PENERAPAN ZERO ENTRY HACKING DIDALAM SECURITY MISCONFIGURATION PADA VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TESTING)

Rama Sahtyawan [1)]

[1)] *Teknologi Informasi FTTI UNJANI Yogyakarta*
email : ramasahtyawan@unjaya.ac.id

Abstraksi

Serangan terhadap sistem jaringan komputer mengalami update serangan menjadi lebih canggih. Perusahaan dituntut untuk memastikan Cyber Security yang aman untuk melindungi dari serangan hacker. Penelitian ini, Mengimplementasikan VAPT (Vulnerability Assessment and Penetration Testing) menggunakan metode ZEH (Zero Entry Hacking)Penetration Testing Methodology untuk mengetahui kerentanan SMB (server Message block) dan RDP(remote desktop) pada server yang dapat dieksploitasi serta memberi penyerang hak akses terhadap server yang mampu memanipulasi data pada server.

***Kata Kunci* :**
Cyber Security, vapt, zeh, smb, rdp.

Pendahuluan

Didalam menyelesaikan masalah ancaman *Cyber*, sebaiknya sebuah perusahaan mematuhi regulasi keamanan yang berlaku, VAPT *(Vulnerability Assessment and Penetration Testing)* terbukti Sebagai alat penilaian yang menjamin untuk memastikan Keamanan *Cyber* dalam sebuah perusahaan. Penerapannya sudah menjadi bagian yang tidak terpisahkan dari Quality Assurance Techniques untuk keamanan sistem yang digunakan oleh perusahaan. *Vulnerability Assessment*, bertujuan untuk menemukan kemungkinan ancaman dan subset yang digunakan hacker sebagai ruang input dalam mengeksploitasi kesalahan logis dalam sistem untuk mendapatkan keuntungan dengan mengarahkan sistem ke kondisi tidak aman [1].
Penetration Testing bertujuan menilai tingkat kesulitan penyerang / peretas untuk menembus kontrol *Cyber security* sebuah perusahaan, terhadap akses tidak sah ke sistem Informasinya. VAPT dilakukan dengan mensimulasikan seorang peretas yang menyerang sistem menggunakan tools manual atau otomatis.Penguji VAPT dilakukan dengan cara memindai semua komponen sistem untuk kerentanan yang ditemukan, Evaluasi keamanan dalam hal ini dbutuhkan suatu Teknik yang didasarkan pada naluri dan pengalaman penguji.[2]. Proses VAPT juga disebut dengan Ethical Hacking. VAPT membantu mengidentifikasi dan mengendalikan ancaman dan kerentanan, sehingga mereka dapat dihilangkan sebelum peretas / penyerang ingin melakukan mengeksploitasi kedalam sistem.

Tinjauan Pustaka

Menurut penelitian oleh (Kiezun, Guo, dkk., 2009)

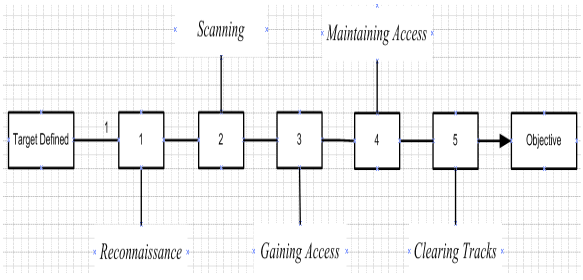
Melakukan analisis lubang keamanan yang dapat disusupi serangan terhadap website yang dibuat berbasis HTML menggunakan CMS Wordpress. sehingga bisa mengambil alamat "id=", dalam penelitian ini menguji beberapa serangan antara lain phising dan SQL Injection [3]. A Vulnerability para piranti lunak dan keras yang terdapat misconfiguration pada lubang keamanan yang dapat disalahgunakan oleh orang yang tidak memiliki otoritas[4]. Pada vulnerability scanners digunakan untuk mengecek lubang kerentanan yang terdapat pada sebuah aplikasi dan dapat menganalisis port yang tidak terkunci dan alamat IP (TCP/UDP) serta memberikan report tentang aplikasi tersebut [5]. Dengan dilakukannya penetration testing pada jaringan komputer disebuah perusahaan, maka menutup lubang keamanan yang rentan untuk disusupi oleh hacker [6].

Metode Penelitian

Metodologi ZEH (Zero Entry Hacking) merupakan suatu metodologi yang digunakan dalam penetration testing yang terdiri dari pengintaian sistem, scan, eksploitasi lubang keamanan, post eksploitasi [7].

a. Prinsip Kerja Sistem

Pada prinsip kerja sistem yang ditangani oleh institusi yang berkembang dalam keamanan jaringan yang biasa disebut *EC-Council*, informasi tersebut terdiri 5 tahapan seorang hacker mencoba masuk kedalam lubang keamanan secara *step by step* [8], seperti gambar dibawah ini



Gambar 1 Zero Entry Hacking (ZEH) methodology.

Langkah-langkah dalam gambar 1 dijelaskan sebagai berikut:

1. **Pengintaian Target *(Reconnaissance)***
   Reconnaissance adalah langkah pertama penyusup dalam merancang mencari informasi sebanyak-banyaknya *(information gathering)* dari sebuah sasaran yang dituju sebelum melakukan aksi serangan. Adapun toolsnya menggunakan perintah *ping, whois* dan dnsmap disebuah terminal, dan menangkap informasi kepada arsitektur jaringan komputer tersebut menggunakan maltego.
2. **Pemindaian *(Scanning)***
   Pemindaian adalah sebuah tahapan seorang *hacker* menggunakan bernacam-macam *tools* mencoba berusaha mencari lubang masuk kedalam titik temu sebagai target serangan dengan mencoba men-scan awal port dalam sistem jaringan (*port scanning*), atau bisa juga melalui pemetaan jaringan (*network mapping*), Dalam *scanning* terdapat beberapa langkah model diantaranya*:*
   a) Pre-Attack: suatu proses pengendusan sebelum melakukan serangan dengan memata-matai terhadap lokasi yang menjadi target.
   b) *Port Scanne*r: suatu proses pengendusan didalam melakukan serangan dengan memata-matai *port* yang terbuka dengan bantuan aplikasi seperti *port scanners, vulnerability scanners.*
   c) *Extract Information*: hacker berhasil masuk ke sasaran yang dituju dan memperoleh data informasi melalui port yang tidak terkunci dan terbuka sehingga penyusup dengan mudah untuk masuk melakukan penyerangan.
3. **Mendapatkan akses *(Gaining Access)***
   Sebuah proses dimana hacker melakukan percobaan untuk memperoleh otoritas akses di sistem operasi, selanjutnya penyusup menyerang sistem seperti password cracking dan denial of service.
4. **Mempertahankan Akses *(Maintaining Access).***
   Mempertahankan Akses menjelaskan tentang aktifitas penyusup dalam memperoleh otoritas sistem. Penyusup akan menambal lubang keamanan di sistem dari ancaman Penyusup dapat merubah data dan informasi tersebut.
5. **Menghapus Tracks *(Clearing Tracks).***
   Menghapus Tracks adalah proses penyusup menghapus bermacam kejanggalan didalam sistem yang dilalui agar penyusup tidak diketahui lokasinya, setelah itu penyusup menghapus rekam jejak log tersebut.

b. Komponen Pendukung

Didalam komponen tersebut dilakukan pengujian untuk melihat kerentanan terhadap lokasi website menggunakan tools, diantaranya:

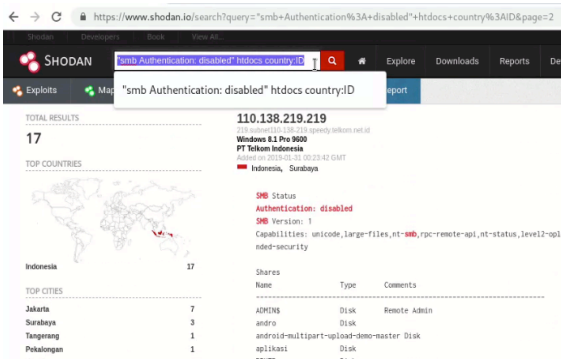
1). **Kali Linux**
Kali Linux merupakan sistem operasi Linux yang memiliki keunikan pada pengujian penetrasi. Kali Linux disebut juga dengan *BackTrack*, dengan berfokus pada pengujian kolaborasi tiga penetrasi Linux yang beragam: Auditor*, IWHAX,* dan *WHOPPIX*..

2) ***DbVisualizer***.
DbVisualizer adalah perangkat database yang dikembangkan dengan banyak platform bisa digunakan di berbagai sistem operasi.

Hasil Analisa dan Pembahasan

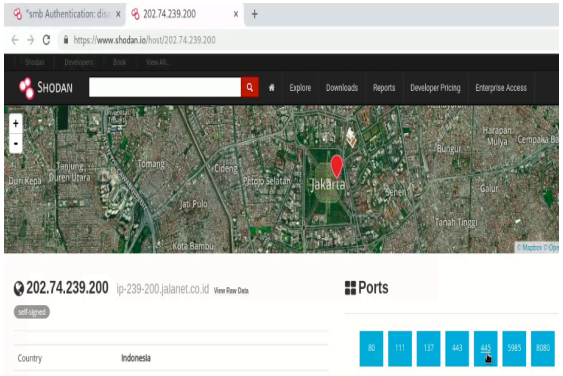
Hasil Analisa dan pembahasan lebih lanjut akan dijelaskan tahapan prosesnya menggunakan metode Zero Entry Hacking (ZEH). Adapun langkah-langkahnya sebagai berikut :

1. **Pengintaian Target *(Reconnaissance)***
   Pada tahap ini, peneliti memposisikan diri menjadi seorang hacker, untuk mencari informasi tentang target yang akan disusupi, dibawah ini peneliti melakukan langkah-langkah berikut ini :
   mencari bug smb, di smbclient "//xxx.xxx.xxx.xxx/htdocs" –N menggunakan shodan.io seperti gambar dbawah ini



Gambar 2

Setelah itu, Check Ports tersebut



Gambar 2

a) Download file config.php
\\xxx.xxx.xxx.xxx\htdocs\amor\config\config.php

```
<?php
    $server="blah.blah.com";
    //$server="localhost";
    $database="blah";
    $user="sa";
    $password="blah";
?>
```

2. Pemindaian *(Scanning).*

Setelah kita mengetahui bahwa ternyata target menggunakan Ms sql server, selanjutnya melakukan scanning port ke situs web tersebut dengan menggunakan nmap, lalu akan tampil seperti dibawah ini:

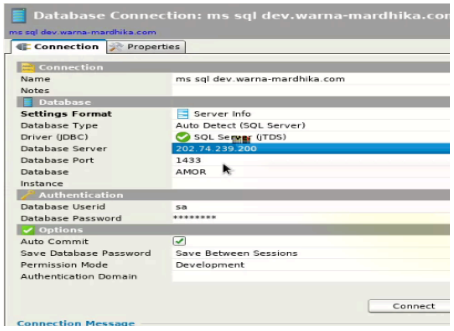
```
Nmap scan report for ip-239-200.jalanet.co.id
Host is up (0.16s latency).
Not shown: 982 closed ports
PORT      STATE    SERVICE
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open     http
111/tcp   open     rpcbind
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
1433/tcp  open     ms-sql-s
2049/tcp  open     nfs
2383/tcp  open     ms-olap4
3389/tcp  open     ms-wbt-server
5678/tcp  filtered rrac
8080/tcp  open     http-proxy
49152/tcp open     unknown
```

Gambar 4

Ternyata port 1433 dan 3389 open, langkah selanjutnya, kita mencoba untuk remote sql servernya untuk exploit shell.

3. Mendapatkan akses *(Gaining Access).*

peneliti mencoba mendapatkan otoritas hak akses dalam sistem operasi, peneliti menggunakan *DBVisualizer* untuk remote db via gui seperti gambar dibawah ini

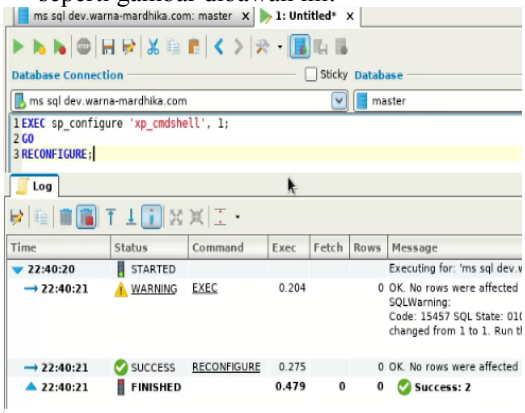


gambar 5

Tahapan selanjutnya, peneliti mengecek menjalankan script sebagai berikut :

a). Cek xp_cmdshell untuk status enable dirubah menjadi disable.

b) Jika config_value bernilai 0 berarti disable seperti gambar dibawah ini:



Gambar 6

c) Untuk test apakah xp_cmdshell sudah enable, jalankan script berikut :

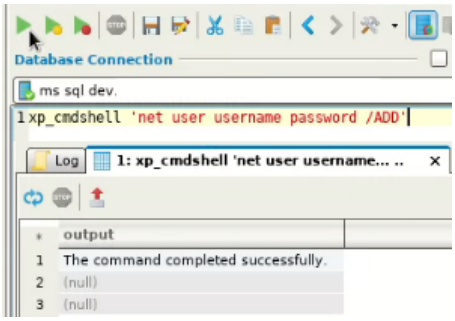
Xp_cmdshell 'dir'

4. *Maintaining access*

Pada *Maintaining access* ini peneliti akan menambal lubang keamanan dalam sistem tersebut dari ancaman penyusup lainnya, dengan membuat portal rahasia untuk mendapatkan akses kembali ke dalam sistem tersebut yang bertujuan dalam memanipulasi data tersebut, berikut tahapannya:

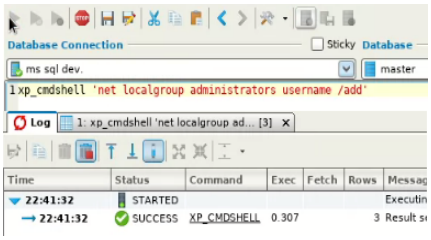
a) Add user ke group administrator. jalankan script berikut :

Xp_cmdshell 'net user username password /ADD', Seperti gambar dibawah ini:



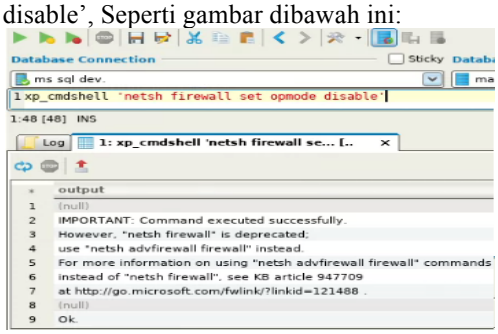
Gambar 7

b) Add user ke dalam group administrator, jalankan script berikut : *Xp_cmdshell 'net localgroup administrator username/add'*, Seperti gambar dibawah ini:



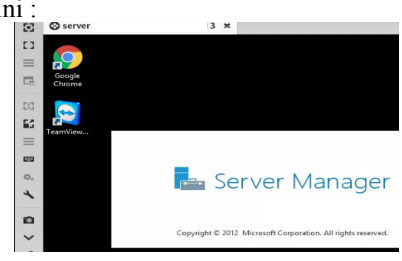
Gambar 8

c) Disable firewall, jalankan script berikut : Xp_cmdshell 'netsh firewall set opnode disable', Seperti gambar dibawah ini:



Gambar 9

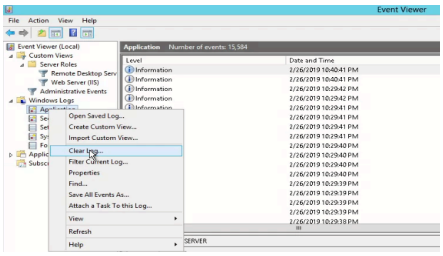
d) Setelah berhasil create new user dan menambahkan di group administrator, maka selanjutnya peneliti menggunakan ke RDP (*remote desktop*), dan berhasil masuk server tujuan, adapun tampilannya seperti dibawah ini :



Gambar 10

5. *Clearing Tracks.*

Menghilangkan rekam jejak setelah berhasil masuk ke sistem dengan cara menghapus *log* yang didalamnya terdapat serangan oleh penyusup, dengan cara menghapus history di event viewer



Gambar 11

Kesimpulan

Hasil pengujian dan analisa (VAPT) Vulnerability Assessment and Penetration Testing dengan metode Zero Entry Hacking menunjukkan banyak celah yang harus diperhatikan karena banyak sekali kesempatan bagi penyerang untuk menyerang kelemahan sistem keamanan.

Saran

a. Menggunakan sistem operasi dan kernel yang stabil dan tidak mengandung bugs, secara berkala melakukan update informasi dan pathching jika ada bug

b. Seorang admin web dan admin server sebaiknya melakukan testing terlebih dahulu, sehingga meminimalisir kesalahan coding yang akan menimbulkan bug/celah

c. Mengoptimalkan tugas dari network administrator untuk mengamati semua aktifitas yang mengakses server, log secara berkala dan mewaspadai adakah yang mencoba bruteforce dan mengecek apakah ada yang mengakses file-file aneh berextensi php

Daftar Pustaka

[1] S. Sparks, S. Embleton, R. Cunningham and C. Zou, "Automated vulnerability analysis: Leveraging control flow for evolutionary", *IEEE 23rd Annual Computer Security Applications Conference,* Dec 10-14, 2007, Miami, Florida

[2] A. Austin and L. Williams, "One technique is not enough: A comparison of vulnerability discovery techniques", *IEEE International Symposium on Empirical Software Engineering and Measurement*, Sep 22-23, 2011, Guenther, Ruhe.

[3] P. Xiong and Peyton, "A Model driven Penetration test framework for Web Applications", *IEEE 8th Annual International Conference on Privacy, Security & Trust*, Aug 17-19, 2010,Ottawa, ON, Canada.

[4] Kiezun, A., Guo, P. J., Jayaraman, K., & Ernst, M. D. (2009). Automatic creation of SQL injection and cross-site scripting attacks. *Proceedings - International Conference on Software Engineering*, 199–209. https://doi.org/10.1109/ICSE.2009.5070521

[5] EC-Council, "CEH 8 Module 20 Penetration Testing." 2012.

[6] D. P. N. Andrew Whitaker, "Penetration Testing and Network Defense", Indianapolis: Cisco Press, 2006

[7] A. Austin and L. Williams, "One technique is not enough: A comparison of vulnerability discovery techniques", *IEEE International Symposium on Empirical Software Engineering and Measurement*, Sep 22-23, 2011, Guenther, Ruhe.

[8] Engebretson, P. "The Basics of Hacking and Penetration Testing: Ethical hacking and Penetration Testing Made Easy." Waltham : Syngress, 2011