別紙.TIPS-1　実習資料

仙台 CTF 2019 セキュリティ技術勉強会 実習

TIPS-1 パケット解析

2019年9月28日

仙台 CTF 推進プロジェクト

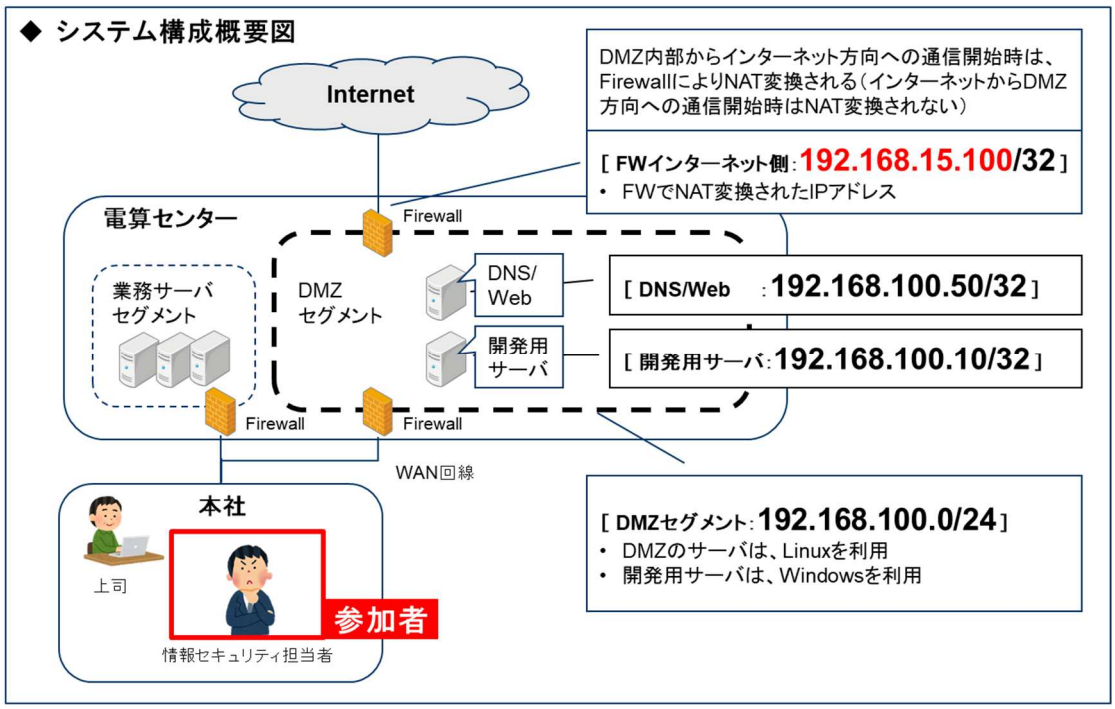
目次

本実習の概要

あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。

とある休日の夜、あなたが自宅で SNS を閲覧していたところ、「うちのサーバが 192.168.15.100 から大量の RDP アクセス受けてる。仙台シーテーエフの IP みたいだけど乗っ取られているのか？とりあえずファイアウォールで遮断しておこう。」と投稿されていることを発見しました。

DMZ のネットワークを流れる通信の記録から、外部に攻撃しているサーバを特定してください。



［補足情報］

・　8 月 25 日　22:36:16～22:36:37 の 21 秒間のキャプチャデータです。

・　攻撃がすでに始まっており、攻撃の一部を取得したデータになります。

実習１　パケット解析

実習内容

DMZ のネットワークを流れる通信の記録から、外部に攻撃しているサーバを特定してください。

① 仙台シーテーエフのサーバと相互に通信を行っている、仙台シーテーエフの管理外のサーバの IP アドレス

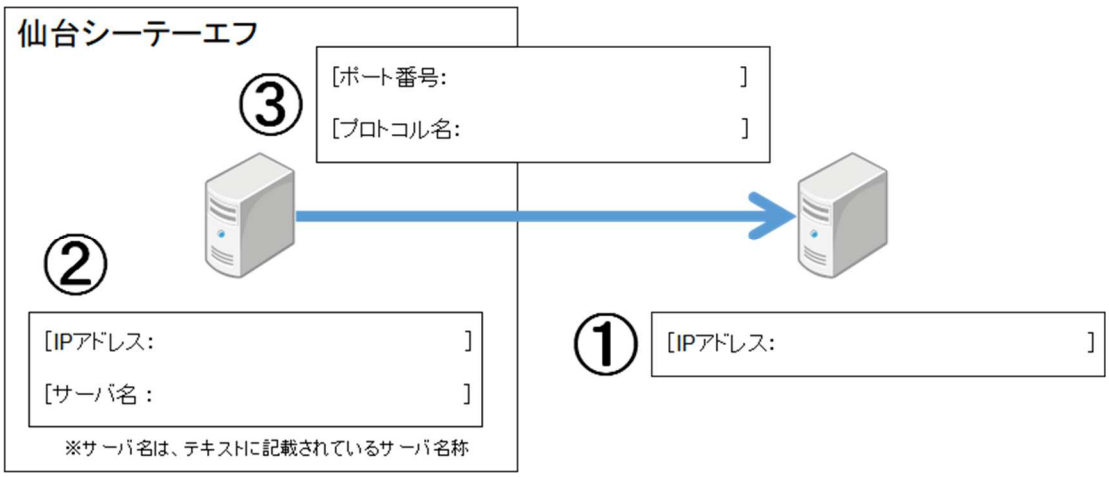
② ①の通信を行っている仙台シーテーエフのサーバの IP アドレス

③ ②のサーバの通信先(Destination)のポート番号とプロトコル名（推測）

[実習用データ]
実習用仮想マシンに格納してあります。

フォルダ　：　/var/samba/public/tips1
ファイル　：　pcap_dmz.pcap

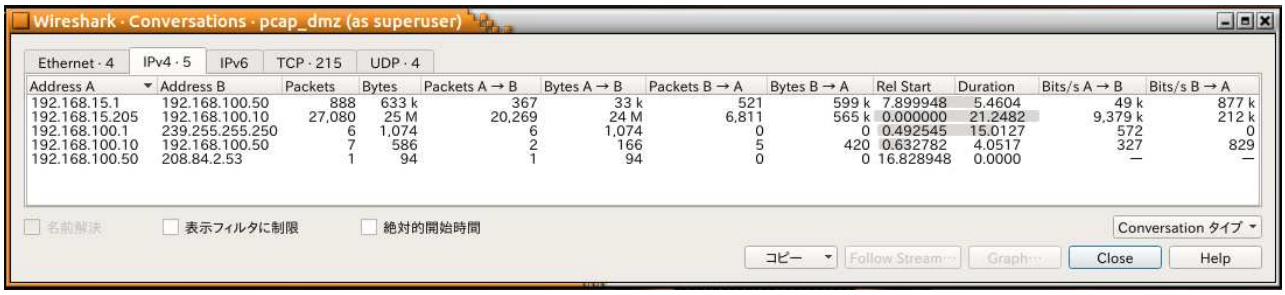
回答記入欄



実習1の解説

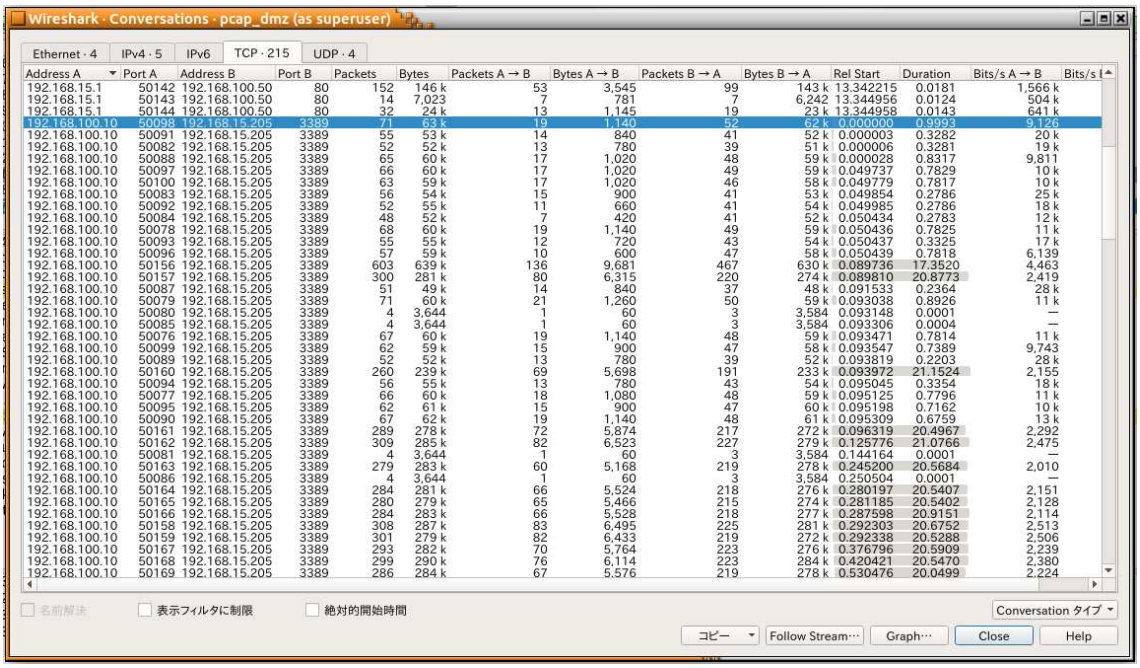
wireshark を利用して解析します。

1. 実習用仮想マシンを起動します。
2. wireshark を起動します。
3. メニューバー「ファイル」->「開く」を選択し、ファイル選択画面からキャプチャしたファイル「/var/samba/public/tips1/pcap_dmz.pcap」を選択し、「Open」ボタンを押します。
4. メニューバー「統計」->「対話」を選択します。「IPv4」タブを参照します。仙台シーテーエフの管理外の IP アドレスで相互に通信を行っているのは2行目の「Address A: 192.168.15.205」であることが分かります。そして、「Address A: 192.168.15.205」と通信しているのは「Address B: 192.168.100.10」です。テキストの「株式会社仙台シーテーエフ」のシステム構成から、「192.168.100.10」は、「開発用サーバ」です。



IP アドレス	説明
192.168.15.1	仙台シーテーエフのウェブサーバにアクセスしたお客様の機器の IP アドレス
192.168.15.205	仙台シーテーエフ 開発用サーバから攻撃を受けているサーバ
192.168.100.10	仙台シーテーエフ 開発用サーバ
192.168.100.50	仙台シーテーエフ DNS/Web サーバ
239.255.255.255	UPnP でデバイス検索を行うためのメッセージ(M-SEARCH)で使われるブロードキャストアドレス。UPnP とは、Universal Plug and Play(ユニバーサル プラグ アンド プレイ)の略です。
208.84.2.53	マイクロソフトの「ネットワーク接続インジケーター Network Connection Status Indicator」(NCSI)と呼ばれる機能で、いくつかの接続テストを行ってインターネット接続の有無を判定しています。そのうちのひとつである「www.msftconnecttest.com」の IP アドレスが「208.84.2.53」です。

5. 同じウインドウで「TCP」タブを参照します。下にスクロールすると「Address A: 192.168.100.10(開発用サーバ)」「Address B: 192.168.15.205(攻撃対象)」の組み合わせのデータが表示されます。



192.168.100.10（開発用サーバ）のポート番号は5万番台が多数ありますが、192.168.15.205（攻撃対象）のポート番号は「3389」固定であることがわかります。これは、通信を最初に受ける側（通常はサーバ）が 192.168.15.205（攻撃対象）であることを示しています。また、「3389」はリモートデスクトップサービス（RDP）の待ち受けポートの標準番号です。

上記から、192.168.100.10（開発用サーバ）がリモートデスクトッププロトコルを用いて外部に攻撃を行っていることが推察できます。

以上で演習は終了です。お疲れさまでした。

回答例