LONTAR KOMPUTER VOL. 7, NO.2, AGUSTUS 2016 **p-ISSN 2088-1541**
DOI: 10.24843/LKJITI.2016.v07.i02.p04 **e-ISSN 2541-5832**

Pengujian Dan Analisa Anti Komputer Forensik Menggunakan Shred Tool

Budi Rahardjo[a1], I Putu Agus Eka Pratama[b2]

[a]Sekolah Teknik Elektro dan Informatika (STEI) Institut Teknologi Bandung
Jl Ganesha no 10, Bandung, Indonesia, telp.+62 222502260
[1]budi.rahardjo@paume.itb.ac.id

[b]Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Jalan Raya Kampus Unud, Bukit Jimbaran, Bali, Indonesia, telp. +62 3617853533
[2]eka.pratama@unud.ac.id

Abstrak

Komputer forensik dan anti komputer forensik adalah dua bidang yang saling berlawanan. Komputer forensik dilakukan oleh ahli komputer forensik guna memperoleh data dan bukti akurat dari kasus cyber crime untuk penyelidikan, sedangkan anti komputer forensik dilakukan oleh attacker untuk menghilangkan jejak sekaligus menyulitkan ahli komputer forensik dalam melakukan tugasnya. Bagi attacker, pemilihan tool anti komputer forensik yang default di mesin target, dinilai lebih efektif dan cepat dibandingkan menginstalasi terlebih dahulu di mesin korban. Untuk itu dipilihlah shred sebagai aplikasi anti komputer forensik pada mesin GNU/Linux. Jika anti forensik berhasil, ahli forensik akan sulit melakukan komputer forensik terhadap data yang menjadi barang bukti cyber crime. Paper ini memaparkan mengenai anti forensik yang dilakukan oleh attacker terhadap mesin remote GNU/Linux untuk kasus cyber crime di jaringan komputer. Anti forensik dilakukan menggunakan shred terhadap file syslog untuk menghapus jejak kejahatan sekaligus menyulitkan proses forensik oleh ahli komputer forensik. Pengujian dilakukan pada 3 buah komputer berbasis GNU/Linux pada intranet Lab Sinyal Sistem ITB. Masing - masing bertindak sebagai mesin target (server), mesin firewall, dan mesin attacker. Dilakukan proses anti komputer forensik dan komputer forensik di mesin server. Hasil pengujian dicatat dan dianalisa untuk kemudian ditarik kesimpulan.

Kata kunci: *Anti Forensik, Shred, GNU/Linux, Network*.

Abstract

Computer forensics and anti computer forensics are two opposing fields. Computer forensics is done by a computer forensics expert in order to obtain accurate data and evidence of cyber crime cases for investigation, while the anti-computer forensics conducted by the attacker to remove traces at once difficult computer forensics expert in performing its duties. For the attacker, the selection of anti-computer forensics tool that default on the target machine, more effective and faster than installing it first on the victim machine. For this reason the author chose shred as anti computer forensics applications on GNU / Linux machine. If anti forensic work, forensic experts would be difficult to perform computer forensics to data as evidence of cyber crime. This paper describes the anti-forensics performed by the attacker to remote machines GNU / Linux for cyber crime cases in a computer network. Anti forensic performed using shred the syslog file to remove traces of the crime at the same time make it difficult for the forensic process by computer forensics expert. Tests performed on three pieces of computer-based GNU / Linux on System Signals Lab intranet ITB. Each act as the target machine (server), firewall machine, and the machine attacker. Doing the anti computer forensics and computer forensics at the server machine. The test results are recorded and analyzed in order to then be deduced.

Keywords: *Anti Forensic, Shred, GNU/Linux, Network.*

1. Pendahuluan

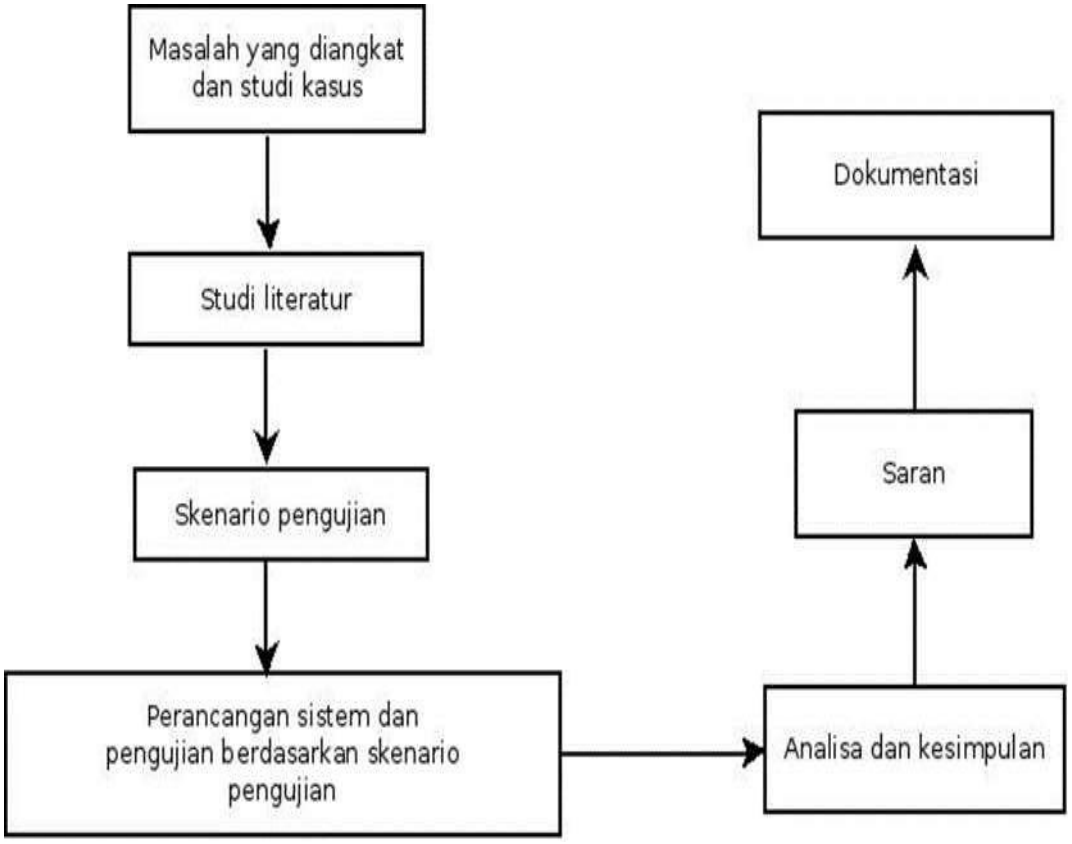
Sebagaimana halnya di dunia nyata, kejahatan di dunia komputer dan jaringan komputer, juga memerlukan adanya proses forensik. Ilmu ini disebut dengan komputer forensik, yang

memadukan antara elemen hukum dan *computer science*. Di sisi lain, pelaku kejahatan, dalam hal ini attacker, berusaha menutupi jejak kejahatannya dan menyulitkan proses komputer forensik. Ilmu ini dikenal sebagai anti komputer forensik. Komputer server pada umumnya menggunakan sistem operasi dari distribusi (distro) GNU/Linux atau basis UNIX lainnya (misal BSD, Solaris). Pada umumnya, setiap OS GNU/Linux telah dipaketkan dengan aplikasi shred, yang berguna untuk melakukan over write berulang - ulang terhadap isi suatu file atau folder, sehingga menyulitkan proses pembacaan file saat recovery. Oleh attacker, tool ini disalah gunakan untuk melakukan anti komputer forensik. Attacker cukup masuk ke mesin target dan menjalankan shred ke file atau direktori yang berpotensi menjadi barang bukti cyber crime (misal ke /var/log/syslog). Shred amat cepat dan mematikan dalam hal menghapus suatu jejak dan bukti kejahatan dunia maya. Di dalam paper ini, akan dijelaskan secara detail mengenai komputer forensik, anti komputer forensik, aplikasi shred, struktur file di GNU/Linux, dan penggunaan shred sebagai aplikasi anti komputer forensik. Sebelum dilakukan pengujian, dilakukan paper review terlebih dahulu, terhadap sejumlah referensi mengenai teknik - teknik pengujian anti forensik, yang telah dilakukan oleh Blunden [1], Perklin [2], Garfinkel [3], Sporea [4], Pajek [5], Mrshl [6], Peron [7], dan Stuttgen [8]. Dari referensi – referensi ini, dapat diketahui mengenai apa saja penelitian sebelumnya yang telah dilakukan (sebagai State of The Art) sekaligus menjadi pedoman di dalam penelitian ini. Selanjutnya,dilakukan proses pengujian di dalam penelitian ini, dengan menggunakan teknik pemanfaatan Shred Tool.

Selain itu, di dalam penelitian ini, juga dilakukan PoC (*Proof of Concept*) terhadap tiga buah komputer berbasis GNU/Linux, yang saling terhubung dalam suatu jaringan. Masing – masing komputer diposisikan sebagai komputer target (server), komputer firewall, dan komputer attacker. Selanjutnya, dilakukan proses anti komputer forensik menggunakan shred pada komputer korban (/var/log/syslog), secara remote melalui SSH. Langkah selanjutnya adalah melakukan proses komputer forensik terhadap file syslog. Parameter sukses tidaknya proses anti forensik yang dilakukan dilihat dari kemampuan untuk recovery file yang dihapus dengan shred maupun membaca kembali isi file hasil recovery tersebut. Untuk bisa menguasai komputer target, attacker memiliki rincian metode penyerangan, sedangkan sysadmin memiliki rincian metode bertahan. Keduanya menggunakan konsep 7 layer OSI. Penulis akan merinci langkah menyerang dan bertahan yang dilakukan oleh sysadmin dan attacker. Hasil pengujian dicatat, dianalisa, lalu ditarik kesimpulan. Dilanjutkan dengan pemberian saran untuk perbaikan ke depannya. Diharapkan melalui paper ini, diperoleh gambaran mengenai salah satu teknik anti forensik menggunakan shred di jaringan komputer, sekaligus meningkatkan kesadaran mengenai keamanan sistem bagi para Sysadmin.

2. Metodologi Penelitian

Perancangan skenario pengujian di dalam penelitian ini, menggunakan metodologi penelitian Design Science Research Method (DSRM) [9] yang terdiri atas tujuh langkah terurut. Meliputi pemilihan masalah yang diangkat dan studi kasus berdasarkan topik penelitian, studi literatur dari berbagai sumber referensi (paper, web) mengenai topik yang diangkat, menyusun skenario pengujian, perancangan sistem dan pengujian sistem berdasarkan skenario yang dibuat, analisa dan kesimpulan, penyajian saran, serta dokumentasi. Gambar di bawah ini, menunjukkan bagan dari metodologi penelitian yang digunakan.



Gambar 1. Alur untuk metodologi penelitian

Selain itu, di dalam penelitian ini, juga digunakan metodologi Systematic Literature Review (SLR) [10], untuk membantu di dalam melakukan paper review terhadap sejumlah referensi, terkait dengan penelitian yang telah dilakukan sebelumnya oleh para peneliti sebelumnya tersebut.

2.1. Skenario Pengujian

Urutan skenario pengujian yang digunakan di dalam penelitian ini, yaitu sebagai berikut (dengan aktor terdiri dari Attacker, Sysadmin, dan ahli forensik) :

a. Attacker menguasai mesin target, namun lupa menghapus jejak di file syslog.
b. Sysadmin melakukan pengamanan pada 7 layer OSI untuk mencegah terulangnya kembali penyerangan tersebut.
c. Attacker mencoba menguasai kembali mesin target, agar dapat melakukan anti forensik terhadap file syslog. Attacker memanfaatkan shred yang terdapat secara default di mesin target.
d. Sysadmin meminta bantuan ahli forensik untuk melakukan forensik ke mesin target setelah attacker melakukan anti forensik pada file syslog. Di dalam skenario pengujian pada penelitian ini, diuji coba sebagai sysadmin, attacker, dan ahli forensik, menggunakan 2 buah komputer GNU/Linux Ubuntu 9.10 dan 1 buah notebook GNU/Linux Ubuntu 9.04 di jaringan Lab Sinyal Sistem (LSS) ITB.

2.2. Kebutuhan *Hardware* Dan *Software*

Untuk mendukung jalannya penelitian ini, dibutuhkan adanya sejumlah perangkat keras komputer (*Hardware*) dan perangkat lunak komputer (*Software*) yang akan diujikan. Adapun *Hardware* dan *Software* yang dibutuhkan di dalam penelitian ini, antara lain sebagai berikut :

1. Untuk mesin attacker, digunakan sebuah notebook Toshiba M300, dengan spesifikasi : Intel P8400, VGA ATI Radeon, RAM 1024 MB, wifi, dan LAN Card. *Software* yang digunakan d dalamnya berupa: sistem operasi GNU/Linux Ubuntu 9.04, Shred, Terminal, rm, Open SSH Server dan Open SSH Client. Untuk mesin server dan mesin firewall,

masing – masing menggunakan sebuah komputer dengan spesifikasi: Intel Pentium 5, RAM 512 MB, VGA Onboard Intel, dan LAN Card. *Software* yang digunakan pada masing – masing komputer ini berupa sistem operasi GNU/Linux Ubuntu 9.10, OpenSSH Server, Open SSH Client, terminal, rm, dan Shred.

2. Untuk media jaringan komputer, digunakan intranet ITB di Lab Sinyal System (LSS) ITB. Mesin attacker menggunakan media wireless, sedangkan mesin server dan mesin firewall menggunakan media wired pada switch 16 port. Pengalamatan yang digunakan untuk semua komputer adalah secara statis. Rincian pengalamatan (IP Address) disampaikan pada point 4,5, dan 6.
3. Untuk pengalamatan pada mesin attacker, digunakan IPV4 167.205.16.119, BCast 167.205.16.255, Subnet Mask 255.255.255.0, dan Gateway 167.205.67.65. Untuk pengalamatan pada mesin server (target), digunakan IPV4 167.205.67.78, Bcast 167.205.67.127, Subnet Mask 255.255.255.192, dan Gateway 167.205.67.65. Untuk pengalamatan pada mesin firewall, digunakan IPV4 167.205.67.107, Bcast 167.205.67.127, Subnet Mask 255.255.255.192, dan Gateway 167.205.67.65.
4. Semua komputer menggunakan perangkat mouse, keyboard, dan LCD monitor standar.
5. Proses dokumentasi di dalam penelitian ini, menggunakan aplikasi Open Source berupa Open Office Writer 3.0 dan Lyx GUI LATEX 1.6.2. Sedangkan untuk desain bagan sistem, mengggunakan aplikasi Open Source berupa DIA Diagram 0.96.1.

3.1. Kajian Pustaka

3.2. Struktur File System Di GNU/Linux

Filesystem adalah metode dan struktur data yang digunakan oleh sistem operasi untuk menjaga track suatu file pada disk atau partisi dan merupakan cara untuk mengorganisasikan file pada disk[11]. GNU/Linux memiliki banyak jenis filesystem, namun yang terkenal adalah ext (terutamanya ext4 [12]) dan reiserfs. File sistem di GNU/Linux ada yang bersifat journaling (ext4, ext3, reiserfs) maupun tidak. Sebagaimana filesystem lainnya di OS berbasis UNIX lainnya, GNU/Linux memiliki struktur direktori hirarki tunggal yang diawali dengan root (dilambangkan dengan /). Di dalam root terdapat sub direktori dengan fungsi masing - masing. Untuk mengetahui semua sub direktori pada sistem operasi GNU/Linux Ubuntu 9.04, digunakan perintah berikut ini :

```
root@my-machine:/# ls -la total 108
drwxr-xr-x 2 root root 4096 2010-08-02 08:33 bin
drwxr-xr-x 3 root root 4096 2010-08-02 08:34 boot
drwxr-xr-x 17 root root 4320 2011-04-06 17:10 dev drwxr-xr-
x 168 root root 12288 2011-04-06 17:08 etc drwxr-xr-x 5
root root 4096 2010-08-02 17:19 home
lrwxrwxrwx   1   root   root   33   2010-05-30   01:33
initrd.img   -> boot/initrd.img-2.6.28-11-generic
drwxr-xr-x 21 root root 4096 2010-11-13 12:11 lib
drwx------ 2 root root 16384 2010-05-30 01:19 lost+found
drwxr-xr-x 3 root root 4096 2011-04-06 17:08 media drwxr-
xr-x 2 root root 4096 2009-04-13 16:33 mnt drwxr-xr-x 4
root root 4096 2010-07-21 12:13 opt
dr-xr-xr-x 172  root  root 0 2011-04-06 11:01 proc drwx----
-- 22  root  root 4096  2011-04-02 15:18 root drwxr-xr-x 2
root root 4096 2010-08-02 08:33 sbin drwxr-xr-x 3 root root
4096 2010-05-30 22:01 srv drwxrwxrwt 18 root root 4096
2011-04-06 17:47 tmp drwxr-xr-x 14  root root 4096 2010-05-
30 22:58 usr drwxr-xr-x 16 root root 4096 2010-07-14 13:11
var
```

Sub direktori yang penting dalam root yaitu */bin, /boot, /dev, /etc, /home, /initrd, /lib, /lost+found,*

/media, /mnt, /opt, /proc, /root, /sbin, /usr, /var, /srv, dan */tmp*. Penulis hanya membahas 2 saja yaitu /home dan /var, sesuai dengan cakupan paper ini. /home adalah rumah untuk setiap user. GNU/Linux dan OS berbasis UNIX lainnya adalah sistem operasi multi user environment, sehingga setiap user memiliki /home masing - masing dengan semua privillege (rea d, write, delete, dan sebagainya). Misalkan user putu-shinoda dengan lokasi /home/putu-shinoda. /var berisi variabel data berupa system logging files, mail, printer spool directories, serta transient dan temporary file. Untuk mengetahuii isi dari sub direktori /var, digunakan perintah berikut :

```
root@my-machine:/home/putu-shinoda# cd /var root@my-machine:/var# ls -la
total 56
drwxr-xr-x 18 root root  4096 2011-04-06 11:08 log
drwxrwsr-x  2 root mail  4096 2009-04-20 20:59 mail
drwxr-xr-x  2 root root  4096 2009-04-20 20:59 opt drwxr-xr-x 21 root root   800 2011-04-06 18:10 run drwxrwxrwt  4 root root  4096 2011-04-05 19:50 tmp drwxrwxrwx 19 root root  4096 2011-02-23 11:56 www
```

Salah satu bagian yang terpenting adalah */var/log/syslog,* yang merupakan tempat sistem mengirimkan log. Untuk mengecek log, dapat dilakukan secara real time dengan menggunakan perintah *tail -f /var/log/syslog*. Pada paper ini, anti forensik dilakukan di file syslog. Pada Linux dan OS basis UNIX lainnya, setiap file dan direktori memiliki info index node (inode), termasuk juga status dari file atau direktori tersebut. Hal ini sangat penting pada saat forensik, untuk mengetahui keadaan suatu file. Termasuk juga dalam hal ini proses *recovery,* jika yang terhapus adalah nomor inode itu (bukan isi file maupun file secara keseluruhan).

Inode merupakan alamat dari sebuah blok disk. Informasi dari suatu inode dapat dilihat dengan mengetikkan perintah ls dan stat. Perintah ls akan menampilkan alamat pertama suatu file. Suatu file memiliki format dan struktur berupa nama, konten, dan informasi administratif (permission, waktu modifikasi). Informasi administratif ini disimpan di inode beserta data lainnya. Terdapat tiga kali penyimpanan di inode, yaitu saat konten terakhir kali dimodifikasi (written), terakhir kali digunakan (read, executed), dan perubahan pada inode itu sendiri (saat mengeset permission). Nomor inode dan keterangan yang lebih lengkap dapat dilihat dengan mengetikkan perintah stat nama_file.

Untuk lebih memahami tentang inode, maka perlu dilakukan sebuah pengujian sederhana (sebelum pengujian utama di dalam paper ini). Berikut merupakan langkah pengujian yang dilakukan pada sistem operasi GNU/Linux Ubuntu 9.04. Pertama – tama, dibuat sebuah file teks bernama manual.txt dengan menggunakan perintah berikut :

```
putu-shinoda@my-machine:~$ touch manual.txt
```

Selanjutnya, dilakukan proses pengecekan keberadaan file manual.txt yang telah dibuat tersebut, dengan menggunakan perintah berikut :

```
putu-shinoda@my-machine:~$ ls -l manual.txt
-rw-r--r-- 1 putu-shinoda putu-shinoda 0 2011-04-16 00:20 manual.txt
```

Langkah selanjutnya adalah melihat inode dari file manual.txt yang telah dibuat, dengan menggunakan perintah berikut :

```
putu-shinoda@my-machine:~$ ls -i manual.txt 3691951 manual.txt
```

Selanjutnya, dilakukan proses penggalian keseluruhan informasi dari file tersebut, dengan menggunakan perintah berikut ini :

```
putu-shinoda@my-machine:~$ stat manual.txt
File: `manual.txt'
```

```
Size: 0   Blocks: 0   IO Block: 4096   file kosong biasa
Device: 801h/2049d  Inode: 3691951   Links: 1
Access:   (0644/-rw-r--r--)     Uid:   (   1000/putu-shinoda)
Gid:   (
1000/putu-shinoda)
Access: 2011-04-16 00:20:31.000000000 +0700
Modify: 2011-04-16 00:20:31.000000000 +0700
Change: 2011-04-16 00:20:31.000000000 +0700
```

Setelah pengujian dilakukan terhadap suatu berkas file baru, kemudian dicoba untuk dilakukan pengujian serupa pada direktori dan sub direktori. Untuk itu dibuatlah sebuah direktori baru bernama berkas, untuk kemudian digali informasi inode dan informasi keseluruhan dari folder tersebut, dengan menggunakan perintah berikut :

```
putu-shinoda@my-machine:~$ mkdir kotak putu-shinoda@my-
machine:~$ ls -di kotak/ 9947429 kotak/
putu-shinoda@my-machine:~$ stat kotak/
File: `kotak/'
Size: 4096    Blocks: 8    IO Block: 4096   direktori
Device: 801h/2049d      Inode: 9947429     Links: 2
Access:   (0755/drwxr-xr-x)     Uid:   (   1000/putu-shinoda)
Gid:   (
1000/putu-shinoda)
Access: 2011-04-16 00:22:26.000000000 +0700
Modify: 2011-04-16 00:22:16.000000000 +0700
Change: 2011-04-16 00:22:16.000000000 +0700
```

Dari kedua buah pengujian yang telah dilakukan di atas (untuk berkas file dan folder), dapat diperoleh informasi mengenai nilai inode masing – masing. File manual.txt dan folder bernama kotak, masing – masing memiliki nilai inode 3691951 dan 9947429.

3.3. Komputer Forensik

Menurut CERT di dalam dokumentasinya [13], disebutkan bahwa komputer forensik adalah ilmu yang menggabungkan hukum dan computer science untuk mengumpulkan dan menganalisa data dari sistem komputer, jaringan, wireless communications, dan media penyimpanan, untuk dijadikan barang bukti di pengadilan untuk kasus cyber crime. Integritas dan stabilitas infrastruktur jaringan dapat tetap terjaga dengan adanya komputer forensik. Dengan pengetahuan mengenai hukum dan teknis komputer forensik, capture informasi penting dapat dengan mudah dilakukan di jaringan saat compromize terjadi. Hal ini akan memudahkan menuntut pelaku cyber crime yang tertangkap secara hukum. Keuangan perusahaan juga dapat dihemat dari anggaran untuk menyewa jasa computer security jika setiap staf perusahaan paham dan tanggap mengenai komputer forensik.

3.4. Anti Komputer Forensik

Berlawanan dengan komputer forensik, anti komputer forensik adalah ilmu yang memadukan berbagai teknik untuk menyulitkan proses komputer forensik. Awal mulanya ilmu ini dibentuk sebagai bagian dari proses riset dan pembelajaran komputer forensik yang sedang dikembangkan saat itu. Sayangnya ilmu ini justru disalah gunakan oleh oknum yang tidak bertanggung jawab untuk menghilangkan jejak dalam kasus cyber crime.

Dalam dunia komputer, bukti digital adalah berkas berupa kumpulan data elektronik. Seorang attacker berusaha menyulitkan pekerjaan ahli forensik dalam mengidentifikasi, mengumpulkan, memeriksa, atau melakukan validasi terhadap bukti digital dengan cara menghancurkan, menyembunyikan, memanipulasi, atau mencegah ditemukannya bukti adanya suatu cyber crime. Hal ini dilakukan oleh attacker untuk menghapus jejaknya agar terhindar dari tuntutan hukum. Ada banyak tool yang bisa digunakan untuk melakukan anti forensik. Salah satunya adalah shred, yang ada secara default di setiap distribusi GNU/Linux.

4. Hasil Dan Pembahasan

4.1. Penguasaan Kembali Mesin Target

Sesuai skenario, asumsi, dan batasan masalah yang telah dikemukakan, terdapat proses bertahan dan menyerang yang dilakukan oleh pemilik sistem (sysadmin) dan attacker. Teknikal mengenai prinsip menyerang dan bertahan ini, telah diteliti sebelumnya oleh Pseudoanonymous [14], Jianxin [15], Kapoor [16], dan Ganggan [17]. Sysadmin menerapkan pola pengamanan pada 7 OSI Layer, untuk melindungi mesin dan jaringannya dari serangan attacker. Yaitu sebagai berikut :

a. Pada Physical Layer, pengamanan secara fisik pada mesin dan *Hardware* pendukungnya sesuai ISO 27001/2 mengenai keamanan fisik (physical security).
b. Pada Data Link Layer, pengamanan terhadap intranet menggunakan IPS/NIPS.
c. Pada Network Layer, dilakukan pemasangan firewall, memperbolehkan akses dari IP Address dan Mac Address tertentu saja.
d. Pada Transport Layer, menggunakan IDS (Instrusion Detection System) dan IPS/NIPS.
e. Pada Session Layer, menggunakan VPN dial up dan IPS/NI
f. Pada Presentation Layer, menggunakan SSL dan IPS/NIPS.
g. Pada Application Layer, menggunakan Deny Host pada akses SSH (Preventing SSH Dictionary Attack) dan IPS/NIPS.

Selain pengamanan pada ketujuh layer OSI tersebut, dilakukan juga patch dan update terhadap sistem. Untuk topologi jaringannya, sysadmin meletakkan sebuah mesin firewall di depan mesin server, sehingga mesin server hanya bisa terhubung keluar melalui mesin firewall saja. Attacker melakukan penetration testing untuk pemetaan akses setiap layer, termasuk menguasai mesin firewall agar bisa mengakses mesin server. Beberapa cara yang dilakukannya unuk setiap layer, antara lain adalah:

a. Pada Physical Layer: Social engineering untuk memperoleh akses fisik ke sistem untuk kendali sistem.
b. Pada Data Link Layer: ARP Cache Poisoning MITM, Content Adressable Memory Table Flooding MITM, VLAN Hoping Attack Double Tagging, VLAN Trunking Protocol Attack, Rapid Spanning Tree Protocol Attack.
c. Pada Network Layer: IP Spoofing Attack, IP Fragmentation Aattack, ICMP Smurfing Denial Of Service, BGP Internet Scale MITM, BGP Network Layer Reachability Information Injection Route Poisoning, Label Distribution Protocol Injection Overwrite MPLS Label, GRE Traffic Tunneling MITM, IPSEC Vulnerability Attack.
d. Pada Transport Layer: SYN Flooding, IP Spoofing, DoS/DdoS, ACK Flooding, UDP Flooding, SYN/ACK Scanning Service, SCTP Scanning Enumerated SS7/SIGTRAN.
e. Pada Session Layer: L2TP Attack, DoS Attack , Replay Attack, NetBIOS User Enumeration.
f. Pada Presentation Layer: SSL MITM Attack.
g. Pada Application Layer: Kaminsky Attack DNS Poisoning, HTTP Slowris DoS Attack, DNS Amplification Attack, SNMPv3 HMAC authentication Bypass, SSH Ncrack, SNMP Guessing Brute Force Attack.

Setelah memperoleh kembali akses root di mesin firewall dan mesin server, Attacker segera melakukan anti forensik pada file syslog guna menghapus jejak sekaligus menyulitkan kerja ahli forensik. Pertama – tama, Attacker melakukan remote SSH ke mesin firewall dengan menggunakan perintah berikut ini :

```
root@my-machine:/home/putu-shinoda#          ssh
lsslantai3- machine2@167.205.67.107
lsslantai3-machine2@167.205.67.107's password:
Linux lsslantai3-machine2 2.6.31-14-generic #48-Ubuntu SMP
Fri Oct 16
14:04:26 UTC 2009 i686
lsslantai3-machine2@lsslantai3-machine2:~$
```

Selanjutnya, dari mesin firewall, Attacker melanjutkan proses koneksi SSH ke mesin target (server). Untuk itu, Attacker menggunakan perintah berikut ini :

```
lsslantai3-machine2@lsslantai3-machine2:~$ ssh
lsslantai3- machine1@167.205.67.78 The authenticity of
host '167.205.67.78 (167.205.67.78)' can't be
established.
RSA key fingerprint
is f8:f7:64:b8:9c:b8:bb:cb:38:c2:90:36:ae:a7:86:72.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '167.205.67.78' (RSA) to the
list of known hosts.
lsslantai3-machine1@167.205.67.78's password:
Linux lsslantai3-machine1 2.6.31-14-generic #48-Ubuntu SMP
Fri Oct 16
14:04:26 UTC 2009 i686
lsslantai3-machine1@lsslantai3-machine1:~$
```

Setelah Attacker masuk ke mesin target, selanjutnya Attacker mencoba mengecek file syslog yang menjadi target untuk anti forensik. Attacker menggunakan perintah berikut untuk melakukan pengecekan :

```
lsslantai3-machine1@lsslantai3-machine1:~$ tail -f
/var/log/syslog
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.210155] CPU1
attaching
NULL sched-domain.
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224075] CPU0
attaching
sched-domain:
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224080]
domain 0: span
0-1 level MC
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224084]
groups:01
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224090] CPU1
attaching
sched-domain:
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224093]
domain 0: span
0-1 level MC
Apr 27 12:42:40 lsslantai3-machine1 kernel: [13.224095]
groups:10
Apr 27 12:42:43 lsslantai3-machine1 kernel: [15.688006]
eth0: no IPv6
routers present
lsslantai3-machine1@lsslantai3-machine1:~$
```

Setelah perintah dijalankan, komputer target akan menampilkan informasi. Attacker kemudian mencari tahu nilai inode dari file syslog. Untuk itu, Attacker menggunakan perintah berikut :

```
lsslantai3-machine1@lsslantai3-machine1:~$ stat
/var/log/syslog
File: `/var/log/syslog'
Size: 252306 Blocks: 496 IO Block: 4096 regular file
Device: 805h/2053d Inode: 125 Links: 1
Access: (0640/-rw-r-----) Uid: (101/syslog) Gid: (4/ adm)
Access: 2011-04-27 13:12:24.127224088 +0700
Modify: 2011-04-27 13:17:01.226597858 +0700
Change: 2011-04-27 13:17:01.226597858 +0700
lsslantai3-machine1@lsslantai3-machine1:~$
```

Informasi yang dihasilkan oleh perintah di atas, adalah nilai inode file syslog, yaitu125. Berdasarkan kepada informasi inode tersebut, Attacker kemudian menjadi root di mesin server, untuk kemudian melakukan anti forensik menggunakan shred ke file syslog, memanfaatkan perintah berikut:

```
lsslantai3-machine1@lsslantai3-machine1:~$ sudo su
[sudo] password for lsslantai3-machine1:
root@lsslantai3-machine1:/home/lsslantai3-machine1# shred -
-random- source=/dev/urandom -u /var/log/syslog
root@lsslantai3-machine1:/home/lsslantai3-machine1#
```

Attacker berusaha memastikan dan mengecek, apakah file syslog benar – benar telah terhapus. Hal ini bertujuan untuk menyulitkan ahli forensik saat dilakukan proses forensik. Untuk itu, Attacker menggunakan perintah berikut:

```
root@lsslantai3-machine1:/home/lsslantai3-machine1# ls -la
/var/log/syslog
ls: cannot access /var/log/syslog: No such file or directory
root@lsslantai3-machine1:/home/lsslantai3-machine1# stat
syslog stat: cannot stat `syslog': No such file or
directory root@lsslantai3-machine1:/home/lsslantai3-
machine1#
```

Dari keluaran perintah di atas, terlihat bahwa file syslog sudah terhapus dengan aman.

4.2. Komputer Forensik Di Komputer Target Oleh Attacker

Setelah proses anti forensik dilakukan, Attacker mencoba mengembalikan *(recovery)* file syslog menggunakan lsof, tool recovery di GNU/Linux. Hal ini dilakukan untuk menguji apakah anti forensik yang dilakukan telah berjalan dengan baik atau tidak. Berbekal info nilai inode filesyslog di mesin server yaitu 125, proses pemetaan path pun dilakukan oleh attacker, dengan menggunakan perintah berikut :

```
root@lsslantai3-machine1:/home/lsslantai3-machine1# lsof |
grep 125 rsyslogd 489 syslog 5w REG 8,5 0 125
/var/log/0 (deleted) root@lsslantai3-
machine1:/home/lsslantai3-machine1#
```

Dari perintah di atas, diperoleh info nilai inode 125, PID (Process ID) 489, dan file descriptor 5 (dari 5w). Informasi ini diperlukan pada proses recovery file syslog. Kemudian attacker mencoba melakukan recovery dengan mengkopi kembali syslog dari lokasi pseudo-filesystem.

```
root@lsslantai3-machine1:/home/lsslantai3-machine1# cp
/proc/489/fd/5 syslog
```

Selanjutnya, Attacker melakukan pengecekan, apakah file syslog bisa terbaca setelah proses recovery tersebut, dengan menggunakan perintah berikut :

```
root@lsslantai3-machine1:/home/lsslantai3-machine1# tail -f
/var/log/syslog
tail: cannot open `/var/log/syslog' for reading: No such
file or directory
tail: no files remaining
root@lsslantai3-machine1:/home/lsslantai3-machine1# tail -f
syslog
root@lsslantai3-machine1:/home/lsslantai3-machine1# file
syslog syslog: empty
```

Dari perintah di atas, terlihat informasi di mana file tidak dapat dibaca. Selanjutnya, Attacker melakukan proses pengecekan penghapusan dengan menggunakan pemetaan path sebagai berikut ini :

```
root@lsslantai3-machine1:/var/log# ls -l /proc/489/fd/5
l-wx------ 1 root root 64 2011-04-27 13:23
/proc/489/fd/5 ->
```

```
/var/log/0 (deleted)
```

Berdasarkan kepada perintah yang dijalankan tersebut, diperoleh informasi bahwa info penghapusan file syslog tanggal 27 april 2011 pkl 13.23. Selanjutnya dilanjutkan pengecekan status file syslog dari /proc.

```
–machine1:/var/log# file /proc/489 root@lsslantai3/fd/5
/proc/489/fd/5: broken symbolic link to `/var/log/0
(deleted)'
```

Attacker kemudian mengecek isi di dalam file syslog, dengan menggunakan perintah berikut :

```
root@lsslantai3-machine1:/var/log# tail -f /var/log/syslog
root@lsslantai3-machine1:/var/log# file /var/log/syslog
syslog: empty
```

Dari perintah di atas, terlihat informasi bahwa file syslog hasil recovery isinya telah kosong. Hal ini menandakan bahwa proses anti forensik telah berjalan dengan sukses. Attacker kemudian keluar dari mesin remote (mesin server dan mesin firewall). Sesuai dengan skenario pengujian, sampai di sini, attacker telah berhasil melakukan proses anti forensik dengan baik.

4.3. Komputer Forensic Di Komputer Target Oleh Ahli Forensic

Melanjutkan skenario pengujian, kemudian Syadmin yang menyadari mesinnya dikuasai kembali oleh Attacker, akhirnya memanggil ahli forensik. Ahli forensik mencoba melakukan proses forensik seperti yang dilakukan oleh attacker di atas, namun tidak berhasil, karena file syslog yang ada isinya kosong sehingga tidak dapat dibaca. Berikut adalah perintah yang dijalankan oleh ahli forensik, beserta dengan informasi yang ditampilkan (mengenai kegagalan proses forensik) :

```
root@lsslantai3-machine1:/var/log# tail -f /var/log/syslog
root@lsslantai3-machine1:/var/log# file /var/log/syslog
syslog: empt
```

5. Kesimpulan

Berdasarkan kepada pemaparan praktek pengujian anti forensik yang telah disampaikan di atas dengan menggunakan shred oleh attacker, dapat dilihat bahwa proses anti forensik berjalan dengan baik. File syslog terhapus dengan aman. Meski Attacker telah mencoba melakukan *recovery* file syslog, namun isi di dalamnya kosong atau tidak bisa dibaca. Hal ini akan menyulitkan ahli forensik di dalam melakukan proses komputer forensik.

Dari hasil pengujian dan analisa yang telah dilakukan, dapat disimpulkan bahwa dengan menggunakan shred, bukti forensik dapat dihapus dengan aman dan sulit untuk dikembalikan. Bahkan jika dilakukan recovery, isi di dalamnya kosong atau tidak dapat dibaca. Hal ini menjadi parameter kesuksesan proses anti forensik. Terbukti bahwa shred merupakan salah satu tool anti forensik yang ampuh dan praktis untuk digunakan, karena sudah ada di setiap mesin GNU/Linux secara default. Pengujian sederhana ini, sekaligus menjadi peringatan bagi Sysadmin, untuk menggunakan Shred Tool dengan bijak, agar tidak disalah gunakan oleh Attacker.

Daftar Pustaka

[1] B. Blunden, “Anti Forensic : The Rootkit Connection,” 2009.
[2] M. Perklin, “Anti Forensic And Anti Anti Forensic,” 2011.
[3] S. Garfinkel, “Anti-Forensics : Techniques, Detection and Countermeasures,” in *2nd International Conference on i-Warfare and Security*, 2012.
[4] I. Sporea, “On the Availability of Anti-Forensic Tools for Smartphones,” *International Journal of Security (IJS),* vol. 6, no. 4, pp. 58-64, 2012.
[5] Pajek, P., “Computer Anti Forensics Methods And Their Impact On Computer Forensic Investigation,” University of East London, United Kingdom, 2009.
[6] J. Mrshl, “Anti Forensic Seek And Destroy,” *Echo Community*, 2010.

[7] C. S. J. Peron and M. Legary, "Digital Anti-Forensics : Emerging Trends in Data Transformation Techniques," *Seccuris Labs*, 2011.
[8] J. Stuttgen, *Anti Forensic Resilient Memory Acquisition*. Elsevier Digital, 2013.
[9] C. Armstrong, "Modelling Forensic Evidence System Using Design Science," Curtin University of Technology Bentley, WA, Australia., 2010.
[10] G. Cairns, "Systematic Literature Review Of The Evidence For Effective National Immunisation Schedule Promotional Communications," *ECDC Stock.*, 2012.
[11] B. Nguyen, "Linux Filesystem Hierarchy," 2011.
[12] A. Mathur, M. Cao, S. Bhattacarrya, A. Dilger, A. Tomas, and L. Vivier, "The New Ext4 Filesystem : Current Status and Future Plan," 2011.
[13]CERT, "Computer Forensics," USA, 2011.
[14] Pseudoanonymous, "Network Hack Philosopy," *Kecoak Elektronik*, 2010.
[15] J. Y. Jianxin, "Denial Of Service : Another Example," 2011.
[16] S. Kapoor, "Session Hijacking : Exploiting TCP, UDP, and HTTP Sessions," 2011.
[17] S. Ganggan, "The Review Of Man In The Middle Attack."