

演習手順書

目次

Chapter 0 研修の環境について	4
0.1. 研修で使用するマシンについて	4
Chapter 1 実習 1 スキャン	5
1.1. 【攻撃】 スキャン	5
1.1.1. 稼働サービス、OS の調査	5
1.1.2. 外部からの SSH が利用できることを確認	6
1.2. 【対応】 FW、Web サーバでの対応	8
1.2.1. FW でのログの確認	8
1.2.2. Web サーバでの対応	9
1.2.3. FW での対応	13
1.2.4. 対応後の確認	14
Chapter 2 (オプション) 実習 2 DoS 攻撃	15
2.1. 【攻撃】 DoS 攻撃	15
2.1.1. 事前確認	15
2.1.2. DoS 攻撃 (Slow HTTP DoS 攻撃)	16
2.2. 【対応】 FW、Web サーバでの対応	17
2.2.1. Web サイトへの影響の確認	17
2.2.2. FW でのログの確認	17
2.2.3. Web サーバでの対応	18
2.2.4. 対応後の確認	22
Chapter 3 実習 3 Web 改ざん	23
3.1. 【攻撃】 Web 改ざん	23
3.1.1. 事前確認	23
3.1.2. bash の脆弱性を攻撃	23
3.2. 【対応】 Web サーバでの対応	26
3.2.1. bash のバージョンアップ	26
3.2.2. Web コンテンツの復旧	26
3.2.3. 対応後の確認	27
Chapter 4 (オプション) 実習 4 パスワードクラッキング	28
4.1. 【攻撃】 パスワードクラッキング	28
4.1.1. 事前確認	28
4.1.2. FTP へのパスワードクラッキングの実施	30
4.2. 【対応】 FW、Web サーバでの対応	31
4.2.1. Web サーバでのログの確認	31
4.2.2. FW での対応	32

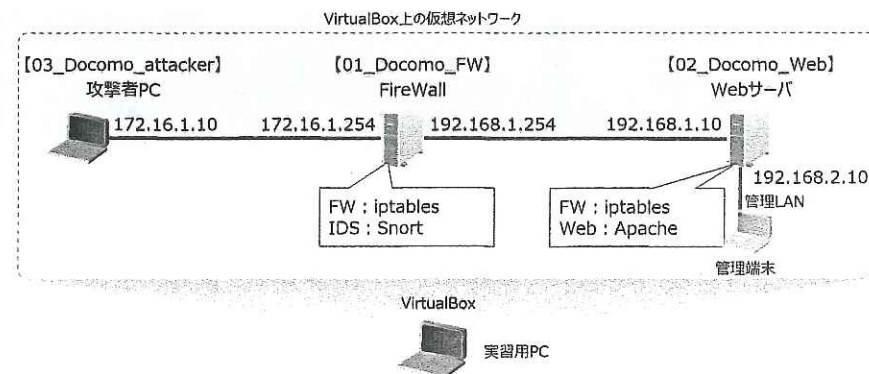
4.2.3. Web サーバでの対応	34
4.2.4. 対応後の確認	36
Chapter 5 (オプションデモ) 実習 5 Web アプリの脆弱性に対する攻撃	37
5.1. 【攻撃】 Web アプリの脆弱性に対する攻撃	37
5.1.1. SQL インジェクション	37
5.1.2. クロスサイトスクリプティング	38
5.1.1. OS コマンドインジェクション	39
Chapter 6 (参考) 性能調査のためコマンドについて	40
6.1. CPU の調査	40
6.1.1. CPU 使用率	40
6.1.2. CPU 待ちプロセス数	40
6.2. メモリの調査	41
6.2.1. 純粋な空きメモリ量	41
6.2.2. スワッピングの発生状況	41
6.2.3. メモリページの統計	42
6.2.4. メモリ、スワップの使用量、空き容量 ※MB 単位	42
6.3. ディスクの調査	43
6.3.1. ディスク負荷率	43
6.3.2. ディスクの容量 (MB 単位)	43
6.3.3. ディレクトリ内のファイル容量 (MB 単位)	44
6.4. ネットワークの調査	44
6.4.1. ネットワークの使用量	44
6.4.2. パケットキャプチャ	44
6.5. プロセスの調査	45
6.5.1. プロセス詳細	45
6.5.2. プロセスのリソース消費状況	45
6.6. 各リソースをまとめて調査	46
6.6.1. sar コマンドによる各リソースの使用状況	46
6.6.1. vmstat コマンドによる各リソースの使用状況	46

Chapter 0

研修の環境について

0.1. 研修で使用するマシンについて

今回の研修で使用するマシンの構成は以下のとおりです。



VM 名	ホスト名	IP アドレス	ユーザ名	パスワード	備考
01_NISA_FW	—	172.16.1.254 192.168.1.254	root	P@ssw0rd	ファイアウォール
02_NISA_Web	www.abchld.com	192.168.1.10 192.168.2.10	root	P@ssw0rd	Web サーバ
03_NISA_attacker	—	172.16.1.10	user	P@ssw0rd	攻撃者 PC