

DAFTAR ISI

HALAMAN SAMBUTAN	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PENSAHAN	iv
HALAMAN PERNYATAAN KEASLIAN	v
HALAMAN PERSEMBAHAN	vi
HALAMAN MOTTO	viii
KATA PENGANTAR	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR	xiv
DAFTAR ISTILAH	xvi
DAFTAR LAMPIRAN.....	xvii
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I PENDAHULUAN	
A. Latar Belakang Masalah	1
B. Rumusan Masalah.....	6
C. Batasan Masalah	6
D. Tujuan Penelitian	7
E. Manfaat Penelitian	7
BAB II TINJAUAN PUSTAKA	
A. Landasan Teori.....	9
B. Penelitian Sebelumnya.....	18
BAB III METODE PENELITIAN	
A. Waktu Penelitian.....	25
B. Metode Pengumpulan Data.....	25
C. Alat dan Bahan Penelitian.....	26
D. Konsep Penelitian	28

BAB IV HASIL DAN PEMBAHASAN

<i>A. Collection</i>	35
<i>B. Examination</i>	39
<i>C. Analysis</i>	46
<i>D. Reporting</i>	61

BAB V PENUTUP

<i>A. Kesimpulan</i>	66
<i>B. Saran</i>	67

DAFTAR PUSTAKA

LAMPIRAN



DAFTAR TABEL

Tabel 2. 1 Penelitian Sebelumnya.....	23
Tabel 4. 1 Terminal Linux	39



DAFTAR GAMBAR

Gambar 2. 1 Arsitektur OS Linux	17
Gambar 2. 2 Struktur sistem operasi Linux	18
Gambar 3. 1 Kerangka Berpikir.....	28
Gambar 3. 2 Skenario Serangan.....	30
Gambar 3. 3 Tahapan-tahapan NIST	32
Gambar 4. 1 Virtual Machine Box.....	35
Gambar 4. 2 Nilai Hash.....	36
Gambar 4. 3 Instalasi OVA.....	36
Gambar 4. 4 Konfigurasi Virtual Machine 1	37
Gambar 4. 5 Start Virtual Machine	38
Gambar 4. 6 Proses booting	38
Gambar 4. 7 Output Date	40
Gambar 4. 8 Output hostnamectl	41
Gambar 4. 9 Output netstat -lntu.....	42
Gambar 4. 10 Output ip a.....	43
Gambar 4. 11 Output hostnamectl	44
Gambar 4. 12 Output cat/etc/passwd	45
Gambar 4. 13 Output etc/passwd	45
Gambar 4. 14 Output cat/etc/passwd	47
Gambar 4. 15 Output /etc/passwd.....	48
Gambar 4. 16 User ID	49
Gambar 4. 17 Output ls /var/log/cron*	50
Gambar 4. 18 Output var/log/cron	51
Gambar 4. 19 Output log cron-20230503	51
Gambar 4. 20 Output file cron-20230517	52
Gambar 4. 21 Output root/Keylogger/linux	53
Gambar 4. 22 Output log secure-20230517	54
Gambar 4. 23 Output log secure-20230517	55
Gambar 4. 24. Output log secure-20230517	55

Gambar 4. 25 Output log secure-20230517	56
Gambar 4. 26 Output mac-robber /mnt/company/	56
Gambar 4. 27 Output /etc/firewalld/zones	57
Gambar 4. 28 Output mtime.....	58
Gambar 4. 29 public.xml.....	58
Gambar 4. 30 Output crontab -l	60



DAFTAR ISTILAH

Keylogger: Perangkat lunak atau perangkat keras yang merekam setiap *keystroke* yang dilakukan pada komputer atau perangkat lain.

NIST: *National Institute of Standards and Technology*, lembaga pemerintah Amerika Serikat yang mengembangkan standar dan panduan untuk berbagai bidang, termasuk forensik digital.

Chain of Custody: Dokumentasi yang mencatat setiap orang yang memiliki atau menangani bukti digital, serta tanggal dan waktu kepemilikan.

Syslog: Sistem *logging* yang digunakan oleh sistem operasi *linux* untuk merekam berbagai macam aktivitas sistem.

CentOS: Distribusi *linux* yang populer, dikenal karena stabilitas dan keandalannya.

Spyware: Perangkat lunak yang dirancang untuk memantau aktivitas pengguna tanpa sepengetahuan mereka.

Virtual Machine: Lingkungan perangkat lunak yang mensimulasikan komputer fisik, memungkinkan pengguna untuk menjalankan sistem operasi lain di dalam sistem operasi utama.

OVA: *Open Virtualization Appliance*, format file yang digunakan untuk mengemas dan menyebarkan perangkat lunak *virtual*.

Hostname: Nama unik yang diberikan kepada komputer atau perangkat lain dalam jaringan.

Netstat: Perintah baris perintah yang digunakan untuk menampilkan informasi tentang koneksi jaringan dan tabel *routing*.

IP Address: Alamat unik yang diberikan kepada setiap perangkat yang terhubung ke jaringan.

User ID: Nomor unik yang diberikan kepada setiap pengguna dalam sistem operasi.

Cron: Penjadwal tugas yang digunakan oleh sistem operasi *Linux* untuk menjalankan tugas secara berkala.

Firewall: Sistem keamanan yang memblokir akses yang tidak sah ke jaringan komputer.

Mtime: *Modified time*, atribut *file* yang menunjukkan kapan *file* terakhir kali dimodifikasi.

Crontab: File konfigurasi yang digunakan untuk menjadwalkan tugas menggunakan *cron*.

DAFTAR LAMPIRAN

Lampiran 1. Kartu Bimbingan Skripsi Pembimbing 1

Lampiran 2. Kartu Bimbingan Skripsi Pembimbing 2

Lampiran 3. Dokumen *Chain of Custody*

