

ペンテスター養成コース ダイジェスト版 (旧 Hacking Expert)

～攻撃者視点で思考できるホワイハッカー養成コース～【2日間】

セキュリティ対策を考える上で、攻撃者の思考や手口に対する理解は欠かせません。近年のサイバー犯罪者によるハッキング行為には、明確な目的があり、考え抜かれた戦略・戦術があります。ターゲットシステムの偵察行為からシステムの脆弱性探索、システムへの侵入、情報探索など、実際のハッキングの手口や技術を実践的な演習を通して学習します。

☑ 研修のゴール

- ・ 攻撃者視点でセキュリティ対策を思考できるようになる
- ・ サイバー攻撃の流れや手口を理解し、説明することができる
- ・ ペネトレーションテストの実施に必要な基礎技術を習得し、対策に活用することができる

☑ 受講対象者

- ・ システム管理者、セキュリティ担当者
- ・ SOC担当者、CSIRT担当者
- ・ 開発エンジニア、製品エンジニア など

☑ 前提知識/望ましいスキルなど

- ・ ネットワークに関する基礎知識
- ・ OS (Windows/Linux) に関する基礎知識
- ・ セキュリティに関する基本用語の理解

☑ 実施アジェンダ

【1日目】

1. はじめに、サイバー犯罪の背景
2. サイバー攻撃の流れ
3. 環境構築 (Setup)
4. 偵察行為 (Information Gathering/OSINT)
5. 状況把握 (1) 発見・スキャン
6. 状況把握 (2) バナーグラブ・列挙
7. 脆弱性調査 (Vulnerability Assessment)
8. ペネトレ計画 (Planning)
9. ペネトレーションテスト (侵入検査 1)
 - ・ Metasploit : サーバサイド、クライアントサイド

【2日目】

- 1 0. 確認演習
- 1 1. ペネトレーションテスト (侵入検査 2)
 - ・ ソーシャルエンジニアリング (Web/メール)
- 1 2. ペネトレーションテスト (影響調査)
 - ・ 権限昇格 : Local Exploit
 - ・ パスワード解析 (ハッシュ解析)
 - ・ ブルートフォース攻撃 (総当たり攻撃)
- 1 3. 報告書 (Reporting)
- 1 4. 総合演習
- 1 5. まとめ、振り返り

☑ 開催要項

- ・ コース名 : ペンテスター養成コース ダイジェスト版 (Hacking Expert)
- ・ 開催日数 : 2日間 (9:30-17:30)
- ・ 実施方法 : オンライン、または、集合研修
- ・ 研修形式 : 座学、実機を使った演習
- ・ 研修費用 : 200,000円 (税別) / 人 (最少催行人数 : 4名)

当社の定期開催は1名様からお申込みいただけます。定期開催の実施スケジュールは、弊社営業へお問い合わせください。また、個別開催も可能です。随時お問い合わせ下さい。



☑ お問い合わせ・お申込み

- ・ ストーンビートセキュリティ株式会社
- ・ TEL 050-6877-5988 メール : training@stonebeat.co.jp
- ・ <https://www.stonebeat.co.jp#training>



Stonebeat Security
Your Trusted Security Advisor

研修テキスト

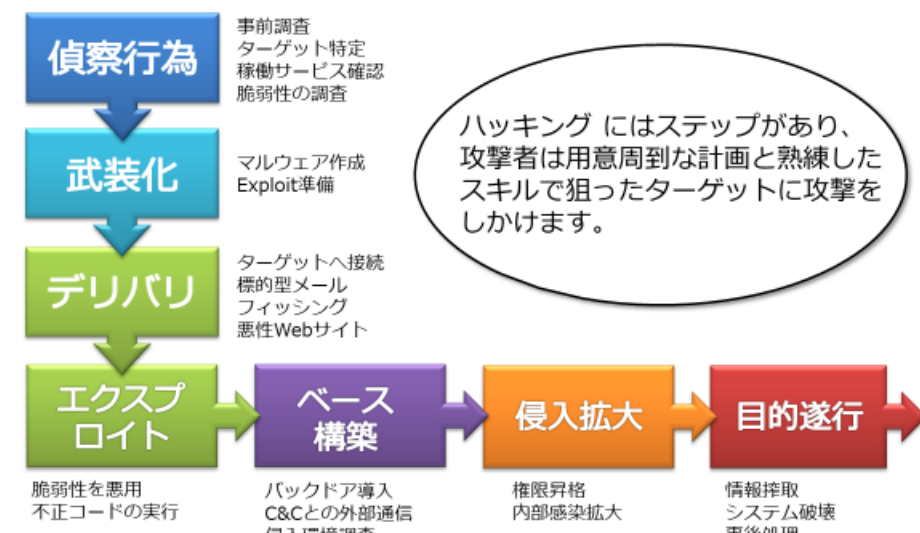
(サンプル)

ハッキングを学ぶ必要性とは？



10

ハッキングのステップ



15

ペネトレーションテストの流れ



- 敵を知る
 - ・組織情報、公開情報、周辺情報 …
 - ・ネットワーク、システム、脆弱性情報 …
 - ・ユーザ情報、アカウント情報 …

1. ターゲットシステムを探す
2. システムの稼働サービス/ポートを調べる
3. 稼働サービスのソフトウェア/バージョンを調べる
4. 脆弱性の有無を調べる
5. 脆弱性を悪用できる攻撃（コード/モジュール等）を確認する
6. 脆弱性を突いてシステムに侵入する

IPアドレス/ OS種別	稼働サービス/ ポート	ソフトウェア/ バージョン	脆弱性の有無	Exploit Code/ Module
192.168.1.1 Ubuntu 8.04	HTTP 80/TCP	Apache httpd 2.2.xx	CVE-XXXX CVE-XXXX	exploit-db.com Metasploit etc.

17

Information Gathering / OSINT

Information Gathering / OSINT

- 攻撃対象とする対象組織に、通信トラフィックを送信せずにターゲットの情報 および その周辺情報、相互関係などを調査し、標的に関する情報を把握することです。

OSINTが必要な理由

- フットプリンティングによって、サイバー犯罪者たちの意図や思考に触れることができます。
- 攻撃者の考え方がわかれば、組織に潜む潜在的なセキュリティ脅威が見えてきます。
- セキュリティ脅威が見えてくると、攻撃者によるサイバー攻撃に対する具体的な対策方法が理解できるようになります。

51

様々な検索の仕方

Google Hacking Database (GHDB)

<https://www.exploit-db.com/google-hacking-database/>



- ・検索例
 - site:co.jp filetype:log
 - site:co.jp "index of" config
 - site:co.jp inurl:wp-includes

Googleを利用した様々な情報検索の仕方が登録されているサイト
自サイトを対象とすることで、情報漏えい等の懸念がないなどの調査に活用

62

偵察行為（情報収集）

Fierce Domain Scan

- DNSへの問い合わせを自動化するPerlのツール（スクリプト）
- Kali Linux にバンドル

1. 対象ドメインのDNSサーバを検索し、クエリ対象に設定
2. 対象ドメインのDNSサーバへゾーン転送を要求
3. 正引きの名前解決に対して、ワードリストを利用してブルートフォースを実施
4. 正引きでレコードが検出されたら、逆引きを 前後 5 IP に対して実行

- 実施例（ドメイン名）：
fierce -dns example.com -wordlist hosts.txt

- 実施例（IPアドレス）：
fierce -range 10.10.10.0-255 -dnsserver ns1.example.com

71

PTF（Penetration Testers Framework）

参考）セットアップ手順 ※全てのモジュールインストールは1時間以上かかります。

```
# git clone https://github.com/trustedsec/ptf.git
# cd ptf
# ./ptf
```

モジュールの表示

```
ptf> show modules
```

全てのモジュールをインストール/アップデートする場合

```
ptf> use modules/install_update_all
```

全てのモジュールをインストール/アップデートする場合

```
ptf > use modules/post-exploitation/john
ptf:(modules/post-exploitation/john)> install
```

91

状況把握：Discover / Scanning

- ターゲットシステムに対して、実際にパケットを送出し、対象システムおよび稼働ポート/サービスを確認します。

- スキャンでは、主に以下項目を確認します。

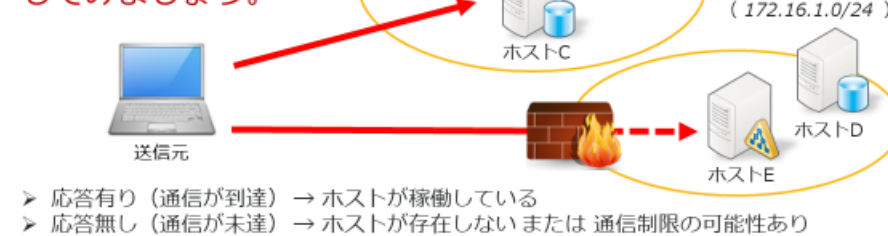
- －ドメイン名（Footprintingで確認済み）
- －IPアドレス/ネットワーク（Footprintingで確認済み）
- －ホストの特定
- －稼働ポート/サービス
- －サービスのバナー情報
- －オペレーティングシステムの推測



94

演習：Nmapコマンドによるホスト探索

ネットワークAとネットワークBへNmapコマンドを実行してみましょう。



- 応答有り（通信が到達）→ ホストが稼働している
- 応答無し（通信が未達）→ ホストが存在しないまたは 通信制限の可能性あり

Nmapコマンドの実行例（ホスト探索）

```
# nmap 192.168.1.0/24 -sP
```

※ -sP オプション：pingスキャン（ホスト発見）のみを実行。ポートスキャンやOS検出などは行わない。

99

稼働ポート/サービスの確認

Nmapによるポートスキャン

➢ 主なスキャンタイプ

1. TCP接続スキャン（-sT）
2. TCP SYNスキャン（-sS）
3. UDP スキャン（-sU）

➢ その他のスキャンタイプ

4. TCP FINスキャン（-sF）
5. TCPクリスマスツリースキャン（-sX）
6. TCP Nullスキャン（-sN）
7. TCP Ackスキャン（-sA）
8. TCPウィンドウスキャン（-sW）
9. TCP RPCスキャン（-sR）



103

ソフトウェア/バージョン、OSの確認

- スキャナでは多くの場合、ポートの開閉がレポートされ、ポートで実行されるサービスなどの基本情報が提供されます。

- 通常、これらは正確な情報ですが、標準外のポートでサービスを実行することもあります。また、攻撃を成功させるためには、OS（プラットフォーム）の確認も必要になります。



プローブを追加して、より詳しい情報を確認してみましょう。

118

（参考）バナーグラブリング / Shodan

Shodan

<https://www.shodan.io/>



システムの オープンポート や接続時に表示する「バナー情報」や「レスポンス（応答）メッセージ」を対象に情報収集する検索エンジン
※無償登録では検索制限あり。

127

脆弱性スキャン

脆弱性スキャナでは、ホストの検出、サービスの検出、バナーグラブリングを組み合わせ、アプリケーションやOSに関連する脆弱性を調べることができます。



132

攻撃モデル：ATT&CK by MITRE

- ATTACK = Adversarial Tactics, Techniques, and Common Knowledge model
- 攻撃者の攻撃手法、戦術を分析して作成されたナレッジベース
- MITRE社が開発、2013年9月より公開
- Post Exploit にターゲットを直したフレームワーク
- <https://attack.mitre.org/>

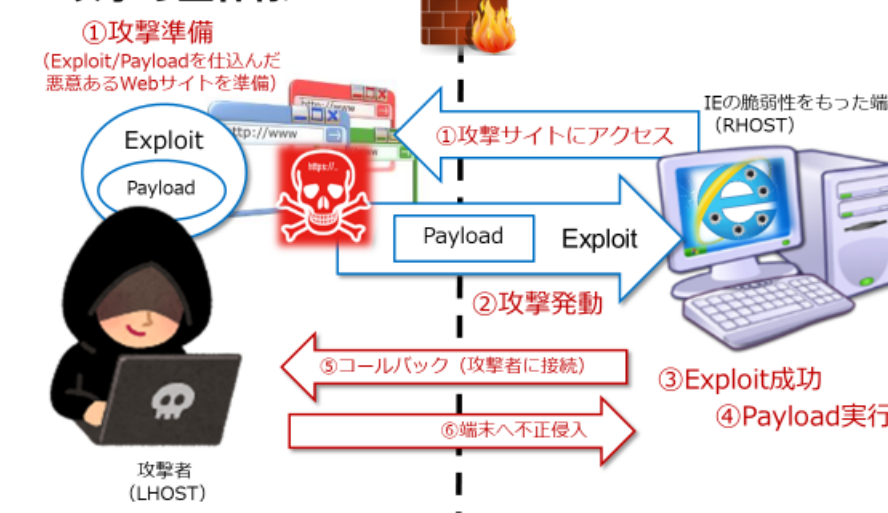


#今知るべきATT&CK | 攻撃者の行動に注目したフレームワーク徹底解説
<https://blogs.mcafee.jp/mitre-attack>

176

演習2：Operation Aurora を悪用

➢ 攻撃の全体像



225