeble there is no need to take action. Perfect remediation would be choosing different usernames for different services will be more thoughtful.
[• < 25s] Deploying 61/80 | SSLyze - Checks for OCSP Stapling.
Scan Completed in 1s
[• < 15s] Deploying 62/80 | Nmap - Checks for MS-SQL Server DB
Scan Completed in 14s
[• < 25s] Deploying 63/80 | WHOIs - Checks for Administrator's Contact Information.
Scan Completed in 11s
[• < 30s] Deploying 64/80 | SSLyze - Checks for Session Resumption Support with [Session IDs/TLS Tickets].
```

Gambar 4. 10 Email Address

Alamat email (email address) digunakan dalam berbagai konteks, terutama dalam keamanan siber, Di Kali Linux, alamat email digunakan dalam berbagai alat dan konteks untuk tujuan pengujian penetrasi, analisis keamanan, dan administrasi jaringan. Dengan memanfaatkan alat-alat yang tersedia di kali linux, para profesional keamanan dapat menguji dan meningkatkan keamanan email.

4.1.10. X-Xss Protection

```
Vulnerability Threat Level
medium X-XSS Protection is not Present [1] No such file or dir
Vulnerability Definition
As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
[• < 35s] Deploying 73/80 | Nikto - Checks the Domain Headers.
Scan Completed in 2s
```

Gambar 4. 11 X-Xss Protection

Dalam konteks keamanan siber, "vulnerable headers" mengacu pada header HTTP yang tidak dikonfigurasi dengan benar atau hilang, yang dapat membuat aplikasi web rentan terhadap berbagai jenis serangan. Di Kali Linux, pengujian header ini merupakan bagian penting dari penilaian keamanan aplikasi web.

Header HTTP komponen dari permintaan dan respons HTTP yang menyediakan informasi tambahan tentang permintaan atau respons tersebut. Header ini dapat digunakan untuk mengontrol perilaku browser dan server.

4.1.11. Vulnerability Headrs

```
Vulnerability Threat Level
medium Some vulnerable headers exposed.
Vulnerability Definition
Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
[• < 45m] Deploying 74/80 | Nmap [Slowloris DoS] - Checks for Slowloris Denial of Service Vulnerability.
Scan Completed in 30m 22s
[• < 35s] Deploying 75/80 | Nikto - Checks for HTTP PUT DEL.
Scan Completed in 1s
[• < 35s] Deploying 76/80 | Nikto - Checks for Shellshock Bug.
Scan Completed in 4s
[• < 35m] Deploying 77/80 | DirB - Brutes the target for Open Directories.
Scan Completed in 3s
```

Gambar 4. 12 Vulnerability Headres

Dalam konteks keamanan siber, "vulnerable headers" mengacu pada header HTTP yang tidak dikonfigurasi dengan benar atau hilang, yang dapat membuat aplikasi web rentan terhadap berbagai jenis serangan. Di Kali Linux, pengujian header ini merupakan bagian penting dari penilaian keamanan aplikasi web.

Header HTTP komponen dari permintaan dan respons HTTP yang menyediakan informasi tambahan tentang permintaan atau respons tersebut. Header ini dapat digunakan untuk mengontrol perilaku browser dan server.

4.1.12. Directories

```
Vulnerability Threat Level
medium Open Directories Found with DirB.
Vulnerability Definition
Attackers may find considerable amount of information from these directories. There are even chances attackers may get access to critical information from these directories.
Vulnerability Remediation
It is recommended to block or restrict access to these directories unless necessary.
[● < 45s] Deploying 78/80 | Wafw00f - Checks for Application Firewalls.
Scan Completed in 1s
[● < 15m] Deploying 79/80 | AMass - Brutes Domain for Subdomains
Scan Completed in 17s
```

Gambar 4. 13 Directories

Direktori struktur fundamental dalam sistem file Linux yang digunakan untuk mengatur dan menyimpan file. Di Kali Linux, seperti di distribusi Linux lainnya, memahami direktori dan hierarki sistem file sangat penting untuk navigasi, manajemen file, dan administrasi sistem.

Direktori Utama pada kali Linux

a. / (Root)

Deskripsi: Direktori root adalah dasar dari hierarki sistem file. Semua file dan direktori lain berada di bawah direktori root.

Penggunaan: Hanya pengguna root yang memiliki izin penuh di direktori ini.

b. /bin

Deskripsi: Berisi program biner penting yang digunakan oleh semua pengguna.

Contoh Isi: Perintah dasar seperti ls, cp, mv, rm.

c. /sbin

Deskripsi: Berisi program biner penting yang biasanya digunakan oleh administrator sistem.

Contoh Isi: Perintah administrasi seperti ifconfig, reboot, shutdown.

d. /etc

Deskripsi: Berisi file konfigurasi sistem.

Contoh Isi: File konfigurasi jaringan (/etc/network), file konfigurasi layanan (/etc/apache2).

e. /home

Deskripsi: Berisi direktori home untuk setiap pengguna.

Contoh Isi: Direktori home untuk pengguna user1 berada di /home/user1.

f. /root

Deskripsi: Direktori home untuk pengguna root.

Penggunaan: Digunakan untuk file pribadi dan konfigurasi root.

g. /var

Deskripsi: Berisi file yang berubah-ubah seperti log, antrian cetak, dan file temporer.

Contoh Isi: Log sistem (/var/log), file email (/var/mail), spool cetak (/var/spool).

h. /tmp

Deskripsi: Berisi file temporer yang dapat dihapus setelah reboot.

Penggunaan: Tempat penyimpanan sementara untuk aplikasi.

i. /usr

Deskripsi: Berisi program dan file yang digunakan oleh pengguna.

Contoh Isi: Program biner (/usr/bin), library (/usr/lib), dokumentasi (/usr/share/doc).

j. /lib

Deskripsi: Berisi library penting yang dibutuhkan oleh program di /bin dan /sbin.

Contoh Isi: Library bersama (/lib/libc.so.6).

k. /opt

: Berisi paket perangkat lunak tambahan.

Penggunaan: Digunakan untuk aplikasi yang diinstal secara manual.

l. /mnt dan /media

Deskripsi: Berisi titik kait (mount points) untuk sistem file yang di-mount secara sementara, seperti drive USB dan CD-ROM.

4.1.13. Subdomain With Amas

```
Vulnerability Threat Level
  medium Found Subdomains with AMass
Vulnerability Definition
  Attackers may gather more information from subdomains relating to the
  parent domain. Attackers may even find other services from the subdomains an
  d try to learn the architecture of the target. There are even chances for the
  attacker to find vulnerabilities as the attack surface gets larger with more
  subdomains discovered.
Vulnerability Remediation
  It is sometimes wise to block sub domains like development, staging t
  o the outside world, as it gives more information to the attacker about the t
  ech stack. Complex naming practices also help in reducing the attack surface
  as attackers find hard to perform subdomain bruteforcing through dictionaries
  and wordlists.
[● < 30s] Deploying 80/80 | ASP.Net Misconfiguration - Checks for ASP.Net Mis
configuration.

Scan Completed in 1s

Preliminary Scan Phase Completed.
```

Gambar 4. 14 Subdomain With Amas

Amass open-source yang digunakan untuk melakukan pengintaian dan pemetaan subdomain secara pasif dan aktif. Ini sangat berguna bagi profesional keamanan siber dan penguji penetrasi untuk menemukan subdomain tersembunyi yang mungkin tidak diketahui atau tidak dipublikasikan. Berikut adalah penjelasan tentang subdomain dan bagaimana menggunakan AMass untuk melakukan pengintaian subdomain di Kali Linux.

4.2. Tools Yang Di Gunakan Dalam Uji Penetrasi

4.2.1. Rapid Scan

Rapid Scan alat open-source yang tersedia di Kali Linux untuk melakukan pemindaian cepat terhadap situs web guna menemukan berbagai jenis kerentanan. Berikut adalah beberapa fungsi utama dari Rapid Scan Banyak kerentanan, termasuk *SQL Injection*, *Cross-Site Scripting (XSS)*, dan kerentanan penyertaan file, dapat ditemukan di aplikasi web populer dengan Rapid Scan. Rapid Scan mengintegrasikan hasil dari berbagai alat keamanan lainnya,

sehingga memberikan laporan yang lebih lengkap dan terperinci. Selain memeriksa aplikasi web, Rapid Scan juga memeriksa konfigurasi server web untuk menemukan kelemahan yang dapat dieksploitasi. Rapid Scan menghasilkan laporan yang dapat disesuaikan berdasarkan kebutuhan pengguna, memungkinkan untuk fokus pada jenis kerentanan tertentu atau bagian spesifik dari aplikasi web.

Rapid Scan dirancang untuk melakukan pemindaian dengan cepat, memungkinkan pengguna untuk dengan cepat mendapatkan wawasan awal tentang status keamanan situs web. Rapid Scan juga memeriksa pengaturan SSL/TLS pada server web untuk memastikan bahwa tidak ada kelemahan dalam implementasi protokol keamanan ini. Rapid Scan dapat dijalankan secara periodik untuk melakukan pemindaian berkala terhadap situs web, memastikan bahwa situs tersebut tetap aman dari kerentanan baru. Rapid Scan sangat berguna bagi profesional keamanan dan administrator jaringan untuk melakukan pemindaian cepat dan efektif terhadap situs web guna mengidentifikasi dan memperbaiki kerentanan.

4.2.2. Tahapan yang di gunakan

1. Nmap: Di gunakan Untuk Pemindaian Port:

```
(kali@kali)-[~/rapidscan]
└─$ sudo nmap -T4 -F 172.16.10.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 13:14 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.54 seconds
```

Gambar 4. 15 Nmap

- T4 berfungsi untuk meningkatkan kecepatan pemindaian
- -F Fast scan, hanya memindai port yang paling umum di gunakan

2. Mascan: pemindaian port yang sangat cepat.

```
(kali@kali)-[~/rapidscan]
└─$ sudo masscan 172.16.10.1 -p1-65535 --rate=1000
[+] resolving router 172.16.10.1 with ARP (may take some time)...
[-] FAIL: ARP timed-out resolving MAC address for router eth1: "0.0.0.0"
[hint] try "--router ip 192.0.2.1" to specify different router
[hint] try "--router-mac 66-55-44-33-22-11" instead to bypass ARP
[hint] try "--interface eth0" to change interface
```

Gambar 4. 16 Mascan

- -p1 -65535 berfungsi untuk memindai semua port
- --rate=1000 berfungsi untuk mengatur kecepatan pemindaian (paket perdetik)

3. Netcat: Pemindaian Port Sederhana

```
(kali㉿kali)-[~/rapidscan]
└─$ sudo nc -zv 172.16.10.1 1-1000
172.16.10.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [172.16.10.1] 1000 (?): No route to host
(UNKNOWN) [172.16.10.1] 999 (?): No route to host
(UNKNOWN) [172.16.10.1] 998 (?): No route to host
(UNKNOWN) [172.16.10.1] 997 (?): No route to host
(UNKNOWN) [172.16.10.1] 996 (?): No route to host
(UNKNOWN) [172.16.10.1] 995 (pop3s): No route to host
(UNKNOWN) [172.16.10.1] 994 (?): No route to host
(UNKNOWN) [172.16.10.1] 993 (imaps): No route to host
^Z
zsh: suspended sudo nc -zv 172.16.10.1 1-1000
```

Gambar 4. 17 Net Cat

- -z berfungsi untuk mode pemindaian , tidak mengirimkan data.
- -v berfungsi untuk mode verbose, memberikan output yang lebih detail.

1.1000 berfungsi untuk rentang port yang akan di pindai.