Difesa

Capire i metodi e i sistemi di difesa per evaderli

Prevenzione

Prevenzione

Formazione del personale

- **Security Awareness**: Formare il proprio personale è fondamentale, infatti le persone sono la prima linea di difesa quando si tratta di attacchi informatici. Molti malware ad esempio sfruttano email di phishing aperte proprio dai non addetti ai lavori, imparare a riconoscerle può prevenire attacchi ransomware o malware più generici.

- L’attività formativa deve essere rivolta anche al personale non tecnico. Le persone che non lavorano nell’IT ad oggi sono poco consci dei rischi che corrono aprendo file o navigando in internet.

Prevenzione

Procedure di sicurezza

- **Policy**: è molto importante definire delle policy di sicurezza, da implementare con strumenti e soluzioni tecnologiche, per avere un buon livello di Security posture.

- **Processi di ricovery ben definiti**: prevenire è meglio che curare, infatti le aziende dovrebbero disporre di piani definiti e conosciuti a tutti da attivare in caso di emergenza. Definire un Ricovery Plan aiuta nel caso di attacchi ransomware, definire un piano di Incident Response aiuta a stabilire come reagire agli attacchi diretti all'organizzazione.

- **Procedure di autorizzazione**: per autorizzare un'azione, a maggior ragione se è un'operazione delicata, la best practice è quella di avere almeno due persone che la autorizzino. In questo modo si abbassa la probabilità di autorizzare qualche azione malevola.

Prevenzione

Security Posture aziendale

La Security Posture è l’insieme di processi, strumenti e awareness che un’azienda attua per la gestione della sicurezza informatica.

Prevenzione

Vulnerability Management

Il **Vulnerability Management** è il processo di identificazione, valutazione, trattamento e segnalazione delle vulnerabilità di sicurezza nei sistemi e nel software. Implementato insieme ad altre tecniche di sicurezza, è vitale alle organizzazioni per dare priorità alle possibili minacce e ridurre al minimo la superficie di attacco.

- Vulnerability Assessment (VA) periodici
- Risk ranking delle vulnerabilità rilevate
- Le remediation devono essere veloci

Hardening

Hardening

Linee guida di sicurezza 1/6

MINIMIZZA SOFTWARE E SERVIZI
Se non hai bisogno di un software o di un servizio, disinstallalo. Il rischio è quello di “aiutare” l’attaccante perché aumenti la tua superficie di esposizione.

UTILIZZA PIÙ SISTEMI PER SERVIZI DIVERSI
Se un attaccante riesce ad exploitare il tuo webserver e sullo stesso sistema c’è un servizio di file sharing, è molto probabile che riuscirà ad accedere anche a quello.

Hardening

Linee guida di sicurezza 2/6

CIFRA LE TRASMISSIONI DATI
Cifrando le comunicazioni si evitano attacchi MITM (man-in-the-middle). Utilizza SFTP, SNMPv3, HTTPS, SSH. Evita di usare protocolli che comunicano in chiaro come TELNET.

NON USARE ACCOUNT CONDIVISI
Ogni persona che accede al sistema dovrebbe avere il proprio account e questo vale anche per i servizi. Inoltre gli account condivisi, oltre a diminuire la sicurezza complessiva di un sistema, rendono difficile l’auditing.

Hardening

Linee guida di sicurezza 3/6

NON FARE LOGIN CON ROOT
Gli utenti dovrebbero utilizzare i propri account e quando necessario utilizzare il comando sudo per eseguire comandi o programmi con altri privilegi. Utilizzando sudo le azioni vengono loggate, migliorando l'auditing.

Al contrario degli altri account **root** è spesso condiviso, pertanto è necessario utilizzarlo sempre con cautela e solo quando strettamente necessario.

MANUTENERE GLI ACCOUNT
Password forti (> 12 caratteri alfanumerici) e cambiate regolarmente aumentano la security posture del sistema. Gli account non più in utilizzo vanno rimossi (o disabilitati, in base alle necessità).

Hardening

Linee guida di sicurezza 4/6

TWO-FACTOR AUTHENTICATION

Per sistemi critici (ad esempio quelli militari o governativi) l'autenticazione dovrebbe essere basata su più fattori, generalmente una password e un codice temporaneo (OTP) o l'impronta digitale.

UTILIZZARE IL PRINCIPIO DEL "LEAST PRIVILEGE"

Non avviare servizi con l'utente root, funzionano ugualmente con i propri account di servizio. Dai agli utenti i privilegi minimi indispensabili per poter svolgere la loro mansione.

Hardening

Linee guida di sicurezza 5/6

MONITORA L'ATTIVITÀ DI SISTEMA

Revisiona periodicamente i log di sistema e inviali ad un sistema centralizzato di logging, tipicamente un SIEM, cosicché se venissero cancellati dal sistema locale avrai una copia.

UTILIZZA IL FIREWALL

Linux possiede un firewall software built-in: netfilters + iptables. Sempre secondo il principio “least privilege”, autorizza solo le connessioni necessarie e “droppa” tutto il resto, anche se il sistema sta dietro un firewall hardware.

Hardening

Linee guida di sicurezza 6/6

CIFRA I DATI SENSIBILI

Oltre alla cifratura delle connessioni, è necessario cifrare i dati sensibili anche quando sono memorizzati sui sistemi, in modo da prevenire un eventuale lettura o alterazione da soggetti non autorizzati. Anche le informazioni nei database vanno cifrate.

Hardening

Full Disk Encryption (FDE)

Il Sistema Operativo deve avere accesso ai file decifrati per poterli leggere e scrivere, ad esempio in Linux la FDE viene supportata da dm-crypt (Device mapper crypt), esso fornisce infatti una cifratura completamente trasparente al sistema e all'utente: viene creato un nuovo Device in /dev/mapper ed è possibile utilizzarlo come un normale disco.

Il modulo kernel si occuperà della traduzione da plaintext a ciphertext.

Quando il sistema è acceso è sbloccato, pertanto la chiave potrebbe essere in RAM!

Hardening

OS Hardening

- Aggiornamenti di sicurezza
- Aggiornamenti di sistema
- Aggiornamenti degli applicativi
- Rimozione dei servizi inutilizzati
- Segmentazione di rete e firewalling

Hardening

OS Hardening - Account

- Password forti
- 2FA (two factor authentication)
- Scadenza password impostata
- Cambio password periodico (es. ogni 90 giorni)
- Lockout in caso di login errato
- Disabilitazione account per inutilizzo

Strumenti di difesa

Strumenti di difesa

Firewall

Dispositivi hardware (o software) che prevengono gli accessi non autorizzati da e verso le reti private.

Il firewall analizza tutti in pacchetti e blocca quelli che non rispettano i criteri di sicurezza impostati (ACL, Access Control List).

Strumenti di difesa

WAF

Un **WAF** (web application firewall) aiuta a proteggere le applicazioni web filtrando e monitorando il traffico HTTP.

In genere protegge le applicazioni web da attacchi come cross-site request forgery (CSRF), cross-site-scripting (XSS), file inclusion e SQL injection.

Un WAF agisce al livello 7 del modello OSI.

Strumenti di difesa

IDS

NIDS:
Network-based IDS, consiste in una macchina posta nella rete in modalità promiscua, in ascolto sul traffico, in grado di generare alert in caso di pattern malevoli.

HIDS:
Host-based IDS, sono in genere applicativi (agent) installati in host specifici, in grado di fare auditing sugli eventi dell’host in analisi.

Strumenti di difesa

IPS

Un **IPS** (**Intrusion Prevention System**) è un sistema che rileva e prevede le

minacce identificate. Monitora costantemente la rete per rilevare possibili

incidenti dannosi e acquisire informazioni in merito.

L'IPS segnala questi eventi all'amministratore di sistema e adotta le misure preventive del caso, come la chiusura dei punti di accesso e la configurazione dei firewall.

Strumenti di difesa

Antimalware

Software in grado di rilevare le minacce malware presenti sulla rete o sul sistema.

Gli **antimalware enterprise** hanno una console di gestione centralizzata.

Strumenti di difesa

Secure Email Gateway

Un **SEG** è un dispositivo o un software utilizzato per il monitoraggio delle e-mail. È progettato per prevenire le email indesiderate come spam, attacchi di phishing, malware o contenuti fraudolenti.

I messaggi in uscita possono essere analizzati per evitare che i dati sensibili lascino l'organizzazione o per **criptare automaticamente le email** che contengono informazioni sensibili.

Tecniche di evasione

Tecniche di evasione

IDS Evasion

Insertion Attack

È una tipologia di attacco che confonde l'IDS facendogli leggere pacchetti non validi, l'IDS accetterà i pacchetti che saranno rifiutati dagli end-system coinvolti (computer, server, ecc…), ciò comporterà l'inserimento di dati nell'IDS.

Obfuscation

È una tecnica di evasione IDS, consiste nell'**encoding** del pacchetto (contente il payload) in maniera tale che sia decifrabile solo dall'host target e non dall'IDS, in genere viene utilizzata la crittografia o l'encoding Unicode.

Tecniche di evasione

Firewall Evasion

- **IP Address Spoofing** - L'attaccante maschera il proprio indirizzo IP come se fosse un host fidato (cambiano l'IP sorgente nell'header dei pacchetti).

- **Bypass di siti web bloccati** - Alcuni siti web permettono di navigare su altri siti web attraverso di essi, evitando così le regole IP-based del firewall.

- **Firewall bypass tramite ICMP Tunneling** - È possibile incapsulare nella parte "payload" di un pacchetto ICMP qualsiasi tipo di dato in quanto spesso non ne è controllato il contenuto.

- **DNS Tunneling** - Tecnica che permette di inviare dati attraverso richieste DNS, che in genere sono sempre consentite.

Tecniche di evasione

Encoding

- Unicode
- Decimal
- Hexadecimal
- URL Encode
- Base64

Web Application Security

Web Application Security

OWASP 2017

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entity
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure Deserialization
9. Componenti con vulnerabilità note
10. Logging e monitoraggio insufficiente

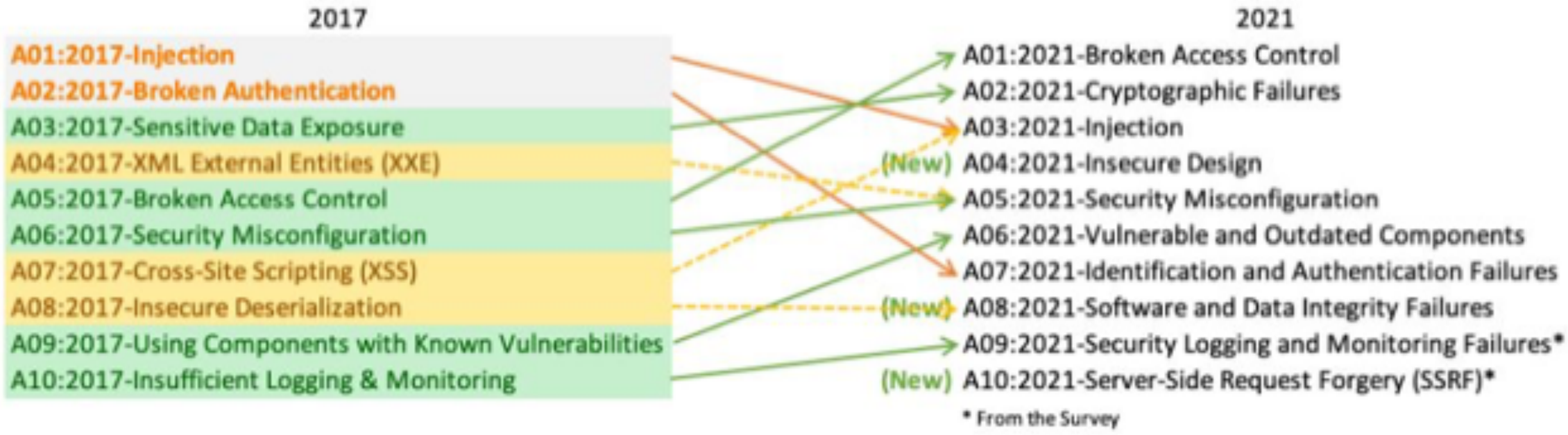
Web Application Security

OWASP 2021

1. Broken Access Control
2. Criptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated components
7. Identification and Authentication failures
8. Software and Data Integrity failures
9. Security Logging and Monitoring failures
10. Server-Side Request Forgery

Web Application Security

OWASP 2021 - Confronto con OWASP 2017



Web Application Security

Broken Access Control

L’**Access Control** permette l’implementazione delle policy di accesso, ad esempio facendo in modo che gli utenti non possano agire al di fuori delle autorizzazioni previste.

I fallimenti tipicamente portano all’information disclosure, alla modifica o alla distruzione di tutti i dati o all'esecuzione di una funzione aziendale al di fuori dei limiti dell'utente.

Web Application Security

Cryptographic Failures

- Determinazione dell'utilizzo della cifratura (at rest, in transit)
- Vengono utilizzati cifrari sicuri?
- I dati sono trasmessi in chiaro?
- Degradazione HTTPS (strict-transport-security)

Web Application Security

Injection

- Code Injection
- SQL Injection
- LDAP Injection
- Come difendersi? Data input validation

Web Application Security

Insecure Design

C'è una differenza tra **progettazione insicura** e **implementazione insicura**. Distinguiamo tra difetti di progettazione e difetti di implementazione per un motivo: hanno cause e rimedi diversi.

Un design sicuro può ancora avere difetti di implementazione che portano a vulnerabilità che possono essere sfruttate. Un design insicuro non può essere corretto da un'implementazione perfetta.

Web Application Security

Security Misconfiguration

- Sistemi/Applicazioni non hardenizzate
- Feature non utilizzate ma attive
- Account di default
- Gestioni non gestite (error handling)
- Security settings in web server

Web Application Security

Vulnerable and Outdated components

- Utilizzo di software datati
- Utilizzo di software vulnerabili
- Componenti di terze parti non testati

Web Application Security

Identification and Authentication Failures

La conferma dell'identità dell'utente, l'autenticazione e la gestione della sessione sono fondamentali per proteggersi dagli attacchi legati all'autenticazione.

- Brute forcing
- Gestione scorretta di SSO
- Information disclosure tramite URL

Web Application Security

Software and Data Integrity Failures

Le **Software and Data Integrity Failures** si riferiscono al codice e all'infrastruttura che non è in grado di proteggere dalle violazioni dell'integrità.

Un esempio di questo è quando un'applicazione si basa su plugin, librerie o moduli da fonti, repository e content delivery network (CDN) non attendibili.

Gli attaccanti potrebbero potenzialmente caricare i propri aggiornamenti da distribuire ed eseguire su tutte le installazioni.

Web Application Security

Security Logging and Monitoring Failures

- Log salvati solo sulla macchina locale
- Log amministrativi poco specifici
- Log applicativi inesistenti o poco esplicativi

Web Application Security

Server-Side Request Forgery

Una **SSRF** si verifica quando un'applicazione web recupera una risorsa remota senza convalidare l'URL fornito dall'utente. Questo permette ad un attaccante di costringere l'applicazione ad inviare una richiesta ad una destinazione inaspettata, anche quando è protetta da un firewall, VPN, o un altro tipo di lista di controllo degli accessi alla rete (ACL).

L'incidenza di SSRF sta aumentando. Inoltre, la gravità di SSRF sta diventando maggiore a causa dei servizi cloud e della complessità delle architetture.

Web Application Security

Footprinting infrastruttura web

SERVER DISCOVERY: Information gathering su location e status dei server. Informazioni su indirizzi IP, nomi DNS e port scanning permettono di svolgere la fase di service discovery in maniera più agile.

SERVICE DISCOVERY: Analizzare il target per identificare le porte in utilizzo.

SERVER IDENTIFICATION: Analizzare l'header delle risposte del server per identificare modello e versione del software web server.

HIDDEN CONTENT DISCOVERY: Scoprire contenuti e funzionalità nascoste che non sono raggiungibili direttamente, in modo da poterle sfruttare.

Web Application Security

Detection di WAF e Proxy

PROXY: Permette di scoprire se il target sta redirezionando le richieste attraverso un proxy server, in genere questi server aggiungono alcuni campi nell'header di risposta. È possibile utilizzare il metodo TRACE (HTTP 1.1) per identificare dei cambiamenti.

WAF: Verificare se la web application in analisi è protetta da un WAF (Web Application Firewall) tramite i cookie nelle risposte (spesso i WAF aggiungono cookie propri alla richiesta di risposta). Utilizzare wafw00f per scoprire che tipologia di WAF è presente.

Web Application Security

OWASP Web Security Testing Guide

È uno standard di sicurezza che definisce le linee guida da seguire per un corretto sviluppo di Web Application.

https://owasp.org/www-project-web-security-testing-guide/stable/

Attività Post-Attacco

Attività Post-Attacco

Incident Management

L’**Incident Management** è un insieme di processi definiti, volti ad identificare, analizzare, priorizzare e risolvere gli incidenti di sicurezza.

Le fasi si suddividono in:

- Vulnerability Handling,
- Incident Handling: Triage, Incident Response, Reporting e Detection, Analisi
- Artifact Handling,
- Announcements,
- Alerts

Attività Post-Attacco

Post-Mortem Analysis

- Stilare un Incident Report
- Monitoraggio post-incident
- Aggiornare IoC di Threat Intelligence
- Identificare nuove misure di sicurezza
- Impara

Attività Post-Attacco

Digital Forensics

Permette l’analisi post-attacco anche nel caso in cui l’attaccante copra le proprie tracce.

- Recovery di log
- Recovery di file eliminati
- Network forensics
- Dump di memoria

Attività Post-Attacco

Log Analysis

- Fondamentale in caso di attacco
- Procedura che andrebbe eseguita regolarmente
- SIEM
- Log applicativi e di sistema
- Log network