Asset testato: 192.168.153.134
Data di completamento: 2023-12-04
Cliente: **nomeTest**
Referente:"nomeRiferimento"
nomeRiferimento
Contatto: mail@dominio.it

Tabella riepilogativa dei risultati

In questa sezione sono riportati i risultati complessivi del test per l'asset indicato nella sezione "Dettagli del test". Seguendo le best practice internazionali, le vulnerabilità individuate sono caratterizzate per livello di rischiosità (Critico, Alto, Medio, Basso e Informativo) in cui è riportata la loro numerosità. I dettagli delle singole vulnerabilità sono riportati nella sezione denominata "Sezione tecnica".

2	2	3	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Livello di Rischio



RISCHIO CRITICO

La situazione informatica aziendale è al massimo rischio, si consiglia di applicare immediatamente i rimedi suggeriti.
La compromissione della risorsa informatica aziendale è altamente probabile, infatti le vulnerabilità **CRITICHE** espongono il sistema sia ad attacchi diretti che indiretti.

Le vulnerabilità individuate dal software AntiHacker di CyLock sono quelle più utilizzate dagli hacker per compromettere i sistemi informatici aziendali.
La presenza di queste vulnerabilità è un campanello d'allarme, cioè la traccia che porta a vie di attacco più insidiose e dannose, ovvero che consentono ad un criminale informatico di ottenere l'accesso al sistema informatico con minore sforzo e che possono condurre ad ottenere i privilegi di amministratore di sistema.

Tra le vulnerabilità trovate sono state individuate delle **RCE (Remote Command Execution)**. Queste vulnerabilità sono tra le più gravi, in quanto permettono di eseguire del codice dannoso sulla macchina coinvolta. Questo tipo di vulnerabilità può portare a diverse casistiche, quali ad esempio **l'attivazione di RDP, l'inserimento di shell, esfiltrazione di dati sensibili**. Si consiglia di sanare immediatamente questa vulnerabilità.

Le **vulnerabilità nella divulgazione di informazioni (IDV)** sono una classe di punti deboli della sicurezza che possono **esporre dati sensibili a utenti non autorizzati.** Queste vulnerabilità si verificano quando un'applicazione Web rivela involontariamente informazioni riservate.

Gli **XSS cross-site scripting** sono molto comuni, permettono di eseguire codice javascript ma nella maggior parte dei casi sono poco

invasivi e di difficile attuazione. Si prestano ad attacchi di phishing e in questo caso possono essere anche invasivi.

Sono presenti attacchi **DDoS e DoS, capaci di negare il servizio agli utenti.** Le complicazioni sono molteplici: ad esempio impossibilità di emettere fatture, inviare mail, inserire ordini, ecc... con rischio di causare grossi danni per l'azienda.

Manca un adeguato rafforzamento della sicurezza in qualsiasi parte dello stack dell'applicazione o autorizzazioni configurate in modo errato sui servizi cloud.

Sono presenti vulnerabilità **SSL di crittografia.** Queste sono le vulnerabilità più comuni, permettono di decriptare il traffico e poterlo vedere in chiaro, permettono attacchi MITM tra i più subdoli e difficili da evitare. Per realizzare attacchi di questo tipo bisogna trovarsi sulla rete nella posizione giusta il chè non è sempre facile se si tratta di reti pubbliche.

Metodologie utilizzate

I test eseguiti dal software EVA sono condotti seguendo rigorose metodologie di sicurezza, tra cui OSSTMM (Open Source Security Testing Methodology Manual) e OWASP (Open Web Application Security Project), al fine di garantire una copertura completa e dettagliata delle possibili minacce, dei vettori d'attacco delle vulnerabilità e delle best practice per fornire una solida base di raccomandazioni e remediation ed aumentare, di conseguenza, il livello generale di sicurezza informatica aziendale. In particolare, la metodologia OSSTMM è una guida completa per condurre test di sicurezza in ambienti operativi reali, mentre la Metodologia OWASP è principalmente utilizzata per identificare e mitigare le vulnerabilità specifiche delle applicazioni web. Nel report, le vulnerabilità sono categorizzate anche in riferimento a questi standard.

Come leggere il report

Il report riporta molte informazioni, dalla classificazione univoca del CVE agli elementi caratterizzanti la vulnerabilità e le remediation. Ogni vulnerabilità è suddivisa per livello di rischiosità, che è misurato tramite il codice internazionale CVSS. Per aiutare il tecnico a comprendere più approfonditamente la possibilità per un criminale informatico di sfruttare la vulnerabilità individuata, oltre il codice CVSS sono state inserite altre informazioni, raggruppate tramite icone, dalla categoria OWASP cui possono essere riferite le stesse vulnerabilità, alla presenza in rete di "istruzioni" per poter sfruttare la vulnerabilità stessa. Nel seguito si riporta la legenda per ogni singola icona:


Gli exploit o il PoC è presente nel database pubblico exploit-db, molto pericoloso perchè chiunque può utilizzarlo


L'exploit è presente nel programma in GitHub, molto pericoloso perchè chiunque può recuperarlo. GitHub è una piattaforma di programmi sorgenti molto utilizzata e quindi di facile accesso


L'exploit è pubblico sul Web, chiunque ne ha accesso e può sfruttarne il potenziale dannoso gratuitamente


Il PoC è riportato nella sezione dedicata della vulnerabilità


L'exploit è presente nel programma Metasploit, molto pericoloso perchè chiunque può utilizzarlo molto facilmente. Metasploit è una piattaforma di exploit con uso facilitato chiunque senza esperienza può utilizzare qualsiasi exploit


L'exploit o il PoC è disponibile a pagamento. Qualsisi vulnerabilità abbastanza degna di essere venduta è disponibile a pagamento. Questo limita l'attaccante, anche se non è sempre così


Dalle informazioni in nostro possesso non è possibile capire se il PoC o l'exploit è pubblico. Questa informazioni può variare nel tempo.


Trovato ZeroDay, i nostri attacchi hanno rilevato una nuova vulnerabilità non presente in rete.


Questa vulnerabilità richiede un test manuale, deve essere verificata da un pentester per la verifica.



Questa vulnerabilità non può essere testata per non dare disservizi al cliente. Gli attacchi DoS interrompono il servizio o potrebbero causare il riavvio della macchina.



La vulnerabilità è riconosciuta ma non esiste ancora un CVE per identificarla



La vulnerabilità è stata testata in maniera indiretta tramite richiesta e risposta del target.

Sezione tecnica

Questa sezione del report è dedicata ai tecnici che si occupano delle attività di remediation delle vulnerabilità individuate tramite il software CyLock . La sezione è suddivisa in due parti, nella prima, sono riportate in apposita tabella le porte scansionate risultate aperte e con vulnerabilità. Ogni porta può avere più vulnerabilità, pertanto in tabella è associato il valore di rischiosità maggiore rispetto a tutte le vulnerabilità che vi sono state trovate. A questa tabella segue poi una sezione dedicata alle note di rilievo o informazioni utili ma fuori perimetro di analisi emerse nel corso del test. Infatti, è bene sottolineare, che nel corso di un VA/PT, il software può individuare informazioni che sono vagliate dai tecnici CyLock e nel caso in cui abbiano un valore, anche solo informativo per il cliente, sono riportate per completezza di analisi. A questa sezione, seguono poi tutte le singole vulnerabilità, suddivise per porta in cui sono state individuate, dalla più rischiosa alla meno rischiosa. Il livello di rischiosità è dato dallo score CVSS associato alla vulnerabilità. Per arricchire l'informazione e consentire al tecnico una valutazione migliore delle attività di remediation da intraprendere, ogni vulnerabilità ha associate altre informazioni, sia testuali, sia mediante le icone che svolgono un ruolo molto importante poiché, ad esempio, possono indicare sia il livello OWASP top 10 della singola vulnerabilità sia la prese, anche gratuita, online di informazioni per sfruttare effettivamente la vulnerabilità individuata. In questo modo, il tecnico potrà prioritizzare, in base al valore dell'asset e l'insieme informativo fornito, le azioni di mitigation possibili.

Attenzione, le informazioni contenute in questa sezione sono da considerarsi come altamente confidenziali e sensibili, pertanto si sconsiglia qualsiasi inoltro, divulgazione o diffusione non autorizzata del presente report e delle informazioni in esso contenute

Lista delle porte scansionate risultate aperte con vulnerabilità

21 TCP	ftp	vsftpd 2.3.4	CRITICAL
22 TCP	ssh	OpenSSH 4.7p1 Debian 8ubuntu1	CRITICAL
80 TCP	http	Apache httpd 2.2.8	HIGH
443 TCP	https	Apache httpd 2.2.8	HIGH

Note tecniche

Abbiamo trovato un file publish.zip protetto da password, trovarla e decifrarla è solo questione di tempo. Si consiglia dunque di eliminare ogni file esposto per evitare di rivelare possibili informazioni sensibili ad estranei.

Vulnerabilità rilevate sulla porta 21

CRITICAL	CVE-2011-2523	CVSS3 9.8	OWASP 1	
vsftpd 2.3.4 contiene una backdoor				

Dettagli

vsftpd 2.3.4 scaricato tra 20110630 e 20110703 contiene una backdoor che apre una shell sulla porta 6200/tcp.

Referenze

https://nvd.nist.gov/vuln/detail/CVE-2011-2523
https://en.wikipedia.org/w/index.php?title=Arbitrary_code_execution&redirect=yes

Rimedio

Aggiorna VSFTPD all'ultima versione disponibile

Vulnerabilità rilevate sulla porta 22

CRITICAL	CVE-2016-1908	CVSS3 9.8	OWASP 2	
OpenSSH < 7.2				

Dettagli

Il client in OpenSSH prima della 7.2 gestisce in modo errato la generazione di cookie non riuscita per l'inoltro X11 non attendibile e si affida al server X11 locale per le decisioni di controllo degli accessi, che consente ai client X11 remoti di attivare un fallback e ottenere privilegi di inoltro X11 attendibili sfruttando i problemi di configurazione su questo server X11 , come dimostrato dalla mancanza dell'estensione SECURITY su questo server X11.

Referenze

https://nvd.nist.gov/vuln/detail/CVE-2016-1908
https://www.automox.com/blog/vulnerability-definition-authentication-bypass

Rimedio

Aggiorna OpenSSH all'ultima versione disponibile.

Vulnerabilità rilevate sulla porta 80

HIGH	CVE-2020-7660	CVSS3 8.1	OWASP 1	
Serialize-Javascript < 3.1.0				

Dettagli

serialize-javascript prima di 3.1.0 consente agli aggressori remoti di iniettare il codice arbitrario tramite la funzione " deletefunctions "all'interno di " index.js ".

Referenze

https://nvd.nist.gov/vuln/detail/CVE-2020-7660
https://en.wikipedia.org/w/index.php?title=Arbitrary_code_execution&redirect=yes

Informazioni Aggiuntive - PoC

eval('('+ serialize({"foo": /1" + console.log(1)/i, "bar": '"@__R--0__@'}) + ')');

Rimedio

Aggiorna il prodotto all'ultima versione disponibile

MEDIUM	CWE-548	NONE	OWASP 3	
Directory Listing				

Dettagli

La directory fornisce a un utente malintenzionato l'indice completo di tutte le risorse che si trovano all'interno della directory. I rischi e le conseguenze specifiche variano a seconda dei file elencati e accessibili. Tutti i file non eseguibili (zip,xlsx...) vengono scaricati, un malintenzionato può quindi leggerne il contenuto.

Referenze

https://cwe.mitre.org/data/definitions/548.html
https://cwe.mitre.org/data/definitions/200.html

Informazioni Aggiuntive - PoC

/dav/
/upload

Rimedio

Inserire all'interno della directory un file index.html vuoto

MEDIUM	CWE-79	CVSS3 6.5	OWASP 7	
0Day - XSS (Cross-site scripting)				

Dettagli

Il prodotto non neutralizza o neutralizza in modo non corretto l'input controllabile dall'utente prima che venga inserito nell'output utilizzato come pagina web che viene offerta ad altri utenti.

Referenze

https://cwe.mitre.org/data/definitions/79.html
https://it.wikipedia.org/wiki/Cross-site_scripting

Informazioni Aggiuntive - PoC

```
1  POST /appCore/ajax.adm_server.php?plf=framework&mn=
   coursepath_notifications_manager&op=list_coursepath_notifications
22 page=1&rows=20&startIndex=0&results=
   <html><img+src=x+onerror=alert(`XSS`)></html>%0a&filter_text=text&
   filter_criteria=filter
```



Rimedio

Sanificare l'input del cliente

MEDIUM	CVE-2020-28500	CVSS3 5.3	OWASP 9	
Lodash < 4.17.21				

Dettagli

Le versioni di Lodash precedenti alla 4.17.21 sono vulnerabili a Regular Expression Denial of Service (ReDoS) tramite le funzioni toNumber, trim e trimEnd.

Referenze

https://nvd.nist.gov/vuln/detail/CVE-2020-28500
https://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_DoS_attack

Informazioni Aggiuntive - PoC

/ajax/libs/lodash.js/4.17.11/lodash.js

Rimedio

Aggiornamento Lodash ultima versione

LOW	CAPEC-103	CVSS3 4.3	OWASP 6	

Clickjacking: X-Frame-Options header missing

Dettagli

Il clickjacking (attacco di ripristino dell'interfaccia utente, attacco di ripristino dell'interfaccia utente, ripristino dell'interfaccia utente) è una tecnica dannosa per indurre un utente Web a fare clic su qualcosa di diverso da ciò su cui l'utente percepisce di fare clic, rivelando potenzialmente informazioni riservate o prendendo il controllo del proprio computer mentre facendo clic su pagine Web apparentemente innocue. Il server non ha restituito un'intestazione X-Frame-Options, il che significa che questo sito Web potrebbe essere a rischio di un attacco di clickjacking. L'intestazione della risposta HTTP X-Frame-Options può essere utilizzata per indicare se un browser deve essere autorizzato o meno a eseguire il rendering di una pagina all'interno di un frame o iframe. I siti possono utilizzarlo per evitare attacchi di clickjacking, assicurandosi che il loro contenuto non sia incorporato in altri siti.

Referenze

https://capec.mitre.org/data/definitions/103.html
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Rimedio

Configura il tuo server web per includere un'intestazione X-Frame-Options. Consultare i riferimenti Web per ulteriori informazioni sui possibili valori per questa intestazione.

Vulnerabilità rilevate sulla porta 443

HIGH	CVE-2016-2183	CVSS3 7.5	OWASP 6	

TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)

Dettagli

I cifrari a blocchi legacy con una dimensione di blocco di 64 bit sono vulnerabili a un pratico attacco di collisione se utilizzati in modalità CBC. Sono interessate tutte le versioni dei protocolli SSL/TLS che supportano suite di cifratura che utilizzano 3DES come cifrario di cifratura simmetrica. La sicurezza di un cifrario a blocchi è spesso ridotta alla dimensione della chiave k: il miglior attacco dovrebbe essere la ricerca esaustiva della chiave, con complessità 2 alla potenza di k. Tuttavia, la dimensione del blocco n è anche un importante parametro di sicurezza, che definisce la quantità di dati che possono essere crittografati con la stessa chiave. Ciò è particolarmente importante quando si utilizzano modalità operative comuni: richiediamo che i cifrari a blocchi siano sicuri con un massimo di 2 fino alla potenza di n query, ma la maggior parte delle modalità operative (ad es. CBC, CTR, GCM, OCB, ecc.) non è sicura con più di 2 alla potenza di mezzo n blocchi di messaggio (il limite del compleanno). Con un moderno cifrario a blocchi con blocchi a 128 bit come AES, il limite di compleanno corrisponde a 256 exabyte. Tuttavia, per un cifrario a blocchi con blocchi a 64 bit, il limite di compleanno corrisponde a soli 32 GB, che in pratica è facilmente raggiungibile. Una volta che si verifica una collisione tra due blocchi di cifratura, è possibile utilizzare la collisione per estrarre i dati di testo normale.

Referenze

https://nvd.nist.gov/vuln/detail/CVE-2016-2183
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption

Rimedio

Configura il server per disabilitare il supporto per la suite 3DES. Per i server Web Microsoft IIS, vedere l'articolo della Microsoft Knowledgebase http://support.microsoft.com/kb/245030/ (http://support.microsoft.com/kb/245030/) 245030 per istruzioni sulla disattivazione della suite di crittografia 3DES. La seguente configurazione consigliata fornisce un livello di sicurezza più elevato. Questa configurazione è compatibile con Firefox 27, Chrome 22, IE 11, Opera 14 e Safari 7. I protocolli SSLv2, SSLv3 e TLSv1 non sono consigliati in questa configurazione. Utilizzare invece i protocolli TLSv1.1 e TLSv1.2. Fare riferimento alla documentazione del fornitore del server per applicare la configurazione di crittografia consigliata: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM -SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA :ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE -RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES :!RC4:!3DES:!MD5:!PSK

INFO	CWE-757	CVSS N/A	OWASP 6	
TLS 1.0 è Attivo				

Dettagli

Un protocollo o la sua implementazione supporta l'interazione tra più attori e consente a tali attori di negoziare quale algoritmo deve essere utilizzato come meccanismo di protezione come crittografia o autenticazione, ma non seleziona l'algoritmo più potente disponibile per entrambe le parti. Quando un meccanismo di sicurezza può essere costretto a effettuare il downgrade per utilizzare un algoritmo meno sicuro, ciò può rendere più semplice per gli aggressori compromettere il prodotto sfruttando un algoritmo più debole. La vittima potrebbe non essere consapevole che viene utilizzato l'algoritmo meno sicuro. Ad esempio, se un utente malintenzionato può forzare un canale di comunicazione a utilizzare testo in chiaro anziché dati fortemente crittografati, potrebbe leggere il canale tramite sniffing, invece di compiere uno sforzo aggiuntivo nel tentativo di decrittografare i dati utilizzando tecniche di forza bruta.

Referenze

https://cwe.mitre.org/data/definitions/757.html
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/04-Testing_for_Weak_Encryption

Rimedio

Si consiglia di aggiornare all'ulitma versione di TLS

Cosa fare adesso

La criticità delle vulnerabilità trovate può variare in base a specifiche caratteristiche: un PoC pubblico risulta molto grave in quanto fruibile da qualunque cyber criminale rispetto a uno a pagamento o non presente sul web.

Le vulnerabilità CRITICHE devono essere sempre trattate con la massima urgenza e priorità. Esse consentono ad un qualsiasi cyber criminale di avere facile accesso a tutti i dati aziendali, senza bisogno di credenziali di autenticazione o di altre informazioni sulle singole vittime. Questo vuol dire che un hacker, anche di livello mediocre, può ottenere il controllo del sito web, accedere al server su cui esso è sviluppato, e quindi compromettere l'intera sicurezza della tua rete.

Quando il test AntiHacker di CyLock ha individuato delle vulnerabilità nel sistema informatico aziendale classificate come Critiche, l'unica cosa da fare è porvi rimedio il prima possibile. Nel Report tecnico di dettaglio, disponibile tramite la richiesta di upgrade del presente documento cliccando qui, è possibile trovare tutte le istruzioni tecniche dettagliate per poter procedere in autonomia. Pertanto, è utile confrontarsi tecnici specializzati per ottenere un supporto personalizzato per la risoluzione le vulnerabilità individuate o per valutare se sono necessarie azioni ulteriori e mirate per proteggere i vostri sistemi. In caso di mancanza di personale tecnico qualificato da parte della Cliente, si ricorda che CyLock può fornire un supporto tecnico specializzato da remoto, consentendo di risparmiare tempo e risorse con un semplice click.

Descrizione dell'attività condotta

Il presente documento è il resoconto delle attività svolte sull'URL/IP Indicato dalla Committente. Gli obiettivi di questa analisi sono stati quelli di misurare il livello di sicurezza dei servizi esposti online e di porre in evidenza eventuali problemi e/o vulnerabilità riscontrate. L'analisi è stata effettuata utilizzando il software proprietario CyLock, che è stato progettato e sviluppato seguendo standard gli internazionali di sicurezza per lo sviluppo del software per l'esecuzione dei test di sicurezza verso infrastrutture ed asset e seguendo le metodologie **OSSTMM e OWASP**.

Tutti i target esterni al target specificato vengono considerati fuori scope. NON verranno testati i domini di terzo livello (es.: esempio.dominio.it), gli IP e tutti gli altri target esterno a quello fornito..

In particolare, OWASP è utilizzato come standard per identificare e classificare i difetti di sicurezza delle applicazioni e fornire dei risultati universalmente riconosciuti ed utilizzabili da personale tecnico per effettuare le successive attività di rimedio, nonchè per soddisfare i requisiti in termini di penetration testing previsti dai seguenti standard: **ISO/IEC 27001** (ISMS), **ISO 22301** (Business Continuity) e **ISO/IEC 20000** (IT Service Management)

Si precisa che le eventuali vulnerabilità che avrebbero potuto portare a situazioni di DoS (Denial of Service) o DDoS (Distributed Denial of Service), ovvero di interruzioni del servizio, sono state espressamente escluse da questo test. Infatti, questa tipologia di

attacco porta ad esaurire le risorse di un sistema informatico che fornisce un servizio ai client, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio. In tali casi, ci si è limitati a dimostrare la possibilità di sfruttare gli exploit disponibili, ovvero gli errori e le vulnerabilità del sistema testato che possono comportare l'assunzione del controllo di un sistema, la concessione di privilegi di amministratore a un intruso malevolo o l'avvio di attacchi di negazione del servizio (DoS). In effetti, i test condotti dal software AntiHacker sono calibrati in modo da non generare disservizi. Si precisa che il software AntiHacker di CyLock è stato ideato e progettato sulla base dei principi di hacking etico (il c.d. ethical hacking), ovvero con la piena volontà di dare supporto alla Cliente nel superare le vulnerabilità riscontrate, nel più generale fine di creare un ambiente online sicuro e nella considerazione che tutte le evidenze raccolte sono protette da riservatezza e di tutela del dato e dell'informazione. Particolare attenzione é stata fatta al rispetto delle normative relative alla privacy (GDPR, Decreto legislativo 30 giugno 2003, n. 196 e ss.mm.ii.).

Software utilizzato & Copyright

Il software EVA CyLock è stato ideato e progettato dalla Società scrivente, attraverso le più avanzate tecniche di ethical hacking oggi note, **inclusa l'integrazione delle tecniche di machine learning ed intelligenza artificiale** per migliorare l'analisi e il testing dei sistemi analizzati.

Si precisa che, nell'ottica di tutelare gli interessi della Società proprietaria degli asset testati, il report completo è fornito ai clienti CyLock che ne hanno fatto richiesta, in formato confidenziale, esclusivamente dopo aver verificato l'identità del richiedente, in quanto contiene informazioni sensibili sullo stato dei sistemi informatici analizzati.

Ogni contenuto presente in questo documento è da intendersi integralmente protetto dai diritti di proprietà intellettuale, in conformità alla normativa vigente in materia di tutela del diritto d'autore.

CyLock™
CYBERSECURITY CLICK&PLAY

I test che abbiamo effettuato

Surface Analysis

Enumerazione degli asset, mappando gli access point del target indicato (es. 65K porte, dir, file, servizi attivi)

Exploitation

Tutte le vulnerabilità sono verificate e testate solo se necessario (es., LFI/RFI, SQLi, XSS)

Encryption test

Analisi delle impostazioni di crittografia e delle vulnerabilità presenti (es. Lucky13, Sweet32, Poodle, Beast)

Configurations test

Verifica delle impostazioni di accesso e autenticazione dei servizi testati (es. Accesso anonimo, git, Bruteforce, Obsolete OS)

OWASP checklist

Sono eseguiti tutti i test previsti dal framework ad eccezione di quelli che possono compromettere l'operatività del target

Metodologia OSSTMM

Esecuzione dell'EVA seguendo gli elementi cardine del framework, dalla posture review integrato con la metodologia PTES per una migliore riuscita.

Le nostre certificazioni

eLearnSecurity Certified Professional Penetration Tester v2 — eCPPT v2

SECURITY CERTIFICATION — MAS — OPSEC SECURITY EDUCATION

eLearnSecurity Web application Penetration Tester — eWPT

CISM Certified Information Security Manager — An ISACA® Certification

Certified Information Privacy Professional/Europe — CIPP — E — iapp

I nostri partner

Socio Clusit — Associazione Italiana per la Sicurezza Informatica

LVenture GROUP

cdp

STARTUP WISE GUYS

Google Cloud for Startups