ISSN: 2745-375 **Djtechno : Journal of Information Technology Research**
Vol. 2, No. 1 Juli Tahun 2021

TEKNIK PENYERANGAN PHISHING PADA SOCIAL ENGINEERING MENGGUNAKAN SET DAN PENCEGAHANNYA

Hendri Ahmadian[1)], Aulia Sabri[2)]
1)Prodi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Ar-Raniry, Indonesia

E-mail: auliasabri43@gmail.com

Abstrak

Di era modernisasi saat ini, informasi adalah aset yang berharga bagi sebuah organisasi maupun tiap individu, karena itu melindungi informasi merupakan hal yang sangat penting bagi organisasi dan individu. Tapi kenyataannya, sistem yang memiliki keamanan tingkat tinggi pun akan tembus jika orang yang berada di dalam sistem itu melakukan kesalahan, dan dengan menggunakan social engineering hacker akan memanfaatkan kesalahan ini. Penelitian ini bertujuan untuk menjelaskan bagaimana penyerang memanfaatkan perilaku manusia dengan teknik penyerangan phishing yang merupakan salah satu metode penyerangan social engineering dengan menggunakan SET. Diakhir tulisan ini, penulis akan mencoba memberikan rekomendasi untuk melindungi informasi yang dimiliki organisasi maupun individu dari serangan Social Engineering.

Kata Kunci: *S*ocial engineering, Teknik penyerangan phishing, SET

Abstract

In modern times, information is a valuable asset for an organization and for each individual, therefore protecting information is very important for organizations and individuals. But in reality, even a highly secure system will break through if the people inside the system make a mistake, and by using social engineering, hackers will exploit this error. This study aims to explain how an attacker exploits human behavior with a phishing attack technique, which is a social engineering attack method using SET. At the end of this paper, the author will try to provide recommendations to protect information held by organizations and individuals from social engineering attacks.

Keywords: Social engineering, Phishing attack techniques, SET

PENDAHULUAN

Istilah social engineering mulai populer dikalangan praktisi IT, khususnya dibidang cybersecurity, karena memang saat memulai serangan ke suatu jaringan atau sistem yang tidak diketahui sama sekali sebelumnya, maka besar kemungkinan harus "bertanya" dan "mencuri dengar" dari orang-orang yang ada disekitar target serangan. Orang-orang yang dimaksud disini biasanya adalah karyawan atau staf dari lembaga atau perusahaan target. Disinilah keahlian social engineering sangat diperlukan. Inti dari social engineering ini adalah menemukan kelemahan manusia yang diistilahkan sebagai human element of networking (Sofana & Primartha, 2019).

Menurut acuan keamanan jaringan yang diterbitkan perusahaan pembuat OS Windows, yaitu Microsoft, Hacker yang menggunakan metode Social Engineering dapat memanfaatkan kecerobohan, kesopanan, kemalasan, bahkan antusiasme dari seorang staff di sebuah organisasi sebagai targetnya. Karena, mungkin korban tidak menyadari kalau mereka telah ditipu atau kalau pun mereka sadar mereka tidak akan memberitahukan kepada orang lain(Rafizan).

Dengan semakin maraknya penggunaan aplikasi sosial media, maka teknik social engineering pun semakin kreatif. Penyerang dapat memanfaatkan facebook, email, instagram, twitter, whatsapps dan aplikasi lain untuk mendapat informasi dari pengguna. Tekniknya pun berbagai macam, mulai dari pura-pura menyamar sebagai orang dikenal, memanfaatkan yayasan, mengirim email berisi link palsu, dan lain-lain (Sofana & Primartha, 2019).Tujuan dari dibuatnya tulisan ini adalah untuk menjelaskan bagaimana cara hacker menyerang dengan memanfaatkan kelemahan manusia menggunakan serangan phising untuk mendapatkan informasi yang berharga kemudian pada akhir tulisan juga akan dijelaskan bagaimana mencegah serangan social engiineering ini.

SOCIAL ENGINEERING

Ada prinsip dalam dunia keamanan jaringan yang berbunyi "kekuatan sebuah rantai tergantung dari atau terletak pada sambungan yang terlemah" atau dalam bahasa asingnya "the strength of a chain depends on the

weakest link". Apa atau siapakah "the weakest link" atau "komponen terlemah" dalam sebuah sistem jaringan komputer? Ternyata jawabannya adalah: manusia. Walaupun sebuah sistem telah dilindungi dengan piranti keras dan piranti lunak canggih penangkal serangan seperti firewalls, anti virus, IDS/IPS, dan lain sebagainya – tetapi jika manusia yang mengoperasikannya lalai, maka keseluruhan peralatan itu tidaklah ada artinya. Para kriminal dunia maya paham betul akan hal ini sehingga kemudian mereka mulai menggunakan suatu kiat tertentu yang dinamakan sebagai "social engineering" untuk mendapatkan informasi penting dan krusial yang disimpan secara rahasia oleh manusia (Indrajit, 2016).

Social Engineering adalah suatu teknik pencurian data atau informasi penting dan berharga dari seseorang dengan menggunakan pendekatan interaksi sosial. Dengan kata lain social engineering adalah suatu teknik serangan yang mengeksploitasi kelemahan manusia (Indrajit, 2016). Contohnya kelemahan manusia yang dimaksud misalnya:

- Rasa Takut – jika seorang pegawai atau karyawan dimintai data atau informasi dari atasannya, polisi, atau penegak hukum yang lain, biasanya yang bersangkutan akan langsung memberikan tanpa merasa sungkan;
- Rasa Percaya – jika seorang individu dimintai data atau informasi dari teman baik, rekan sejawat, sanak saudara, atau sekretaris, biasanya yang bersangkutan akan langsung memberikannya tanpa harus merasa curiga; dan
- Rasa Ingin Menolong – jika seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam kesedihan yang mendalam, menjadi korban bencana, atau berada dalam duka, biasanya yang bersangkutan akan langsung memberikan data atau informasi yang diinginkan tanpa bertanya lebih dahulu.

Social Engineering terbagi menjadi dua, yaitu: berbasis interaksi sosial dan berbasis interaksi komputer. Pada jenis berbasis interaksi sosial, penyerang menggunakan teknik komunikasi yang sangat baik untuk menipu korbannya (Indrajit, 2016). Kemudian, pada jenis yang berbasis interaksi komputer penyerang biasanya menggunakan beberapa metode berikut (Sofana & Primartha, 2019):

- Phishing

Phishing merupakan jenis serangan dengan cara menyamar menjadi orang yang dapat dipercaya atau mewakili pihak tertentu untuk mendapatkan informasi penting dan berharga. Biasanya Phishing dilakukan pada tahap awal serangan untuk mendapatkan kredensial target. Contohnya:

- Banking Link Scam
- Fax Notice Scam
- Dropbox Link Scam
- Facebook Message Link Scam
- Court Secretary Complaint Link Scam

Teknik Phishing ini akan dijelaskan lebih detail pada bab selanjutnya.

- Malvertising

Metode penyerangan Malvertising ini merupakan jenis serangan yang cukup sulit untuk dideteksi karena dapat menyebar dan bekerja pada halaman web tanpa diketahui oleh korban. Cara penyebaran malware ini pun sangat unik, malware dapat tersebar tanpa perlu mengeksploitasi vulnerability dari suatu web atau web server dan bahkan tanpa campur tangan korban seperti mengklik tautan tertentu. Malvertising menggunakan jaringan iklan sebagai perantara dengan memasukkan script berbahaya kedalamnya yang kemudian akan menginfeksi website lain. (cyberthreat, 2020). Contoh dari malvertising adalah:

- Pop-up ads for deceptive downloads
- In-text or in-content advertising
- Web widgets redirection redirecting to a malicious site
- Hidden iframes that spread malware into websites

- Phone scams

Pada metode ini penyerang biasanya menelpon atau mengirim pesan kepada target dengan mengatasnamakan suatu instansi seperti bank untuk mendapatkan informasi penting dari korban.

Fakta menyebutkan, bahwa ada 4 (empat) kelompok di dalam organisasi yang menjadi target dari serangan Social Engineering, yaitu (Indrajit, 2016):

- Staff Helpdesk.
- Tim Technical Support dari divisi teknologi informasi.
- Administrator komputer
- Mitra kerja dari organisasi target
- Staff baru.

TEKNIK PENYERANGAN PHISHING

Phishing merupakan jenis serangan dengan cara menyamar menjadi orang yang dapat dipercaya atau mewakili pihak tertentu untuk mendapatkan informasi penting dan

berharga. Biasanya Phishing dilakukan pada tahap awal serangan untuk mendapatkan kredensial target (Indrajit, 2016). Contohnya situs palsu yang memiliki tampilan yang sama namun berbeda URL. Hacker kemudian memberikan link situs palsu ini kepada target agar login ke situs tersebut dengan menggunakan kredensialnya dan tanpa disadari ia telah mengirimkan username atau passwordnya kepada orang lain/hacker.

Dalam prakteknya metode Social Engineering ini lebih memanfaatkan pendekatan social untuk mengelabui targetnya, seperti mengirimkan SMS yang berisi penipuan bahwa akan mendapatkan hadiah, dana pinjaman, SMS dari Bank, dan lain sebagainya. Supaya lebih memahami mengenai teknik phishing, pada tulisan ini penulis akan melakukan percobaan serangan phishing yang digunakan untuk mencuri/harvesting username atau email dan password dari target dengan menggunakan Social engineering toolkit(SET) yang sudah tersedia dibeberapa distro linux pentest.

SOCIAL ENGINEERING TOOLKIT(SET)

Social Engineering Toolkit (SET) dibuat dan ditulis oleh Dave Kennedy, pendiri TrustedSec. SET merupakan tool pentest berbasis Python open-source yang ditujukan untuk social engineering. Tujuan dari SET adalah untuk mencuri kredensial atau dengan kata lain username/email dan password dari target (TrustedSec, 2019). SET menyediakan banyak fitur yang dapat digunakan dalam social engineering seperti cloning website, phishing, menangkap aktivitas desktop komputer target, dan masih banyak lagi. Tool ini support dengan sistem operasi linux dan mac os x (Trustedsec, 2020)dan biasanya sudah tersedia pada distro linux pentest seperti kali linux dan parrot os atau bisa didownload dari repository githubnya

https://github.com/trustedsec/social-engineer-toolkit .

PERCOBAAN

Pada percobaan ini penulis mencoba memperlihatkan bagaimana serangan phishing dapat dengan mudah dilakukan menggunakan SET untuk mencuri kredensial atau username/email dan password. Serangan phishing yang dilakukan adalah dengan meng-cloning suatu aplikasi website. Aplikasi hasil cloning tersebut kemudian digunakan oleh target yang login dengan username/email dan passwordnya. Jika

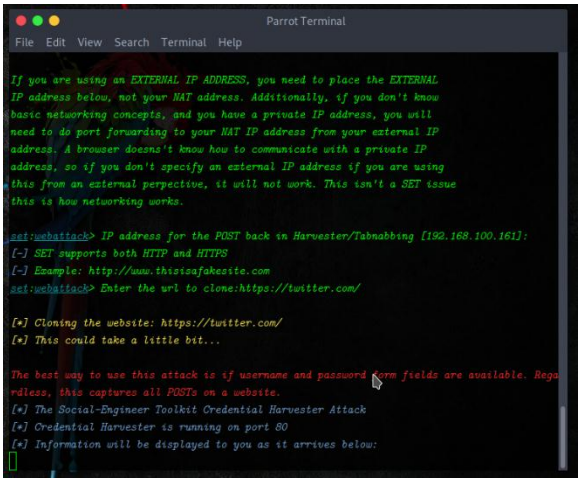
username dan password yang diisi oleh target valid, maka target akan diredirect ke situs asli tanpa menyadari bahwa ia telah mengirim kredensialnya kepada si penyerang.

Tools dan bahan yang digunakan pada percobaa ini adalah:

- Social Engineering Toolkit(SET) yang sudah ter-install pada distro Linux Parrot OS
- Twitter, Sebagai aplikasi yang akan di-cloning.
- Target

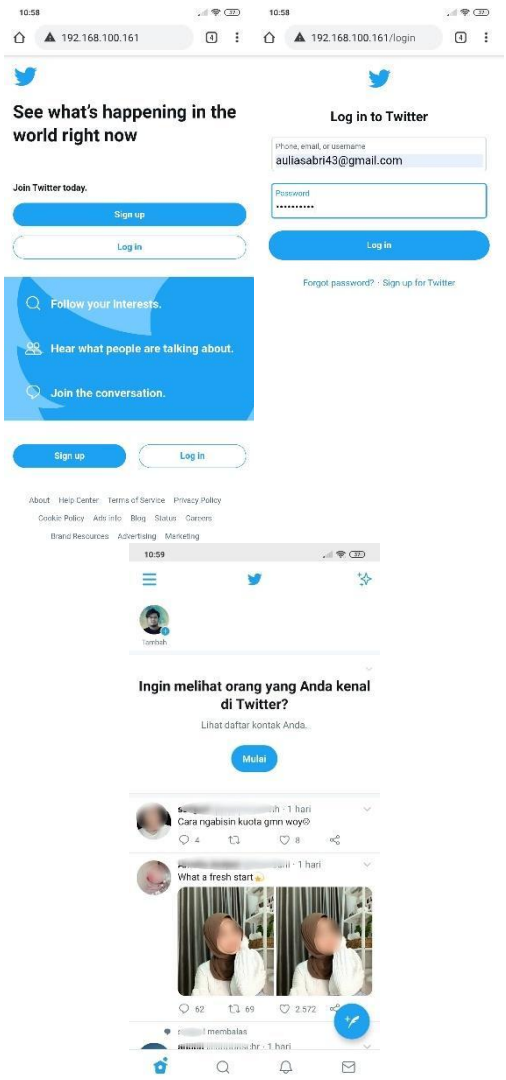
Langkah-langkah untuk melakukan serangan Phishing menggunakan SET adalah:

1. Jalankan SET dengan perintah: **sudo setoolkit**
2. Pilih menu: **social engineering attacks > website attack vectors > credential harvester attack method > site cloner**.
3. Masukkan IP host dan URL dari aplikasi yang akan di clone. Kemudian, SET akan mendengarkan setiap request yang terjadi.



Gambar 1. *Social Engineering Toolkit*

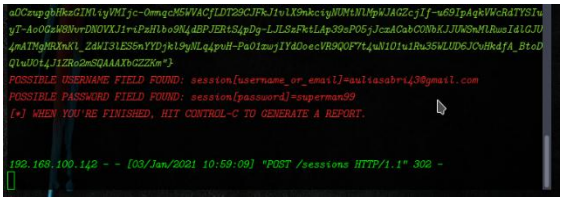
4. Bagikan IP atau link website hasil cloning ke target dan yakinkan target untuk mengklik link tersebut untuk login. Cara membagikan link pun berbagai macam, bisa melalui email, pesan, dan lewat media social lainnya.
5. Jika target telah membuka link yang dibagikan oleh penyerang kemudian login dengan username dan password yang valid, maka target akan diredirect ke situs asli tanpa menyadari bahwa ia telah mengirim kredensialnya kepada si penyerang.



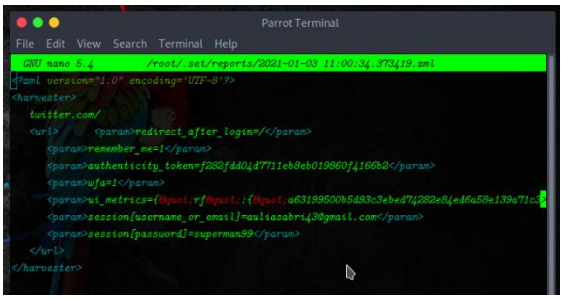
Gambar 2. *Target login twitter*

HASIL

Seperti yang dijelaskan pada langkah ke-5 kredensial target terlihat oleh penyerang jika target memasukkan kredensial yang valid dan target kemudian diredirect ke situs asli. Jika pada langkah ke-5 ini berhasil, maka penyerang bisa melihat langsung username/email dan password target pada log SET atau dengan perintah: **nano /root/.set/reports/[filename].xml**



Gambar 3. *Log report*



Gambar 4. *File report*

Pada gambar diatas terlihat informasi mengenai email: auliasabri43@gmail.com dan password: superman99.

KESIMPULAN

Social Engineering adalah suatu teknik pencurian data atau informasi penting dan berharga dari seseorang dengan menggunakan pendekatan interaksi sosial. Dengan kata lain social engineering adalah suatu teknik serangan yang mengeksploitasi kelemahan manusia. Social Engineering terbagi menjadi dua, yaitu: berbasis interaksi sosial dan berbasis interaksi komputer. Pada jenis berbasis interaksi sosial, penyerang menggunakan teknik komunikasi yang sangat baik untuk menipu korbannya. Kemudian, pada

jenis yang berbasis interaksi komputer penyerang biasanya menggunakan beberapa metode seperti Phishing, Malvertising, dan Phone scams. Pada zaman modernisasi ini sudah banyak tersedia berbagai tools untuk mendukung kegiatan social engineering dengan berbagai macam metode yang ada, contohnya seperti Social Engineering Toolkit(SET). Dengan demikian untuk mengatasi ancaman yang terkait dengan social engineering tidaklah mudah. Berikut ini beberapa cara untuk mengatasi ancaman yang terkait dengan social engineering:

- Password management
  Pengaturan dan policy penggunaan password, misal: jumlah karakter minimum, kombinasi karakter, jadwal penggantian password, perjanjian agar karyawan tidak membagikan password kepada orang lain.
- Two-factor authentication
  Penggunaan metode otentikasi lain selain password utama, misal: fingerprint, SMS sending, smart card.
- Antivirus/antiphishing defenses
  Penerapan multilayer antivirus untuk menangkal email phising dan berbagai jenis serangan social engineering.
- Change management
  Penerapan dokumen change management yang lebih secure dibandingkan sebelumnya(yang sudah ada).

DAFTAR PUSTAKA

cyberthreat, A. R. (2020, July 15). *Malvertising Marak Lagi, Ribuan Domain Tak Dipakai Dijual di Situs Lelang*. Diambil kembali dari cyberthreat.id: https://cyberthreat.id/read/7581/Malvertising-Marak-Lagi-Ribuan-Domain-Tak-Dipakai-Dijual-di-Situs-Lelang

Indrajit, P. R. (2016). *Keamanan Informasi dan Internet.* Yogyakarta: Preinexus.

Rafizan, O. (t.thn.). ANALISIS PENYERANGAN SOCIAL ENGINEERING.

Sofana, I., & Primartha, R. (2019). *Network Security dan Cyber Security.* Bandung: Informatika.

TrustedSec. (2019, September 27). *The Social-Engineer Toolkit (SET)*. Diambil kembali dari TrustedSec: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/

Trustedsec. (2020, Juni 9). *trustedsec/social-engineer-toolkit*. Diambil kembali dari GitHub: https://github.com/trustedsec/social-engineer-toolkit