ISSN: 2252-4983

ANALISIS VULNERABLE PORT PADA CLIENT PENGGUNA PUBLIK WIFI

Jemi Yohanis Babys
Program Studi Teknik Informatika
STIMIK Kupang
Email: betajemz@gmail.com

ABSTRAK

Penggunaan publik *wifi* sangat rentan terhadap *attacker*. Salah satu cara yang dapat dimanfaatkan oleh *attacker* untuk melakukan eksploitasi dan menyebarkan *malware* pada jaringan publik *wifi* adalah dengan cara memanfaatkan *vulnerable port* pada *client*. Untuk mengatasi hal ini, maka dalam penelitian ini dilakukan pengujian keamanan *port* pada *client* yang menggunakan publik *wifi*. Tahapan dalam penelitian ini adalah: 1) *Information gathering*, fungsinya untuk mengetahui target *client*, *port* yang terbuka dan *services* yang berjalan. 2) *Finding vulnerability*, berdasarkan *information gathering*, dilakukan identifikasi untuk mengetahui *potential vulnerability* pada *client*. 3) *Exploiting vulnerabilities*, melakukan *exploitation* terhadap *vulnerability* yang ditemukan. 4) *Recommendation*, bertujuan untuk memberikan solusi berupa saran untuk mengamankan *vulnerability* yang ditemukan. Hasil dari penelitian ini menunjukan bahwa terdapatnya *open port* pada pengguna *public wifi* berpotensi menyebabkan pengguna dieksploitasi oleh *attacker*. Berdasarkan penelitian yang dilakukan, diketahui bahwa, beberapa *user* tidak peduli dengan keamanan informasi, terutama mengenai pentingnya melakukan *update* pada aplikasi maupun *update* pada sistem operasi yang digunakan, dan juga pengguna masih kurang sadar mengenai pentingnya keamanan *open port* yang dapat berpengaruh terhadap keamanan informasi.

Kata kunci: *vulnerability, vulnerable port,* publik *wifi*.

ABSTRACT

The use of public wifi is particularly vulnerable to attackers. One of many ways that attackers can be use to exploit and spread malware on public wifi is by exploiting vulnerable ports on the client. To solve this problem, in this research the researcher will test the security port on the public wifi client. Here are the steps of this research: 1) Information gathering, this stage to find out the target client, open port and running services. 2) Finding vulnerability, based on information gathering, researchers will perform identification to determine potential vulnerability in client. 3) Exploiting vulnerabilities, function of this step is to exploit vulnerability were found in client. 4) Recommendation, aims to provide solutions like advice to secure the vulnerability were found. The results of this study indicate that the presence of open ports on public wifi users has the potential to cause users to be exploited by the attacker. Based on the research, it is known that, some users do not care about the security of information, especially regarding the importance of updating the applications and updating the operating system, and also users are still less aware of the importance of open port security that can affect the security of information.

Keywords: *vulnerability, port, public wifi.*

1. PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi jaringan komputer dan internet saat ini, berkembang juga ancaman terhadap keamanan jaringan. Oleh karena itu, keamanan jaringan harus menjadi perhatian utama dalam membangun jaringan untuk menjamin keamanan informasi digital yang berada di dalamnya [4].

Menurut data yang diperoleh dari *The European Union Agency for Network and Information Security* (ENISA) salah satu masalah keamanan jaringan yang terjadi pada bulan Mei 2017 adalah munculnya *crypto-ransomware* yang sering disebut *WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY* yang menyerang berbagai organisasi dan perusahaan. *WannaCry* menyebar dengan memanfaatkan *vulnerability* pada *port* 445. *Port* 445 merupakan *port* yang digunakan oleh SMB (*Server Message Block*). SMB merupakan protokol pada *Microsoft Windows* yang digunakan untuk melakukan *file-sharing* antar *client* dalam jaringan. Berdasarkan data dari ENISA tersebut diketahui bahwa *WannaCry* menyebar dengan memanfaatkan *vulnerability* pada sistem operasi *Windows* [6].

Serangan yang memanfaatkan *vulnerable port* seperti *WannaCry* bisa saja terjadi lagi, terutama pada jaringan publik seperti publik *wifi* yang sering dijumpai di *cafe*, restoran, hotel maupun *airport*. Jaringan ini penuh dengan resiko keamanan yang tentunya akan mengancam informasi yang terdapat didalamnya [4].

Oleh karena itu, dalam penelitian ini akan menganalisis *vulnerable port* pada *client* yang menggunakan jaringan publik *wifi* untuk mencegah terjadinya eksploitasi dan penyebaran *malware* melalui *vulnerable port*.

2. METODOLOGI PENELITIAN

Metode pengumpulan data dalam penelitian ini adalah sebagai berikut:

2.1 Studi Kepustakaan

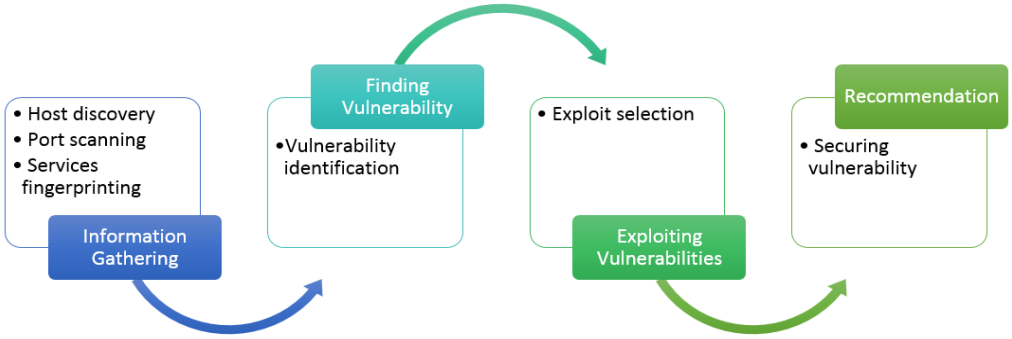
Metode studi kepustakaan dilakukan dengan mempelajari literatur-literatur terkait yang berhubungan dengan penelitian untuk digunakan sebagai acuan.

2.2 Observasi

Pada metode observasi ini akan dilakukan pengamatan secara langsung pada jaringan publik *wifi*. Dalam penelitian ini observasi dilakukan pada jaringan *wifi* di kampus STIMIK Kupang, karena jaringan *wifi* ini cukup untuk mewakili jaringan publik *wifi* yang ada di Kota Kupang.

2.3 Eksploitasi

Dalam penelitian ini eksploitasi digunakan untuk mengetahui *vulnerable port* pada *client*. Eksploitasi dilakukan menggunakan Kali Linux *Operating System*, *Zenmap*, *Nmap*, dan *Metasploit Framework*. Tahapan dalam melakukan eksploitasi dapat dilihat pada gambar 1.



Gambar 1. Tahapan Eksploitasi [8]

2.3.1 Information Gathering

Tahap awal dalam proses pengujian yaitu pengumpulan informasi, informasi yang dikumpulkan berupa *host* (*client*) target yang akan dianalisis, status *port*, dan *services* yang berjalan.

2.3.2 Finding Vulnerability

Tahap ini mencari dan mempelajari *potential vulnerability* dari *services* yang berjalan pada komputer target.

2.3.3 Exploiting Vulnerability

Tahap *exploiting vulnerability* merupakan upaya menguji *vulnerability* yang ditemukan.

2.3.4 Recommendation

Recommendation merupakan tahap memberikan solusi berupa saran untuk mengamankan setiap *vulnerability* yang ditemukan.

Terdapat beberapa penelitian yang menunjukan resiko dari *vulnerable port* diantaranya Navamani, B.A., Yue, C. dan Zhou, X dalam penelitian berjudul *An Analysis of Open Ports and Port Pairs in EC2 Instances*, penelitian ini melakukan analisis untuk menunjukan resiko status *open port* pada *cloud environment*. Analisis dilakukan di *virtual machine* (VM) *instances Amazone Web Services* (AWS) dengan menggunakan *software* pemindai jaringan Zmap yang telah di *costumized*. Proses pemindai

jaringan menargetkan *single port* pada *multiple server*. Penelitian ini menyoroti bagaimana penyerang dapat melakukan serangan yang tidak terdeteksi dengan mengkombinasikan 2 karakteristik *port* yang berbeda didalam sebuah VM *instance*. Selain itu, dipaparkan beberapa cara untuk melindungi *port* dari serangan [3].

Lee, *et. al.* dalam penelitiannya mengenai *Implementation and Vulnerability Test of Stealth Port Scanning Attacks using ZMap of Censys Engine*. Dalam penelitian ini dilakukan proses *sthealt port scanning* menggunakan Zmap di Universitas Ajou. Proses *scanning* dilakukan di dari 12.000 *hosts* pada 2 *range* IP *address*. *Port* yang di *scan* adalah *port* 23 (*telnet*), 25 (smtp), 80 (http), 443 (https), 525 (*printer*) dan port 25565 (game *minecraft*). Berdasarkan hasil penelitian yang dilakukan diketahui bahwa *port* 525 rentan terhadap serangan [2].

Babys, Kusrini, dan Sudarmawan membahas tentang Analisis Aspek Keamanan Informasi Jaringan Komputer (Studi Kasus: STIMIK Kupang). Penelitian ini melakukan analisis terhadap aspek *confidentiality* yang merupakan salah satu aspek dari keamanan informasi. Analisis dilakukan dengan melakukan *scanning* menggunakan Zenmap pada setiap *client* dalam jaringan. Hasil *scanning* menemukan *port* 139 dan 445 terbuka. Berdasarkan hasil *scanning* dilakukan eksploitasi dengan memanfaatkan kelemahan pada *port* 445. Hasil dari penelitian ini adalah ditemukannya kelemahan keamanan baik pada *tools* keamanan yang digunakan maupun kelemahan pada instalasi jaringan. Solusi-solusi yang dihasilkan dalam penelitian ini adalah sebagai berikut: (1) Melakukan segmentasi pada jaringan menggunakan VLAN dengan metode *Access Control Lists* (ACL) dan *Port Security*; (2) Melakukan instalasi *firewall* disetiap *client/host* dalam jaringan untuk melindungi setiap *port* yang terbuka pada sistem operasi yang digunakan, dalam penelitian ini menunjukan bahwa aplikasi McAfee 8.8 mampu melindungi *port* yang terbuka [1].

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan di kampus STIMIK Kupang. Tahap pertama dalam penelitian adalah tahap *information gathering*, pada tahap ini dilakukan proses *scanning* terhadap 378 IP *address* yang dialokasikan pada jaringan *wifi* yang digunakan bersama oleh Mahasiswa/I, dan jaringan *wifi* yang digunakan bersama oleh Dosen dan Pegawai. Proses scanning pada tahap ini bertujuan untuk mencari IP *address* dengan status *open port*. Hasil dari *scanning* yang dilakukan dapat dilihat pada tabel 1 berikut ini.

Tabel 1. Daftar ip *address* dengan status *open port*

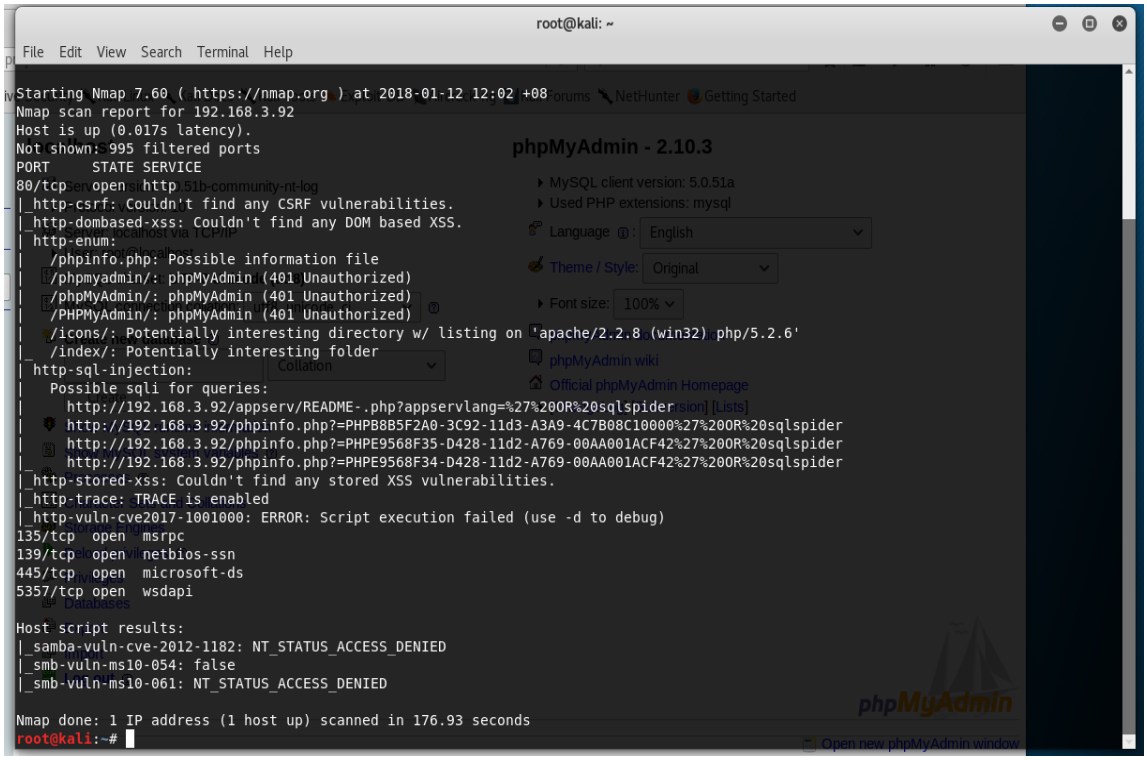
No	IP *address*	*Open port*
1	10.10.16.36/26	80, 8080
2	10.10.16.42/26	80, 135, 139, 445, 8080
3	10.10.16.44/26	80, 135, 139, 445, 5357
4	10.10.16.45/26	80, 135, 139, 445
5	192.168.2.2/26	80, 135, 139, 445, 5357, 49156
6	192.168.2.8/26	80, 135, 139, 445, 1028
7	192.168.2.9/26	80, 135, 139, 445, 49156
8	192.168.2.10/26	80
9	192.168.2.11/26	80
10	192.168.2.15/26	80, 135, 139, 445, 49156
11	192.168.2.16/26	80
12	192.168.2.19/26	80, 135, 139, 445,7070
13	192.168.2.20/26	80
14	192.168.2.50/26	80, 135, 139, 445, 49156
15	192.168.2.51/26	80, 135, 443, 445, 5357
16	192.168.2.55/26	80, 135, 139, 443, 445, 3306
17	192.168.2.56/26	80, 6646
18	192.168.3.13/24	80, 135, 139, 445, 49152, 49153, 49154, 49155
19	192.168.3.55/24	80, 135, 139, 445, 1028
20	192.168.3.92/24	80, 135, 443, 445, 5357
21	192.168.3.93/24	80
22	192.168.3.95/24	80
23	192.168.3.96/24	80
24	192.168.3.100/24	80, 49156
25	192.168.3.151/24	135, 139, 445
26	192.168.3.200/24	80, 135, 139, 445

Berdasarkan hasil *scanning* pada tabel 1 terdapat 26 IP *address* aktif berstatus *open port* dari 378 IP *address* yang dialokasikan. Pada penelitian ini terdapat juga beberapa IP *address* yang tidak terdeteksi hasil *scanning*, hal ini dikarenakan IP *address* tersebut dilindungi oleh *personal firewall*. Berikut merupakan informasi mengenai *port* yang ditemukan dari hasil *scanning* menggunakan Zenmap.

Tabel 2. Daftar *port* hasil *scanning*

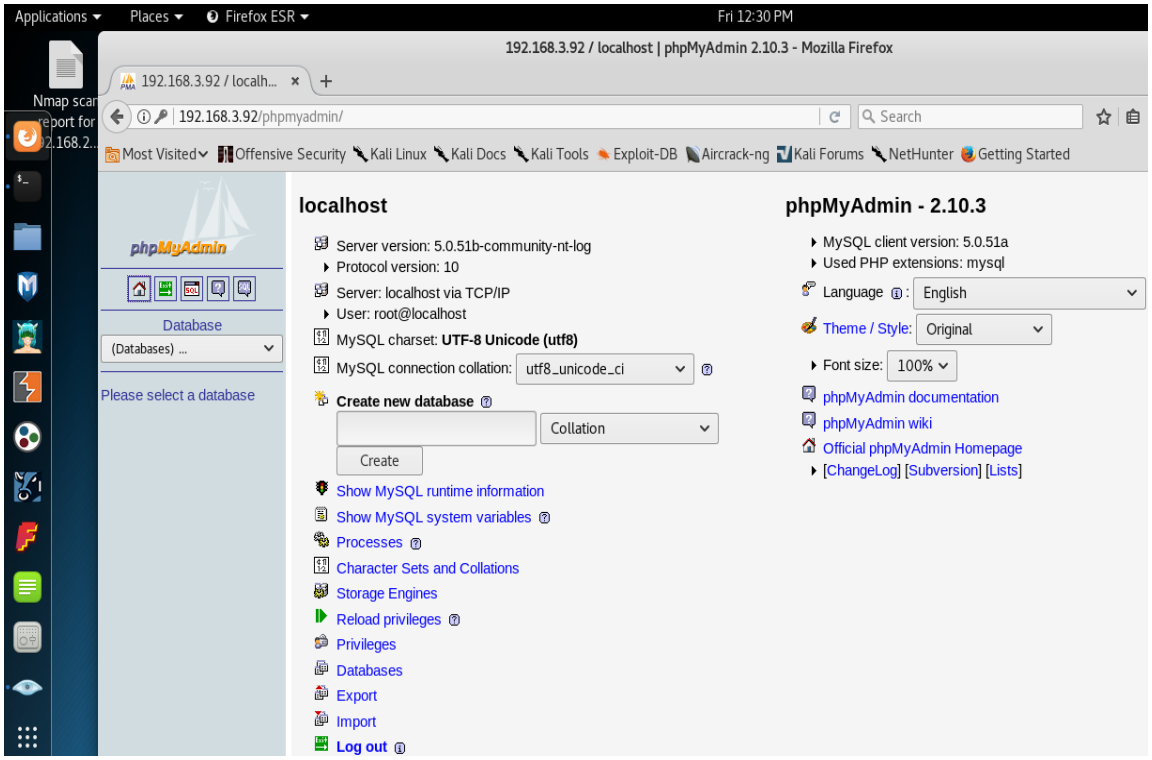
No	*Port*	*State*	*Service*	*Version*
1	80/tcp	*Open*	*Tcpwrapped*	-
			http	*Apache httpd 2.2.21 ((Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1)*
			http	*Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)*
			http	*TP-LINK WA901ND WAP http config*
			http?	-
2	8080/tcp	*Open*	*http-proxy?*	-
			http	*Apache httpd 2.4.6 ((Win32) PHP/5.4.17)*
3	135/tcp	*Open*	*Msrpc*	*Microsoft Windows RPC*
4	139/tcp	*Open*	*Netbios-ssn*	*Microsoft Windows netbios-ssn*
5	445/tcp	*Open*	*Microsoft-ds*	*Microsoft Windows 7 – 10 microsoft-ds (workgroup: WORKGROUP)*
			Microsoft-ds?	-
6	1028/tcp	*Open*	*Unknown*	-
7	49156/tcp	*Open*	*Unknown*	-
8	49152/tcp	*Open*	*Unknown*	-
9	49153/tcp	*Open*	*Unknown*	-
10	49154/tcp	*Open*	*Unknown*	-
11	49155/tcp	*Open*	*Unknown*	-
12	5357/tcp	*Open*	*http*	*Microsoft HTTPAPI httpd 2.0 (SSDP/UpnP)*
13	1028/tcp	*Open*	*Unknown*	-
14	7070/tcp	*Open*	*Ssl/realserver?*	-
15	443/tcp	*Open*	*Ssl/http*	*Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)*
16	3306/tcp	*Open*	*Mysql*	*MySQL (unauthorized)*
17	6646	*open*	*Tcpwrapped*	-
18	513/tcp	*Closed*	*Login*	-
19	2000/tcp	*Closed*	*Cisco-sccp*	-

Berdasarkan hasil *scanning* menggunakan Zenmap yang ditunjukan pada tabel 2 terdapat total 19 *port*. Dari 19 *port* tersebut terdapat 17 *port* dengan status *open port* dan 2 *port* dengan status *closed port*. Tahap berikut dalam penelitian ini adalah *finding vulnerability* menggunakan *nmap* untuk mengetahui *potential vulnerability*. Berdasarkan hasil *scanning* menggunakan *nmap* terdapat *potential vulnerability* seperti yang ditunjukan pada gambar 2 dan gambar 4.



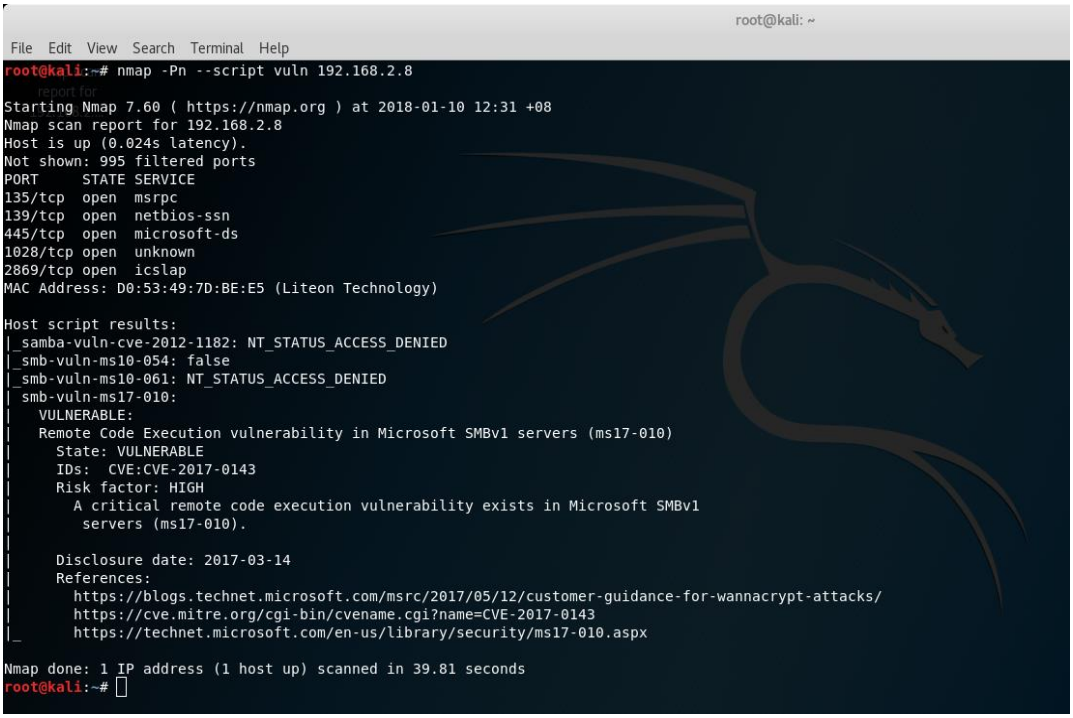
Gambar 2. *Potential Vulnerability* Pada *Port* 80

Pada gambar 2 menunjukan *potential vulnerability* di *port* 80 pada *user* dengan IP 192.168.3.92/24. *Vulnerability* ini dikarenakan terbukanya akses aplikasi *phpmyadmin* ke publik, seharusnya aplikasi *phpmyadmin* tidak dibuka aksesnya ke publik. *Vulnerability* ini berhasil di eksploitasi, ini ditunjukan pada gambar 3 dimana *attacker* berhasil *login* ke aplikasi *phpmyadmin*. hal ini tentunya beresiko terhadap keamanan data apabila didalam aplikasi *phpmyadmin* tersebut tersimpan *database* yang sifatnya penting.



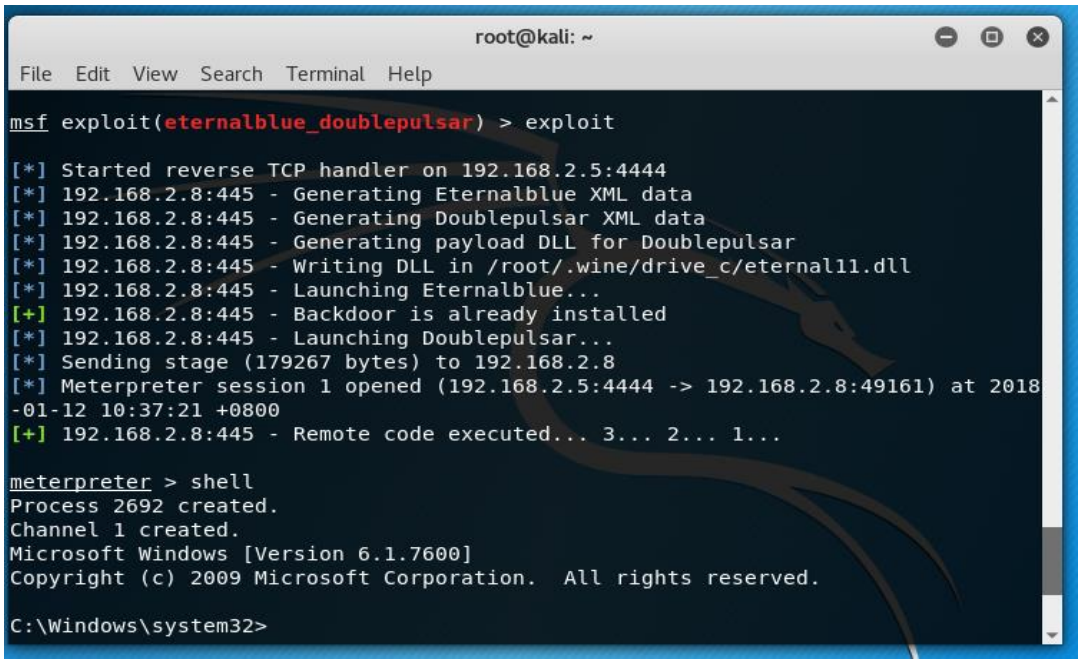
Gambar 3. Akses *Phpmyadmin*

Vulnerable port yang ditemukan berikutnya adalah pada *port* 445 milik *user* dengan IP 192.168.2.8/26, dapat dilihat pada gambar 4. *Port* 445 merupakan *vulnerable port* yang sebelumnya telah dimanfaatkan oleh *crypto-ransomware WannaCry* untuk menyebar [6]. *Vulnerability* ini terjadi karena *user* belum melakukan *update* pada sistem operasi *Windows* yang digunakan. Seperti diketahui bahwa *Microsoft* telah mengeluarkan *update* untuk mengamankan *vulnerability* pada *port* 445. Oleh karena itu, *user* disarankan untuk melakukan *update* secara periodik [7].



Gambar 4. *Potential Vulnerability* Pada *Port* 445

Pada gambar 5 berikut menunjukan *port* 445 pada *user* dengan IP 192.168.2.8/26 berhasil di eksploitasi. Terbukanya *port* 445 dikarenakan pengguna mengaktifkan fungsi *file-sharing* pada sistem operasi *Microsoft Windows*. Oleh karena itu, disarankan apabila pengguna tidak melakukan aktifitas *file-sharing* dalam jaringan publik *wifi* maka fungsi ini baiknya dinonaktifkan.



Gambar 5. *Exploit Vulnerability* Pada *Port* 445

Dari hasil eksploitasi yang dilakukan dalam penelitian ini ditemukan 2 *vulnerable port* yaitu, *port* 80 dan *port* 445. Fungsi dari masing-masing *port* dapat dilihat pada tabel 3 berikut.

Tabel 3. Daftar *vulnerable port*

No	*Port*	*State*	*Service*	Fungsi
1	80/tcp	*Open*	*http?*	Digunakan oleh aplikasi *phpmyadmin* untuk administrasi *database*
2	445/tcp	*Open*	*Microsoft-ds*	Digunakan oleh SMB untuk *file-sharing* dalam jaringan

4. KESIMPULAN

Penggunaan publik *wifi* penuh dengan resiko keamanan, hal ini dikarenakan publik *wifi* biasanya memiliki banyak pengguna dengan banyak motivasi yang tidak diketahui. Oleh karena itu, perlu kesadaran dari pengguna publik *wifi* mengenai keamanan sehingga bisa berinternet secara aman dan terhindar dari tindakan eksploitasi yang memanfaatkan *vulnerable port*. Berdasarkan pengujian yang telah dilakukan disimpulkan bahwa terdapat beberapa hal yang bisa dilakukan untuk menghindarkan pengguna publik *wifi* dari tindakan eksploitasi yang memanfaatkan *vulnerable port*.

a. Melakukan *update* secara periodik baik pada sistem operasi yang digunakan maupun pada aplikasi yang digunakan.
b. Menggunakan *personal firewall* yang dapat melindungi setiap *port* yang terbuka.
c. Pada waktu mengakses publik *wifi* pengguna diharapkan menutup aplikasi-aplikasi yang tidak diperlukan yang dapat menyebabkan terbukanya *port*.
d. Pada waktu mengakses publik *wifi*, untuk pengguna sistem operasi Windows diharapkan menonaktifkan fitur *file and printer sharing* dan juga menonaktifkan fitur *network discovery*.

Untuk penelitian selanjutnya diharapkan dapat dikembangkan suatu sistem pada jaringan publik *wifi* yang berfungsi sebagai *network firewall* yang dapat melindungi setiap *client* yang terhubung dari tindakan eksploitasi yang memanfaatkan *vulnerable port*.

DAFTAR PUSTAKA

[1] Babys, Jemi Yohanis., Kusrini. and Sudarmawan., 2013. "ANALISIS ASPEK KEAMANAN INFORMASI JARINGAN KOMPUTER (Studi Kasus: STIMIK Kupang)". *Seminar Nasional Informatika 2013 (semnasIF 2013) UPN "Veteran" Yogyakarta*, ISSN: 1979-2328, E-7 – E14.

[2] Lee, S., Im, S.Y., Shin, S.H., Roh, B.H. and Lee, C., 2016. Implementation and vulnerability test of stealth port scanning attacks using ZMap of censys engine. *Information and Communication Technology Convergence (ICTC) International Conference*, pp. 681-683.

[3] Navamani, B.A., Yue, C. and Zhou, X., 2017. An Analysis of Open Ports and Port Pairs in EC2 Instances. *IEEE 10th International Conference*, pp.790-793.

[4] Pawar, M.V. and Anuradha, J. 2015. Network security and types of attacks in network. *Procedia Computer Science, 48,* pp.503-506.

[5] Symantec employee. The risks of public Wi-Fi, https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html, diakses jam 08.38 WITA tanggal 20 Februari 2018.

[6] The European Union Agency for Network and Information Security (ENISA). WannaCry Ransomware Outburst, https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst, diakses jam 08.40 WITA tanggal 20 Februari 2018.

[7] The Microsoft Security Response Center. Customer Guidance for WannaCrypt attacks, https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/, diakses jam 08.34 WITA tanggal 20 Februari 2018.

[8] Weidman, Georgia. (2014). *Penetration testing: A Hands-On Introduction to Hacking.* San Francisco: No Starch Press, Inc.