Virtual Machines Forensics

Andrea Di Maio
dimaio-andrea@tiscali.it

Pasquale Salza
pasquale.salza@gmail.com

Sicurezza
A.A. 2010-2011

Indice

- Introduzione
- Le macchine virtuali
- Indagine forense
- Due scenari di Anti-Forensics
- Intercettazione delle VM
- Riferimenti
- Conclusioni

Introduzione

La sicurezza nell'ambito della virtualizzazione non è ancora ad un livello di sviluppo sufficiente.

L'indagine forense nel campo non può essere condotta allo stesso modo di un'indagine tradizionale.

Per sviluppare tale branca della sicurezza, è necessario conoscere innanzitutto il «nemico» (Anti-Forensics).

Le macchine virtuali

Il mondo delle macchine virtuali, le loro componenti essenziali e le applicazioni moderne.

Tipologie

La virtualizzazione può essere classificata in:

- **Emulazione**
  Non si utilizzano direttamente le risorse fisiche ma, queste, sono del tutto emulate.
- **Full Virtualization**
  La virtualizzazione avviene solo se l'hardware è compatibile con il sistema ospite.
- **Paravirtualization**
  La maggior parte dell'hardware fisico è interfacciato direttamente con il sistema ospite.

Hypervisors

L' *hypervisor* è il componente chiave per un sistema virtualizzato.

Può essere classificato come:

- *Bare-Metal Hypervisor* (tipo 1)
- *Embedded Hypervisor*
- *Hosted Hypervisor* (tipo 2)

Applicazioni

La virtualizzazione, a fronte di una leggera perdita prestazionale rispetto alla macchina fisica, slega completamente le risorse utilizzate dall'hardware fisico.

Questo porta diversi vantaggi, come:

- costi minori
- recupero in caso di malfunzionamenti
- sandbox
- strumenti di analisi forense

Indagine forense

Le attività dell'investigatore forense nel campo delle macchine virtuali, le modalità di analisi e l'utilizzo delle macchine virtuali come strumento per l'analisi forense.

Macchine virtuali come strumenti investigativi

C’è l’esigenza di preservare un’immagine estratta da una memoria volatile o da una memoria di massa.

Grazie alle macchine virtuali è possibile avviare una simulazione completa di un sistema sospetto.

Penguin Sleuth Kit

L'obiettivo è quello di portare una serie di strumenti per l'analisi forense al ricercatore comune, senza che questi conosca strettamente Linux.

Caine

Caine è un tool che offre un ambiente completo per tutte le fasi dell'indagine forense.

Macchine virtuali interrotte

Dato il largo impiego in molti ambiti aziendali, anche le macchine virtuali necessitano di essere esaminate.

Una macchina virtuale è costituita semplicemente da un file memorizzato su un dispositivo.

Tracce di virtualizzazione

Nei sistemi Windows è possibile riscontrare alcune tracce:

- **File d'installazione**
  Sono artefatti dovuti all'installazione di un programma di virtualizzazione o nella registrazione della configurazione.
- **Registro di sistema**
  Es. MUICache.
- **Files di prefetch**
  Registrano informazioni sugli eseguibili per esecuzioni successive in modo velocizzato.
- **Page file**
  Windows effettua lo swap dei dati tra memoria volatile e memoria di massa memorizzando i dati in un file.

Prevenire è meglio che curare

Trovare tracce di esecuzione non è sufficiente a rilevare l'attività all'interno dell'ambiente virtuale.

L'unica arma a possibile è l'esecuzione di un keylogger.

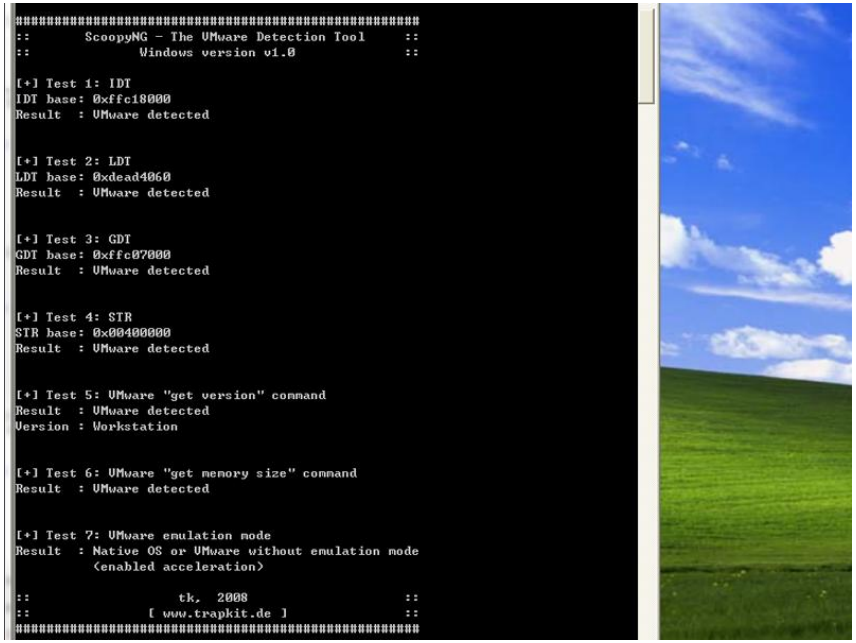
Macchine virtuali in esecuzione

Le macchine virtuali sospette potrebbero essere in esecuzione su di un cluster quindi spesso non prelevabili.

Le indagini corrispondono in pieno a quelle effettuate con macchine fisiche in esecuzione ma si distinguono nella fase preliminare di riconoscimento tra ambiente virtuale e fisico.

ScoopyNG

ScoopyNG analizza le eventuali impronte digitati lasciate dal software di virtualizzazione VMware.



Due scenari di Anti-Forensics

La realizzazione di due soluzioni per due diversi scenari di Anti-Forensics tramite l'uso di dispositivi portatili con relativi software per la virtualizzazione e la sicurezza portabili.

Scenario 1:
Utilizzo in luogo pubblico

QEMU

QEMU è un software che implementa un particolare sistema di emulazione.

È composto da due parti:

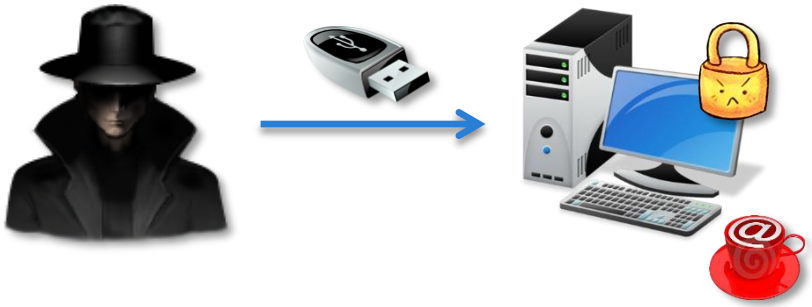
- emulazione
- emulatore di Sistema

Alternate Data Streams

I flussi di dati alternativi o *ADS* (*Alternate Data Streams*) sono disponibili univocamente su partizioni NTFS.

Permette di aggiungere flussi di dati a ogni singolo file.

Pro e contro – Scenario 1



Pro	Contro
• Avvio senza permessi di amministratore • Avvio da qualsiasi postazione	• Lentezza • Limitazione nella scelta dei sistemi operativi emulabili • Sicurezza limitata

Scenario 2:
Utilizzo in luogo autorizzato

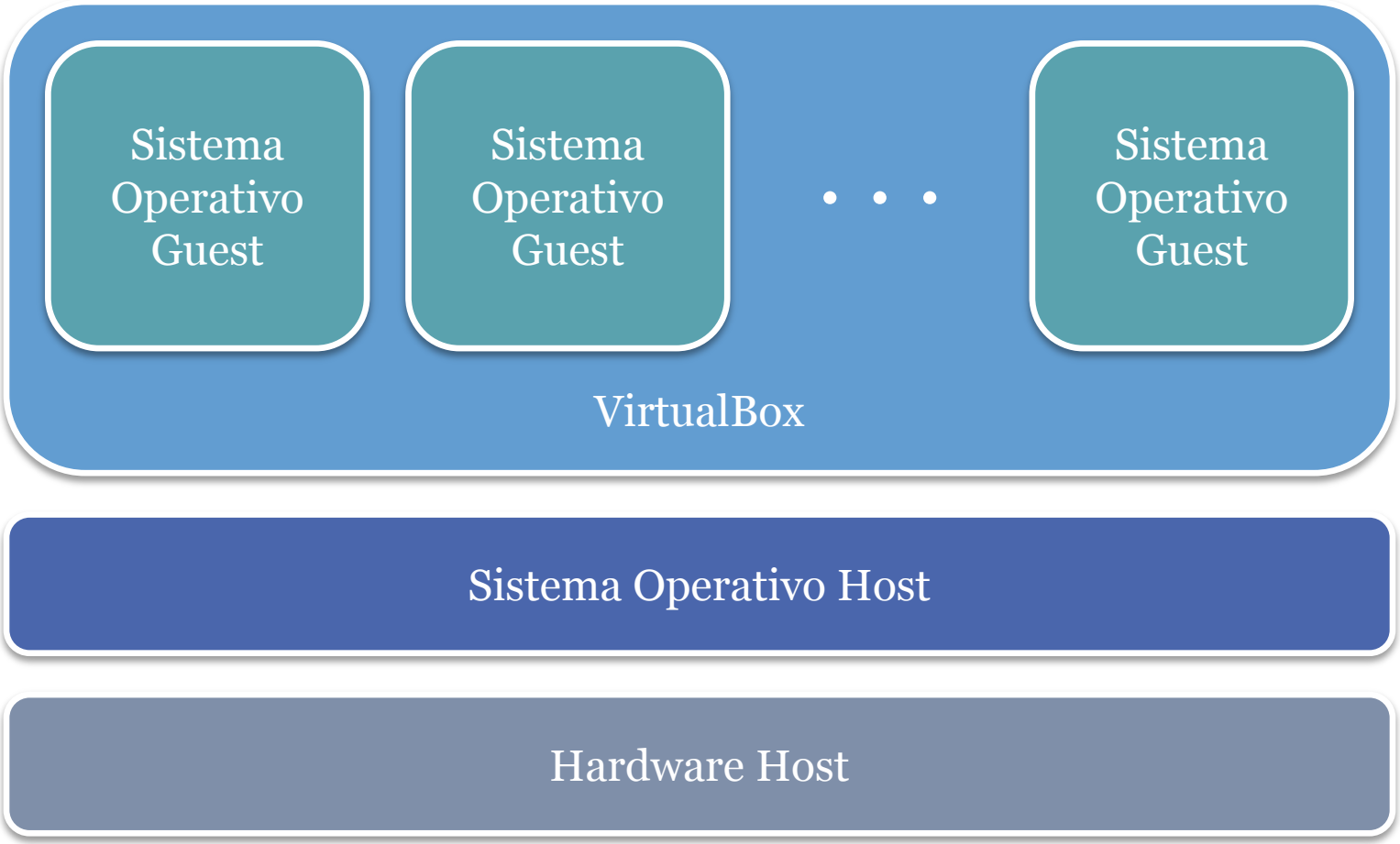
VirtualBox

È un software di virtualizzazione sviluppato dalla *Oracle Corporation*.

Emula i seguenti componenti hardware:

- hard disk, tramite i file *VDI* (*Virtual Disk Images*)
- scheda grafica, una *VESA* con 12 MB di RAM
- scheda di rete
- scheda audio, una *Intel ICH AC'97* o una *SoundBlaster 16*

VirtualBox - Architettura



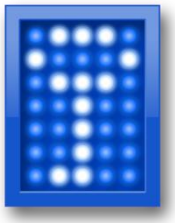
VirtualBox – Esecuzione del codice

VirtualBox tenta di eseguire quanto più codice guest possibile in maniera nativa (sul processore host).

Rispetto al contesto dell'architettura «*ring*» di *Intel*, utilizza la seguente strategia per l'esecuzione del codice guest:

- il codice ring 3 (modalità utente) è eseguito direttamente dal processore host
- il codice ring 0 (istruzioni privilegiate) è eseguito come ring 1, ove possibile
- in caso di errori, utilizza un ricompilatore dinamico basato su *QEMU*

TrueCrypt

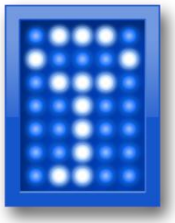


È un noto applicativo utilizzato per la crittazione *on-the-fly* (*OTFE*, *On-the-fly Encryption*) di:

- interi dischi rigidi
- partizioni
- dischi virtuali

Questi elementi prendono il nome di «*volumi*».

TrueCrypt – Volumi

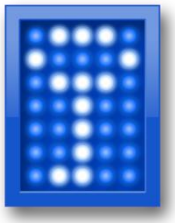


Ogni volume è crittato attraverso una password, secondo svariati algoritmi di crittazione.

Una volta creato un volume è possibile, tramite il programma, montarlo come una periferica rimovibile (previo inserimento della password corretta).

Sarà possibile leggere e scrivere velocemente (on-the-fly) i file contenuti in esso.

TrueCrypt – Plausible deniability



TrueCrypt garantisce che non possa essere provato in alcun modo l'utilizzo di un volume come contenitore di file crittati.

Visto dall'esterno l'intero volume presenterà dei dati del tutto casuali e privi di correlazione.

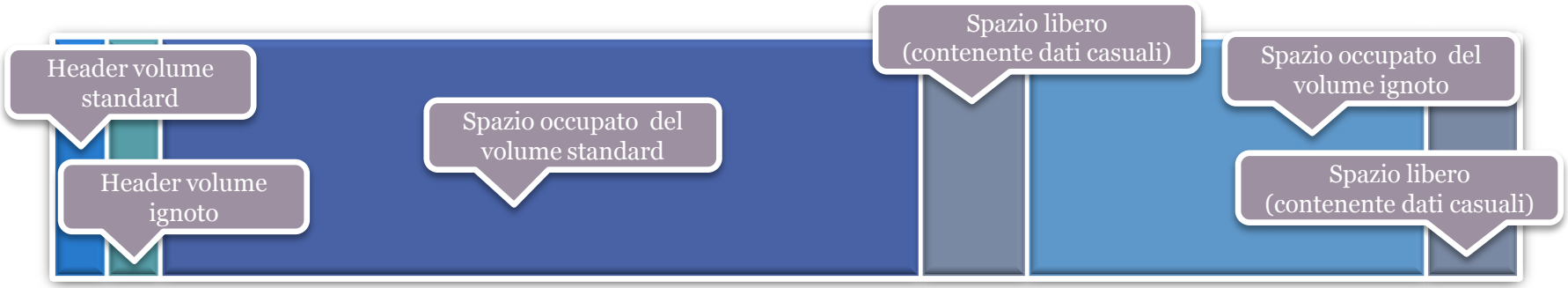
Questa garanzia, chiamata «*plausible deniability*» (negazione plausibile), è ulteriormente accentuata dalla possibilità di creare «*volumi ignoti*».

TrueCrypt – Volumi ignoti

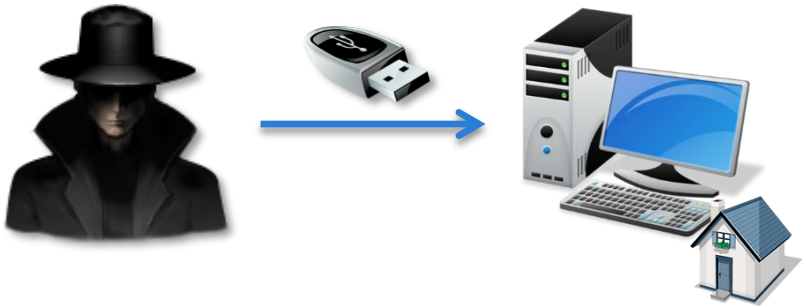
È possibile creare un volume nascosto, protetto da un'ulteriore password, all'interno di un volume *TrueCrypt* standard esistente.

Il volume occuperà lo spazio libero non occupato dai file del volume standard.

La presenza di due password garantisce la protezione in caso di estorsione.



Pro e contro – Scenario 2



Pro	Contro
• Velocità • Ampia scelta tra i sistemi operativi emulabili • Maggiore sicurezza	• Anonimia minore

Intercettazione delle VM

I test effettuati tramite l'uso di keylogger per intercettare le attività all'interno dell'ambiente virtualizzato.

I keylogger utilizzati

I test sono stati effettuati tramite tre prodotti software:

- Spytech SpyAgent 7.50.11
- REFOG Personal Monitor 7.1
- The Best Keylogger

Il test somministrato

Il test è consistito nell'esecuzione dei due scenari visti prima e dell'inserimento di input da tastiera.

In seguito sono state verificate le seguenti proprietà di rilevazione:

- Apertura programma
- Rilevamento tastiera
- Screenshots finestra
- Screenshots tutto schermo

I risultati – Scenario 1

Tutti e tre i software verificano le proprietà per il primo scenario.

L'apertura di QEMU è rilevata così come l'input da tastiera e la cattura delle schermate.

I risultati – Scenario 2

Tutti e tre i software verificano le proprietà per il secondo scenario, tranne che per l'intercettazione dell'input da tastiera.

I risultati – Riassunto

		Spytech SpyAgent	REFOG Personal Monitor	The Best Keylogger
Scenario 1	Apertura programma	✓	✓	✓
	Rilevamento tastiera	✓	✓	✓
	Screenshots finestra	✓	✓	✓
	Screenshots tutto schermo	✓	✓	✓
Scenario 2	Apertura programma	✓	✓	✓
	Rilevamento tastiera	✗	✗	✗
	Screenshots finestra	✓	✓	✓
	Screenshots tutto schermo	✓	✓	✓

Riferimenti

Eoghan Casey
Handbook of Digital Forensics and Investigation
Academic Press, 2009

T. Killalea, D. Brezinski
Guidelines for Evidence Collection and Archiving
http://www.ietf.org/rfc/rfc3227.txt

Greg Kipper, Diane Barrett
Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments
Syngress, 2010

TrueCrypt
Plausible deniability
http://www.truecrypt.org/docs/?s=plausible-deniability

Conclusioni

È molto semplice creare un sistema portatile in grado di nascondere l'identità di un utente e la sua attività.

La combinazione dei giusti strumenti può produrre un sistema portatile con una tracciabilità minima.

I risultati sono stati entusiasmanti per la contro parte, ossia l'Anti-Forensics.

L'analisi forense ha necessità di stare al passo coi tempi e con le nuove tecnologie quindi, in tal senso, è strettamente necessario che gli strumenti d'indagine si adattino e crescano allo stesso ritmo dei loro oggetti di studio.