

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

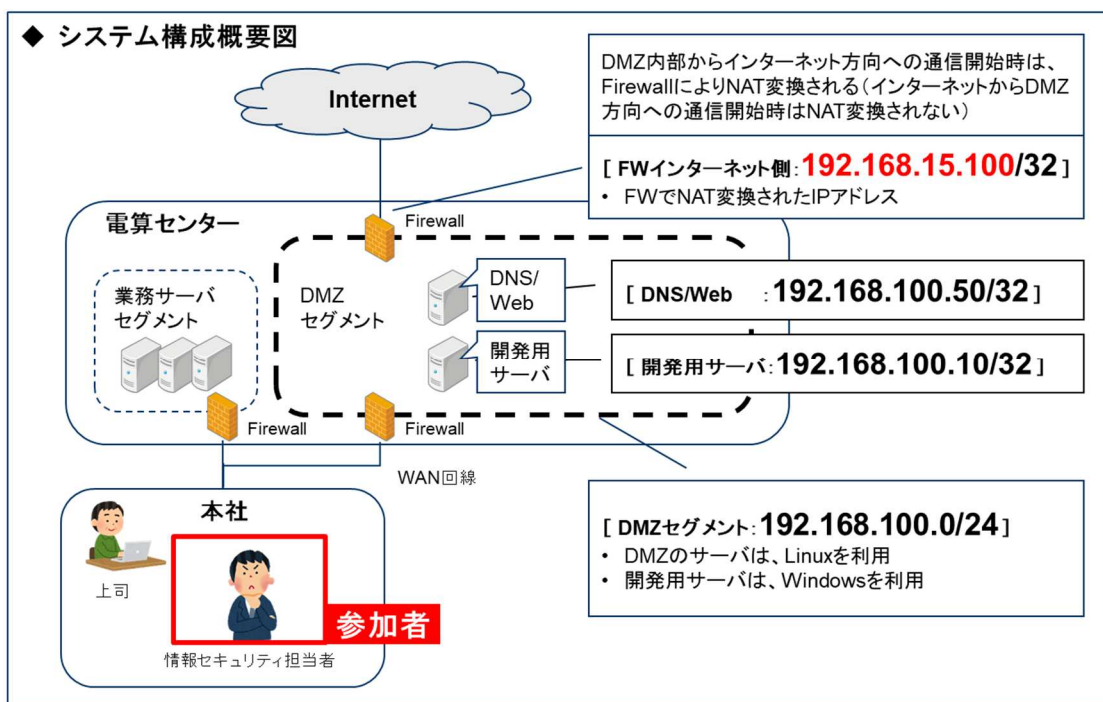
本実習の概要.....	1
実習1パケット解析.....	2
実習1の解説.....	3

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 みただけで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。

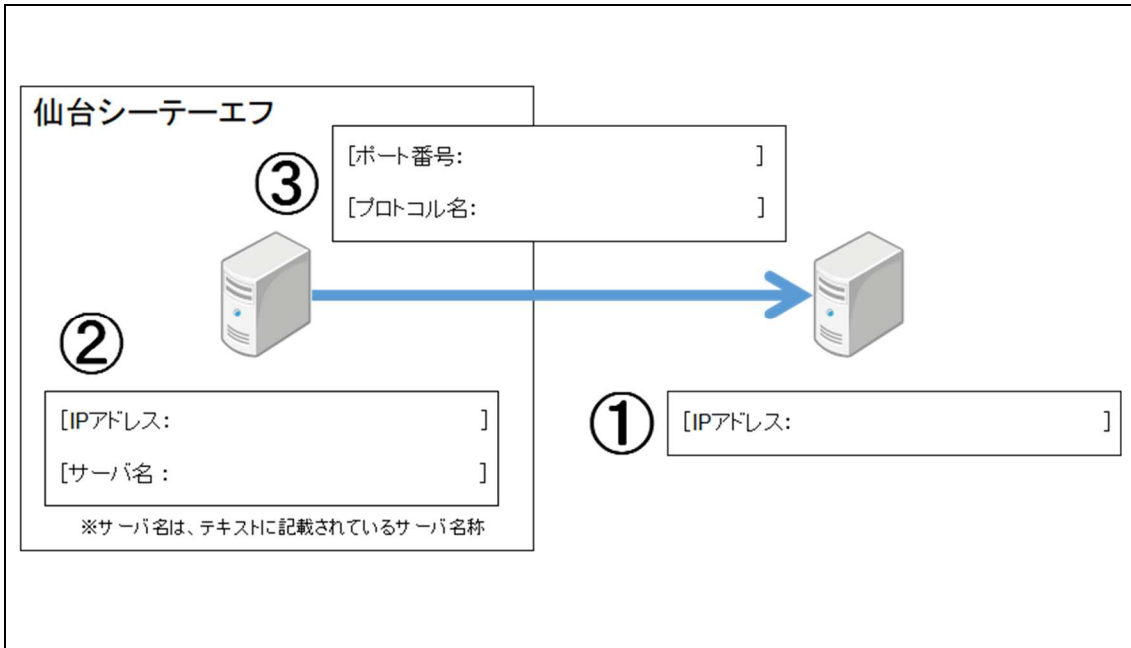
- ① 仙台シーテエフのサーバと相互に通信を行っている、仙台シーテエフの管理外のサーバの IP アドレス
- ② ①の通信を行っている仙台シーテエフのサーバの IP アドレス
- ③ ②のサーバの通信先(Destination)のポート番号とプロトコル名(推測)

[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。

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.15.1	192.168.100.50	888	633 k	367	33 k	521	599 k	7.899948	5.4604	49 k	877 k
192.168.15.205	192.168.100.10	27,080	25 M	20,269	24 M	6,811	565 k	0.000000	21.2482	9,379 k	212 k
192.168.100.1	239.255.255.250	6	1,074	6	1,074	0	0	0.492545	15.0127	572	0
192.168.100.10	192.168.100.50	7	586	2	166	5	420	0.632782	4.0517	327	829
192.168.100.50	208.84.2.53	1	94	1	94	0	0	16.828948	0.0000	—	—

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 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. 同じウィンドウで「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。

Wireshark - Conversations - pcap_dmz (as superuser)

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.15.1	50142	192.168.100.50	80	152	146 k	53	3,545	99	143 k	13.342215	0.0181	1,566 k	—
192.168.15.1	50143	192.168.100.50	80	14	7,023	7	781	7	6,242	13.344956	0.0124	504 k	—
192.168.15.1	50144	192.168.100.50	80	32	24 k	13	1,145	19	23 k	13.344958	0.0143	641 k	—
192.168.100.10	50092	192.168.15.205	3389	71	63 k	19	1,120	52	52 k	0.000000	0.9595	917 k	—
192.168.100.10	50091	192.168.15.205	3389	55	53 k	14	840	41	52 k	0.000003	0.3282	20 k	—
192.168.100.10	50082	192.168.15.205	3389	52	52 k	13	780	39	51 k	0.000006	0.3281	19 k	—
192.168.100.10	50088	192.168.15.205	3389	65	60 k	17	1,020	48	59 k	0.000028	0.8317	9,811	—
192.168.100.10	50097	192.168.15.205	3389	66	60 k	17	1,020	49	58 k	0.049737	0.7829	10 k	—
192.168.100.10	50100	192.168.15.205	3389	63	59 k	17	1,020	46	58 k	0.049779	0.7817	10 k	—
192.168.100.10	50083	192.168.15.205	3389	56	54 k	15	900	41	53 k	0.049854	0.2786	25 k	—
192.168.100.10	50092	192.168.15.205	3389	52	55 k	11	660	41	54 k	0.049985	0.2786	18 k	—
192.168.100.10	50084	192.168.15.205	3389	48	52 k	7	420	41	52 k	0.050434	0.2783	12 k	—
192.168.100.10	50078	192.168.15.205	3389	68	60 k	19	1,140	49	59 k	0.050436	0.7825	11 k	—
192.168.100.10	50093	192.168.15.205	3389	55	55 k	12	720	43	54 k	0.050437	0.3325	17 k	—
192.168.100.10	50096	192.168.15.205	3389	57	59 k	10	600	47	58 k	0.050439	0.7818	6,139	—
192.168.100.10	50156	192.168.15.205	3389	603	639 k	136	9,681	467	630 k	0.089736	17.3520	4,463	—
192.168.100.10	50157	192.168.15.205	3389	300	281 k	80	6,315	220	274 k	0.089810	20.8773	2,419	—
192.168.100.10	50087	192.168.15.205	3389	51	49 k	14	840	37	48 k	0.091533	0.2364	28 k	—
192.168.100.10	50079	192.168.15.205	3389	71	60 k	21	1,260	50	59 k	0.093038	0.8926	11 k	—
192.168.100.10	50080	192.168.15.205	3389	4	3,644	1	60	3	3,584	0.093148	0.0001	—	—
192.168.100.10	50085	192.168.15.205	3389	4	3,644	1	60	3	3,584	0.093306	0.0004	—	—
192.168.100.10	50076	192.168.15.205	3389	67	60 k	19	1,140	48	59 k	0.093471	0.7814	11 k	—
192.168.100.10	50099	192.168.15.205	3389	62	59 k	15	900	47	58 k	0.093547	0.7389	9,743	—
192.168.100.10	50089	192.168.15.205	3389	52	52 k	13	780	39	52 k	0.093819	0.2203	28 k	—
192.168.100.10	50160	192.168.15.205	3389	260	239 k	69	5,698	191	233 k	0.093972	21.1524	2,155	—
192.168.100.10	50094	192.168.15.205	3389	56	55 k	13	780	43	54 k	0.095045	0.3354	18 k	—
192.168.100.10	50077	192.168.15.205	3389	66	60 k	18	1,080	48	59 k	0.095125	0.7796	11 k	—
192.168.100.10	50095	192.168.15.205	3389	62	61 k	15	900	47	60 k	0.095198	0.7162	10 k	—
192.168.100.10	50090	192.168.15.205	3389	67	62 k	19	1,140	48	61 k	0.095309	0.6759	13 k	—
192.168.100.10	50161	192.168.15.205	3389	289	278 k	72	5,874	217	272 k	0.096319	20.4967	2,292	—
192.168.100.10	50162	192.168.15.205	3389	309	285 k	82	6,523	227	279 k	0.125776	21.0766	2,475	—
192.168.100.10	50081	192.168.15.205	3389	4	3,644	1	60	3	3,584	0.144164	0.0001	—	—
192.168.100.10	50163	192.168.15.205	3389	279	283 k	80	5,168	219	278 k	0.245200	20.5684	2,010	—
192.168.100.10	50086	192.168.15.205	3389	4	3,644	1	60	3	3,584	0.250504	0.0001	—	—
192.168.100.10	50164	192.168.15.205	3389	284	281 k	66	5,524	218	276 k	0.280197	20.5407	2,151	—
192.168.100.10	50165	192.168.15.205	3389	280	279 k	65	5,466	215	274 k	0.281185	20.5402	2,128	—
192.168.100.10	50166	192.168.15.205	3389	284	283 k	66	5,528	218	277 k	0.287698	20.9151	2,114	—
192.168.100.10	50158	192.168.15.205	3389	308	287 k	83	6,495	225	281 k	0.292303	20.6752	2,513	—
192.168.100.10	50159	192.168.15.205	3389	301	279 k	82	6,433	219	272 k	0.292338	20.5288	2,506	—
192.168.100.10	50167	192.168.15.205	3389	293	282 k	70	5,764	223	276 k	0.376796	20.5909	2,239	—
192.168.100.10	50168	192.168.15.205	3389	299	290 k	76	6,114	223	284 k	0.420421	20.5470	2,380	—
192.168.100.10	50169	192.168.15.205	3389	286	284 k	67	5,576	219	278 k	0.530476	20.0499	2,224	—

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

