SMB通信監視装置

Server Message Block Log Sensor
説明資料

Direx JAPAN DIREX CORPORATION | 日本ダイレックス株式会社

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

目次

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

1. 日本ダイレックスについて

日本ダイレックスは、未知への探究と創造をつづけるネットワーク・システム・インテグレータです。

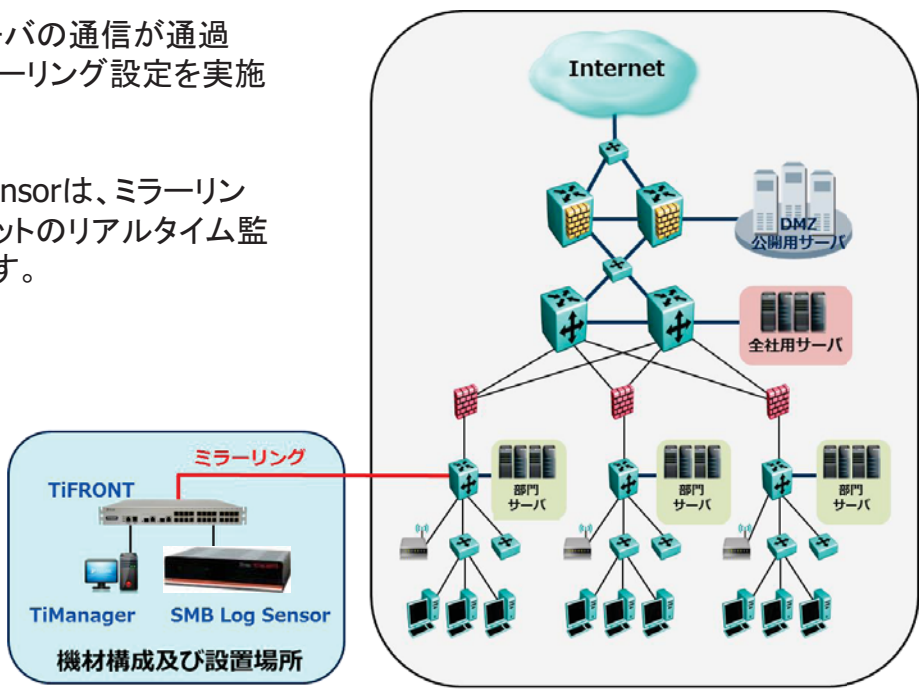
創業以来培ってきた帯域制御技術・計測技術・セキュリティ技術により、レガシー系からオープン系まで、セキュアで最適な情報通信ネットワークシステムの設計・構築・運用サービスを提供しております。

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

2. 接続構成図1

監視対象サーバの通信が通過するSWにミラーリング設定を実施します。

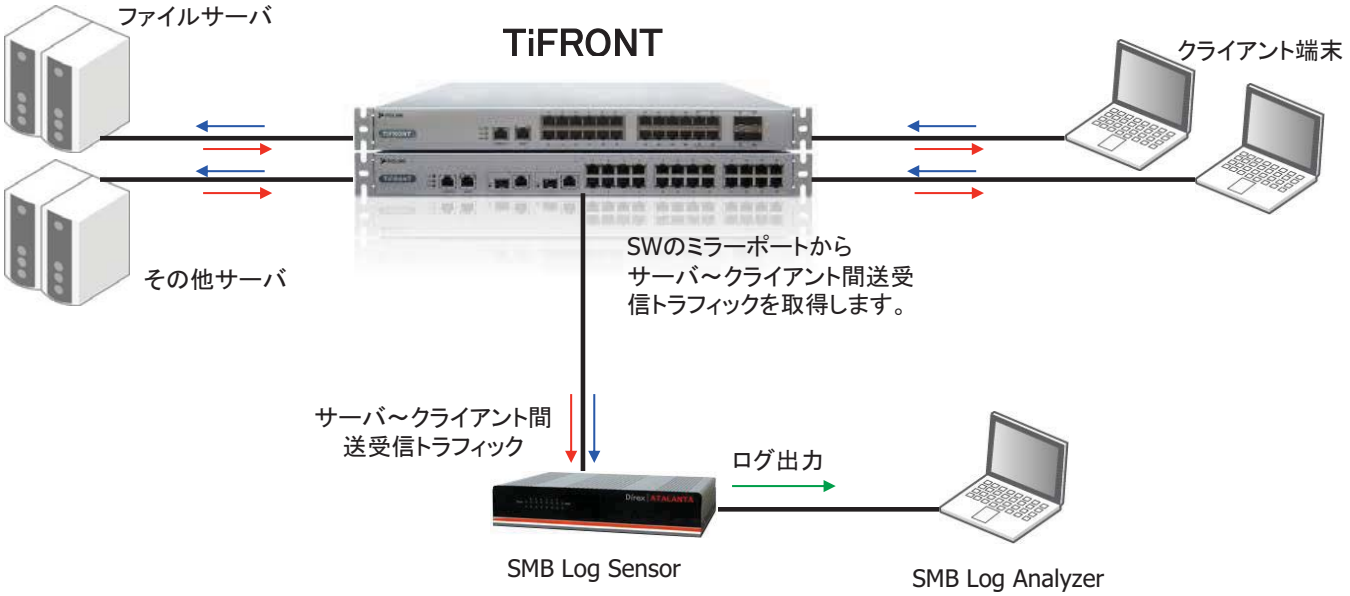
SMB　LOG Sensorは、ミラーリングされたパケットのリアルタイム監視を実施します。



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

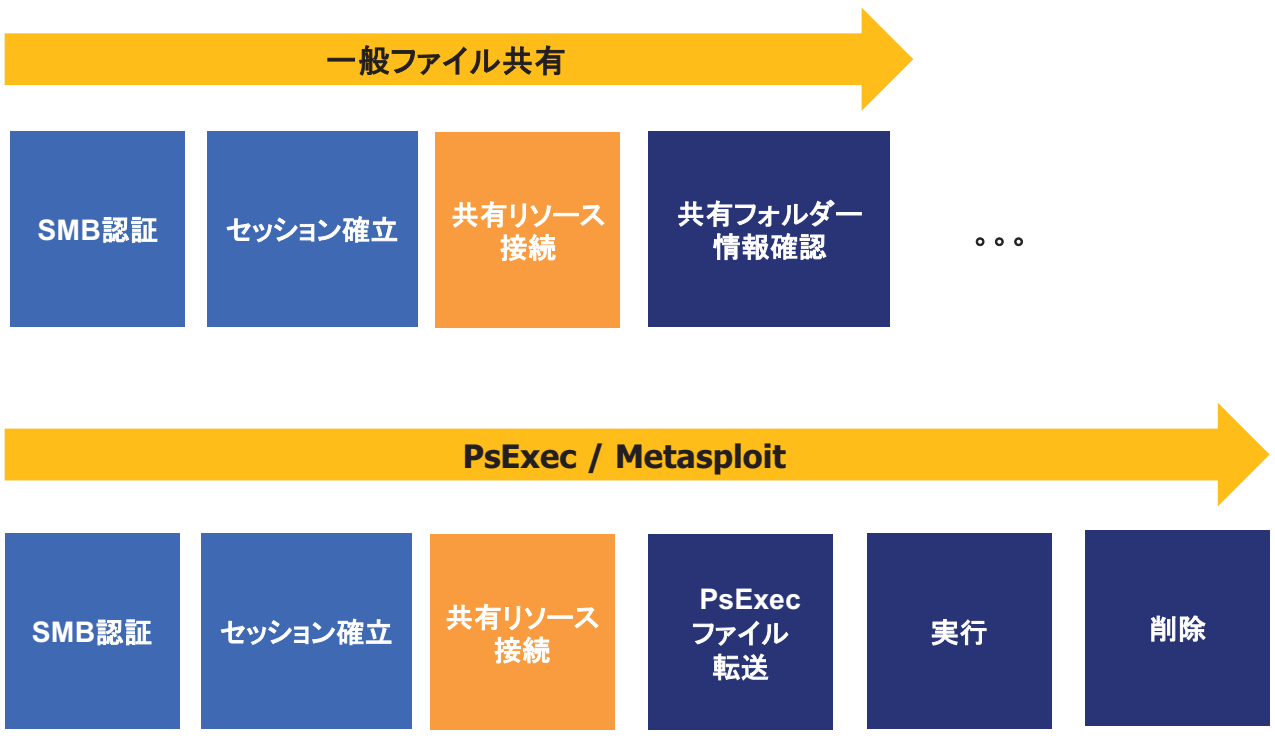
2. 接続構成図2

監視対象サーバ～クライアント間にTiFRONT SWを設置してSMB LOG Sensorでリアルタイム監視を実施することもできます。



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

3. SMB通信フロー



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

4. SMB Log Sensorが監視する内容

SMB Log Sensorは、Windowsファイル共有の通信（SMB通信）の中で
リモートから端末を操作する可能性の高い

①管理者権限（ADMIN＄）でのアクセス
②実行ファイルの転送（*.exeファイル）

を抜き出してリアルタイムに監視します。

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

5. SMB Log Sensorの機能概要 1

5．1　SMB Log Sensorの提供機能（処理内容）

① サーバ/クライアント 双方からSMBパケットを取得
② TCPヘッダ解析
③ NetBIOSヘッダ解析
④ SMBヘッダ解析
⑤ SMBセッションを管理テーブルに登録
⑥ セッション終了後、管理テーブルから削除
⑦ ログ対象となるSMBセッションの内容を、
　管理テーブルから抽出しログを生成
⑧ ログを一旦、メモリ上に保存
⑨ 指定したタイミングでメモリ上のログを、ファイルに保存し転送する

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

5. SMB Log Sensorの機能概要 2

5. 2 監視対象と項目

① 監視対象
- ・SMB 1.0を監視対象とします
- ・TCP ポート番号 445及び 135～139を監視対象とします（NetBIOSも含みます）

② SMB監視項目
- ・SMBのコマンドを対象にSMBシーケンスを監視します。
- ・同一のUIDでSMBセッションを管理します。
- ・SMBセッションで以下のSMBコマンドを管理情報とします。

Session Setup AndX （0x73） → UserName取得
Tree Connect AndX （0x75）
NT Create AndX （0xA2）
Open AndX（0x2D）
Logoff AndX （0x74）

Logoff が無い場合は、コネクション開放または無通信開放で管理します。
UserNameはSession Setup AndXのSecurityBlobから取得します。

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

5. SMB Log Sensorの機能概要 3

5. 3 ログの内容と形式

ログ管理
以下のSMBコマンドからSMBセッションをメモリー上にログとして記録します。

- ・ Tree Connect AndX （0x75） ADMIN＄のみ
- ・ NT Create AndX （0xA2） / Open AndX（0x2D） ＊.exeのみ

- ・ログのフォーマットは、テキスト、カンマ区切りとします。
- ・ログ生成時点で取得できないデータに関しては －（ハイフン）にします。

DATE,TIME,SRC-IP,SRC-PORT,DST-IP,DST-PORT,command, PID, UID, FID,UserName, ADMIN$,PathName改行

例
TreeConnect AndX （0x75）
① 2013/10/01,10:00:00,192.168.0.1,4000,192.168.0.2,455,0x75,12345,23456,-,Direx, ¥¥192.168.0.2¥ADMIN$,-

NT Create AndX （0xA2）
② 2013/10/01,10:00:00,192.168.0.1,4000,192.168.0.2,455,0xA2,12345,23456,0x4000,Direx,¥¥192.168.0.2¥ADMIN$,¥PSEXESVC. EXE

Tree Connect AndXにADMIN$があり、NT Create AndXに *.exeが有るときは、①と②をログに記録します。
Tree Connect AndXにADMIN$があり、NT Create AndXに *.exeが無いときは、①をログに記録します。

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

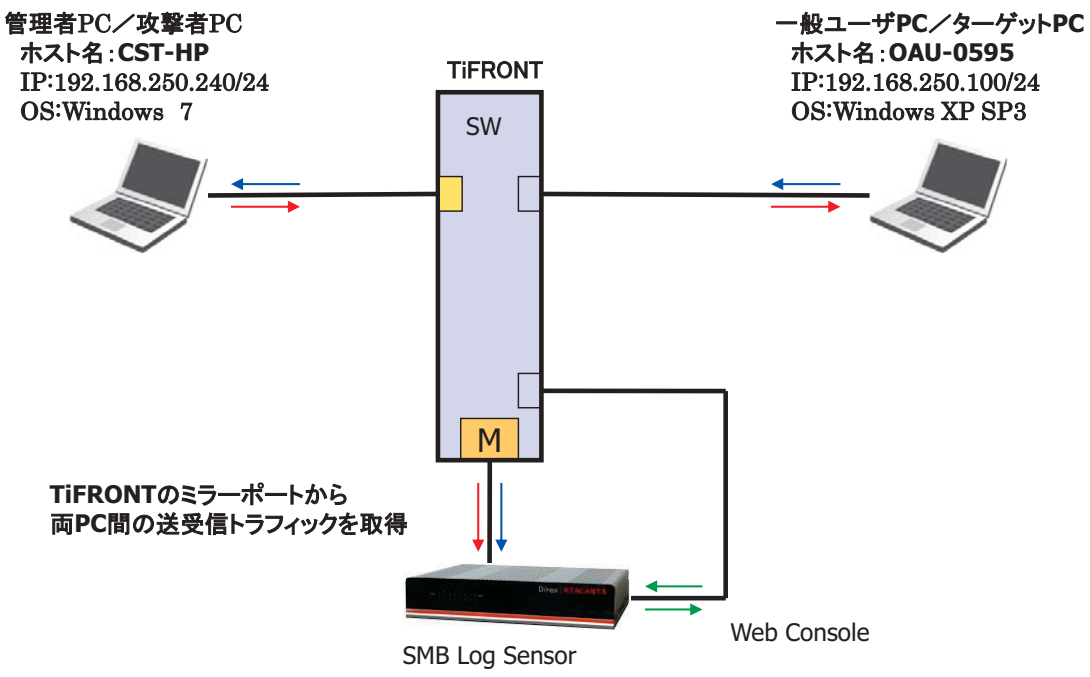
6. デモ概要

1. デモ①
   - 仮説：正規の管理者が正規のツールを使ってリモートアクセス
   - PsExecでリモート接続し、任意のコマンドを実行

2. デモ②
   - 仮説：攻撃者が攻撃用ツールを使ってリモートアクセス
   - Metasploit FrameworkのExploit ModuleであるPsExecで攻撃
   - reverse_tcpにてリモート接続
   - Meterpreterにて情報を盗む

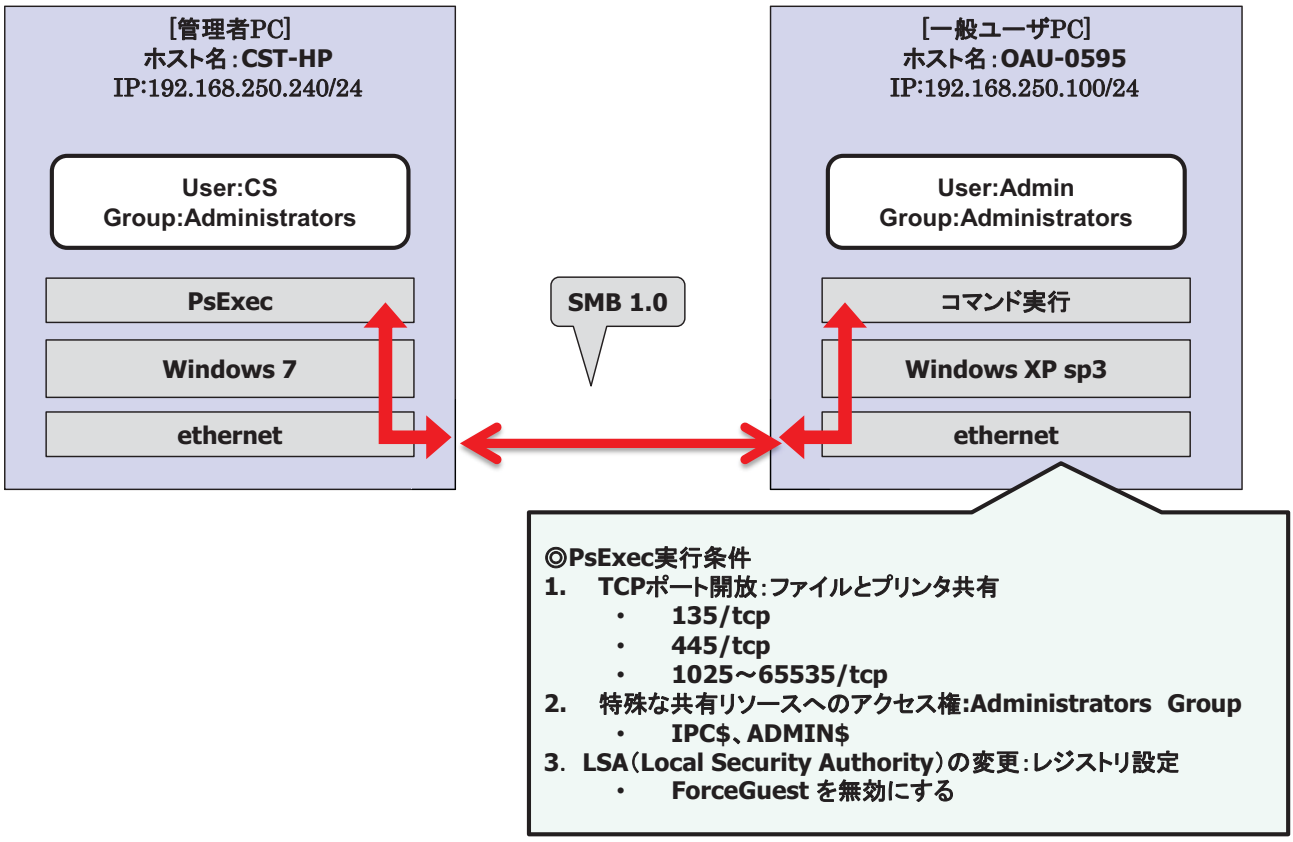
ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

6. 1 デモ環境：接続構成図



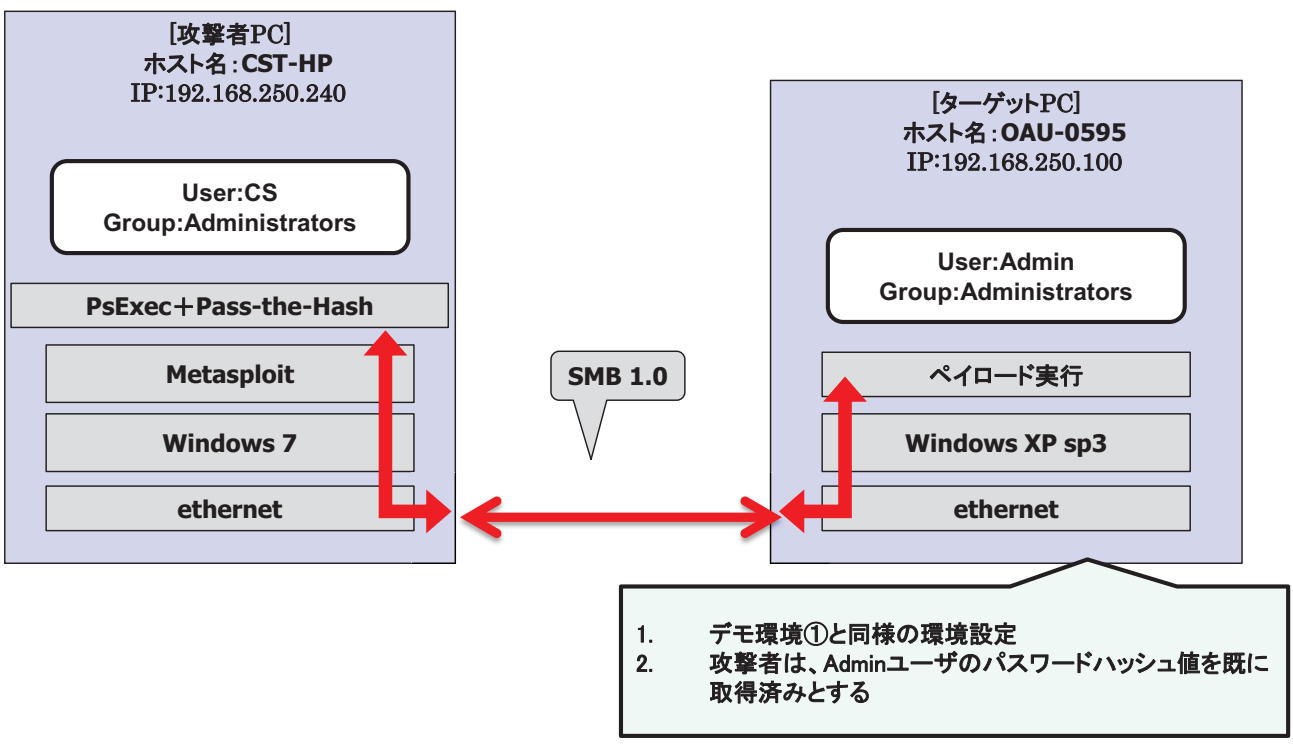
ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

6．2　デモ①　PsExecにてコマンド実行



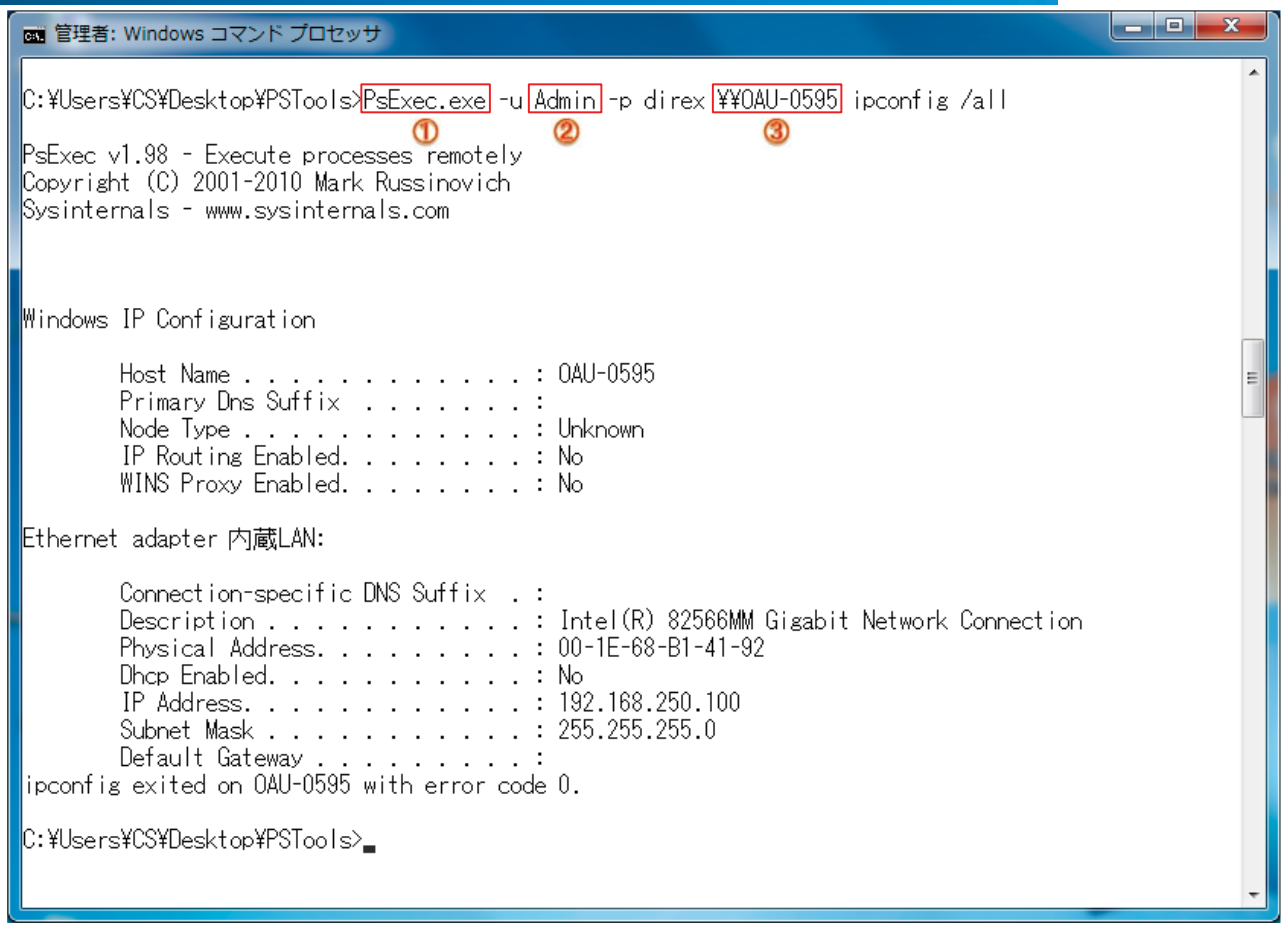
ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

6．3　デモ②　Metasploit：PsExec＋Pass-the-Hashにてペイロード実行



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

PsExecにてコマンド実行したときの管理者PCの画面表示



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

PsExecにてコマンド実行した時のSMB　Log Sensorのログ表示

cEQ 3.5 SMB Log情報 [file:smb_log_001_2014041013.txt]

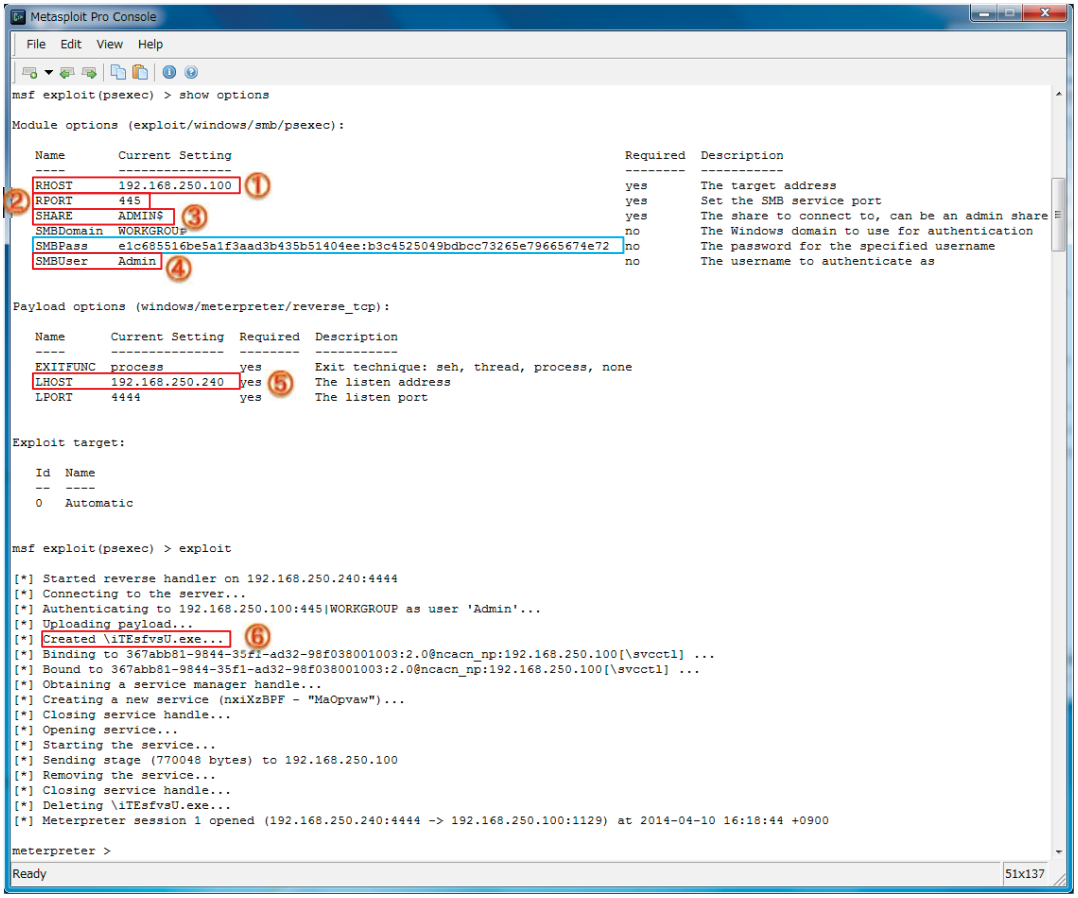
No	日付	時刻	アドレスA	ポートA	アドレスB	ポートB	SMBコマンド	PID	UID	FID	ユーザ名	共有名	実行ファイル名
1	2014/04/10	13:24:21	192.168.250.100	445	192.168.250.240	43714	0x75	65279	4096	-	Admin	¥¥OAU-0595¥ADMIN$	-
2	2014/04/10	13:24:21	192.168.250.100	445	192.168.250.240	43714	0x75	65279	4096	-	Admin	¥¥OAU-0595¥ADMIN$	-
3	2014/04/10	13:24:21	192.168.250.100	445	192.168.250.240	43714	0xA2	4588	4096	0x8002	Admin	¥¥OAU-0595¥ADMIN$	¥PSEXESVC.EXE
4	2014/04/10	13:24:29	192.168.250.100	445	192.168.250.240	43714	0xA2	4588	4096	0x800c	Admin	¥¥OAU-0595¥ADMIN$	¥PSEXESVC.EXE
5	2014/04/10	13:24:29	192.168.250.100	445	192.168.250.240	43714	0xA2	4588	4096	0x800d	Admin	¥¥OAU-0595¥ADMIN$	¥PSEXESVC.EXE

② ③ ①

4月10日 13時24分11秒

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

Metasploit を使用したPsExec＋Pass-the-Hash攻撃時の攻撃者PCの画面表示



ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

Metasploitを使用したPsExec＋Pass-the-Hash攻撃時のSMB Log Sensorのログ表示

cEQ 3.5 SMB Log情報 [file:smb_log_001_2014041016.txt]

No	日付	時刻	アドレスA	ポートA	アドレスB	ポートB	SMBコマンド	PID	UID	FID	ユーザ名	共有名	実行ファイル名
1	2014/04/10	16:18:47	192.168.250.100	445	192.168.250.240	44718	0x75	61095	6144	-	Admin	¥¥192.168.250.100¥ADMIN$	-
2	2014/04/10	16:18:47	192.168.250.100	445	192.168.250.240	44718	0x2D	61095	6144	0x800e	Admin	¥¥192.168.250.100¥ADMIN$	¥iTEsfvsU.exe
3	2014/04/10	16:19:04	192.168.250.100	445	192.168.250.240	44718	0x2D	61095	6144	0x800f	Admin	¥¥192.168.250.100¥ADMIN$	¥iTEsfvsU.exe
4	2014/04/10	16:19:12	192.168.250.100	445	192.168.250.240	44718	0x75	61095	6144	-	Admin	¥¥192.168.250.100¥ADMIN$	-

① ② ⑤ ④ ③ ⑥

4月10日 16時19分15秒

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION

お問い合わせ

日本ダイレックス株式会社

技術グループ　松尾義司

本社：〒101-0047
東京都千代田区内神田2-5-5 城南ビル

Tel : 03-5207-7160（代表）
Email : sales@direx.com （代表）
URL　http://www.direx.com

ALL Rights Reserved, Copyright JAPAN DIREX COPORATION