攻撃者視点で学ぶ
サイバー攻撃の対策ポイント

CYBER COMMAND

横濱 悠平（ヨコハマ ユウヘイ）

プログラマー

- web、モバイルアプリやセキュリティツールの開発
- python, rust, php, java, ruby, nextjs
- 多くのプログラマーを育成

セキュリティエンジニア

- 脆弱性診断
- SOCインフラ構築
- セキュリティ人材育成の講師
- 認定ホワイトハッカー（CEH）

C|EH
CERTIFIED ETHICAL HACKER

“　攻撃者視点で学ぶ、サイバー攻撃の対策ポイント”

なぜ、攻撃者視点？？

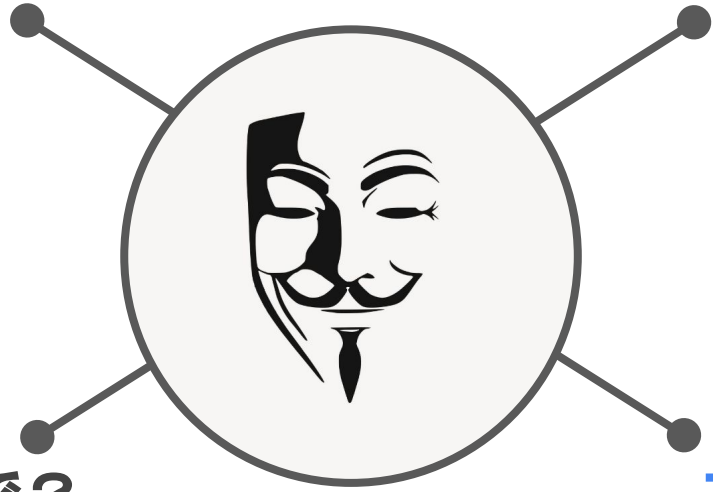
- 実際の攻撃シナリオ
- 守り方の精度
- プロファイリング

情報漏洩やランサムウェアなど様々なサイバー攻撃が取り上げられていますが、このテーマでは攻撃者視点に立って実際に使われているシナリオやパターンを説明しながら守る側の視点を養います。

“プロファイリング”

動機は？

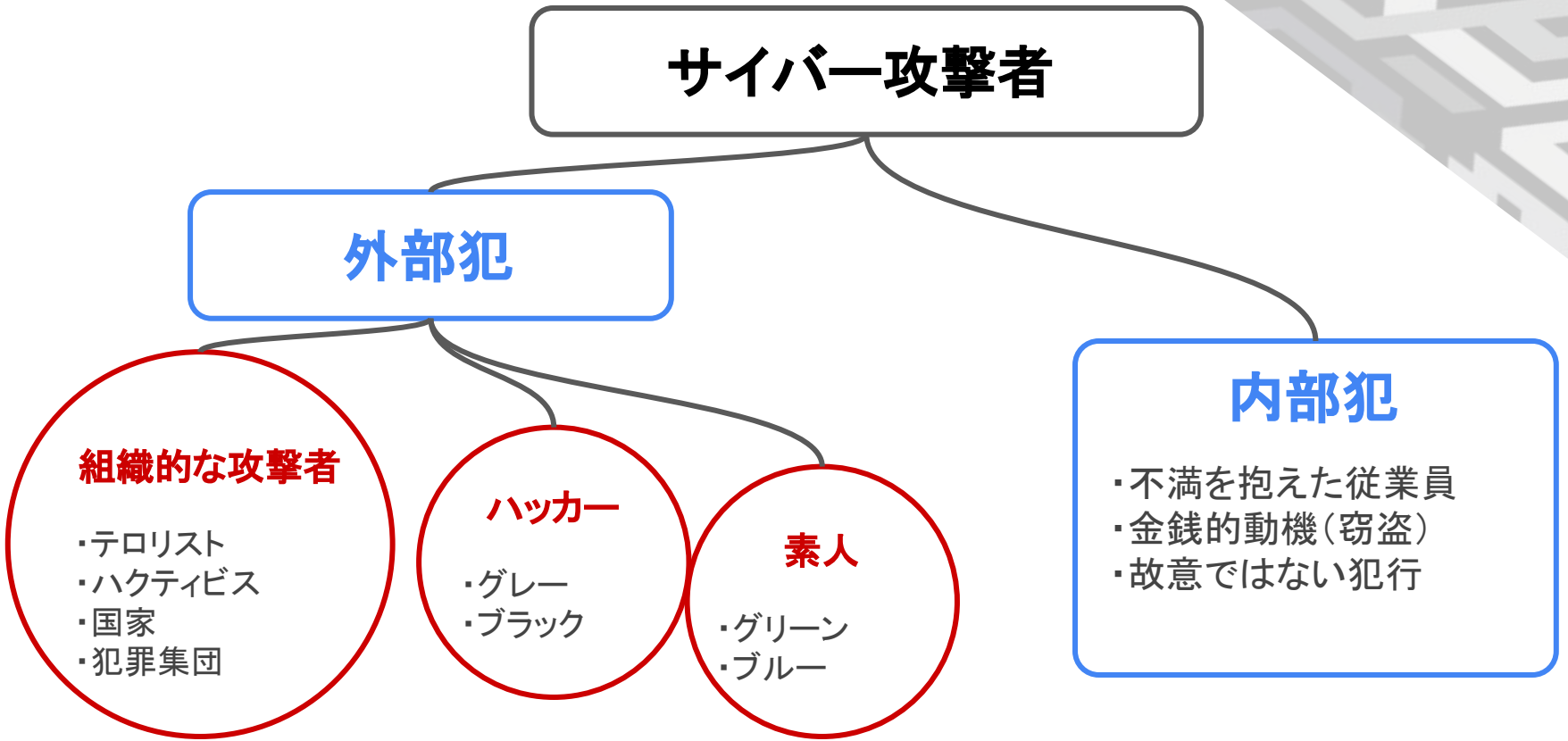
リソースは
どれくらい？



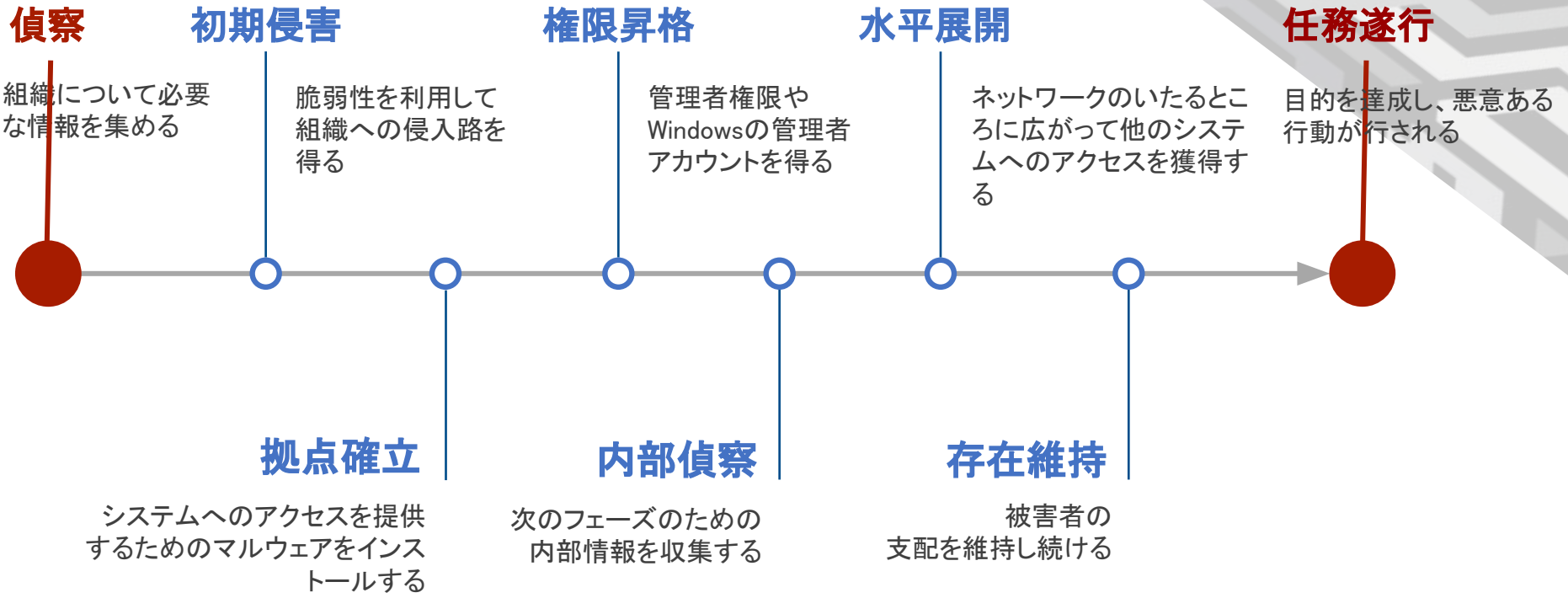
どのぐらいの **時間**で？

プロ意識は高い？

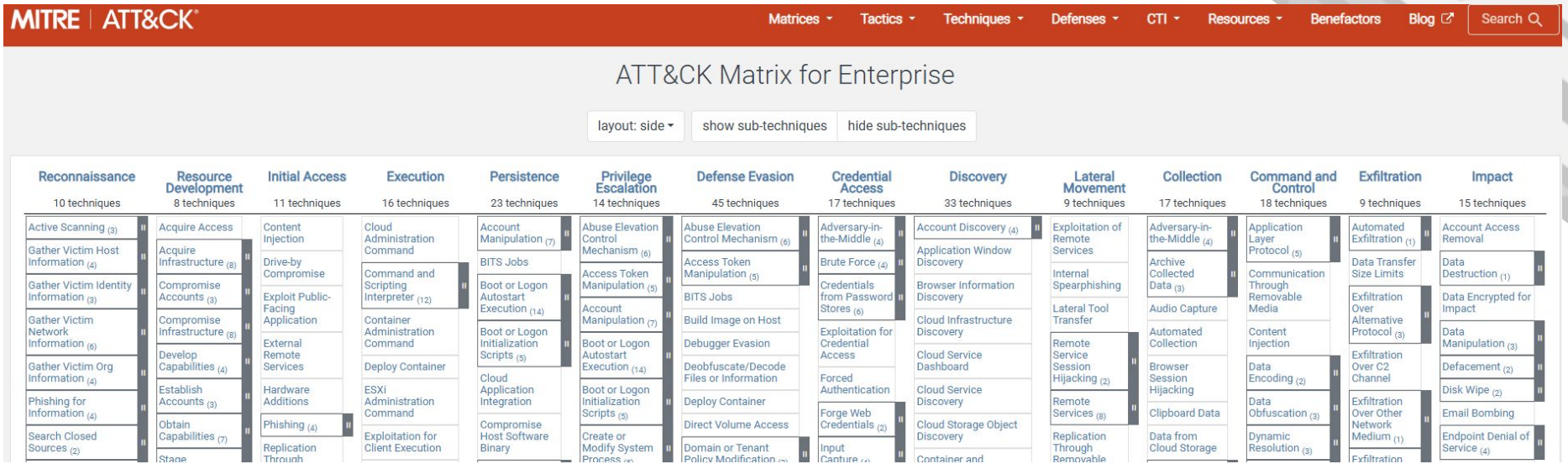
“プロファイリング”


サイバー攻撃者
外部犯
内部犯
組織的な攻撃者
・テロリスト
・ハクティビス
・国家
・犯罪集団
ハッカー
・グレー
・ブラック
素人
・グリーン
・ブルー
・不満を抱えた従業員
・金銭的動機（窃盗）
・故意ではない犯行

APT(Advanced Persistent Threat)



“MITRE”

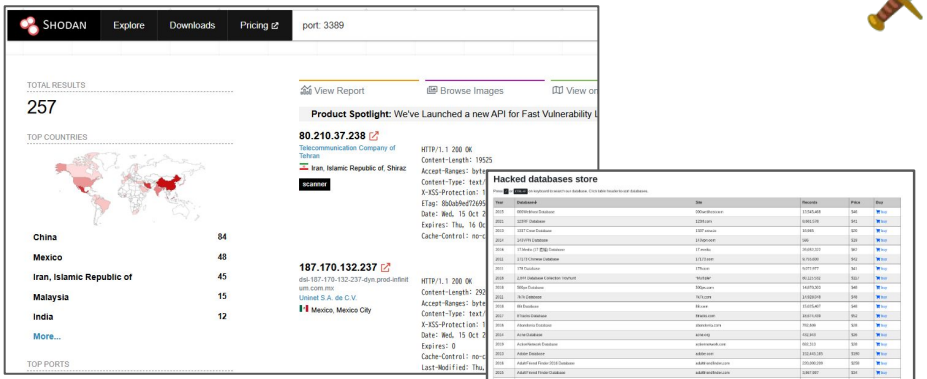

MITRE | ATT&CK
Matrices
Tactics
Techniques
Defenses
CTI
Resources
Benefactors
Blog
Search
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (7)
Initial Access
11 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through
Execution
16 techniques
Cloud Administration Command
Command and Scripting Interpreter (12)
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Persistence
23 techniques
Account Manipulation (7)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Cloud Application Integration
Compromise Host Software Binary
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Account Manipulation (7)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process
Defense Evasion
45 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Credential Access
17 techniques
Adversary-in-the-Middle (4)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture
Discovery
33 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable
Collection
17 techniques
Adversary-in-the-Middle (4)
Archive Collected Data (3)
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Command and Control
18 techniques
Application Layer Protocol (5)
Communication Through Removable Media
Content Injection
Data Encoding (2)
Data Obfuscation (3)
Dynamic Resolution (3)
Exfiltration
9 techniques
Automated Exfiltration (1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (1)
Impact
15 techniques
Account Access Removal
Data Destruction (1)
Data Encrypted for Impact
Data Manipulation (3)
Defacement (2)
Disk Wipe (2)
Email Bombing
Endpoint Denial of Service (4)

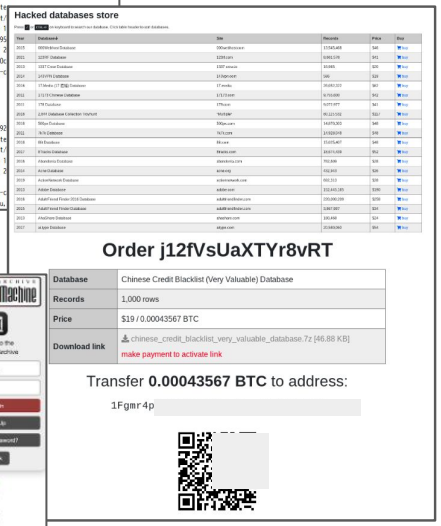
[APTでざっくり版]

ステップ毎の
🎭攻撃者 vs 🛡️防御者
の戦い⚔️

偵察
Recon

攻撃側





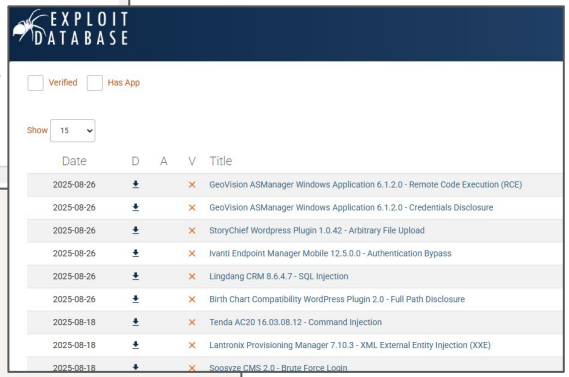
防御側

- 攻撃面の最小化 。公開情報に含める社員情報・公開メール・管理画面などの最小化。
- ダークウェブ上での漏洩監視、クレデンシャル管理 – 流出検知（ID/パスワードのモニタリング）

OSINTサービスを定期的に使う。

初期侵害＆拠点確立
Initial Access

攻撃側




```
import asyncio
import random
import urllib.parse
import sys
import socket
from colorama import init, Fore, Style

init()

class TomcatKiller:
    def __init__(self):
        self.success_count = 0
        self.error_count = 0
        self.invalid_priorities = [
            \\\"u=-1, q=2\\\",
            \\\"u=4294967295, q=-1\\\",
            \\\"u=-2147483648, q=1.5\\\",
            \\\"u=0, q=invalid\\\",
            \\\"u=1/0, q=NaN\\\",
            \\\"u=1, q=2, invalid=param\\\",
            \\\"\\\",
            \\\"u=1, q=1, u=2\\\",
            \\\"u=9999999999999999999, q=0\\\",
```

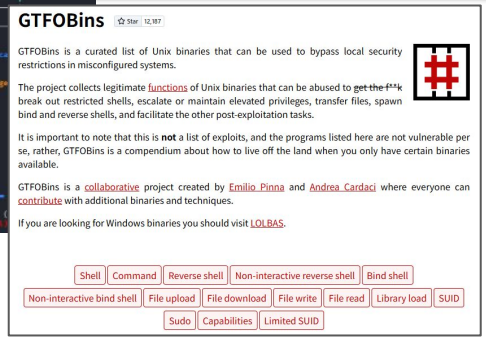
防御側

- 教育、標的型攻撃訓練（定期演習）などの人間的な対策。メールゲート（URL/添付のサンドボックス検査などのシステム的な対策。
- 使用しているクラウドサービスの管理。SGWやCASB等仕組みで。

定期的な診断サービスを利用

権限昇格
Privilege Escalation

攻撃側



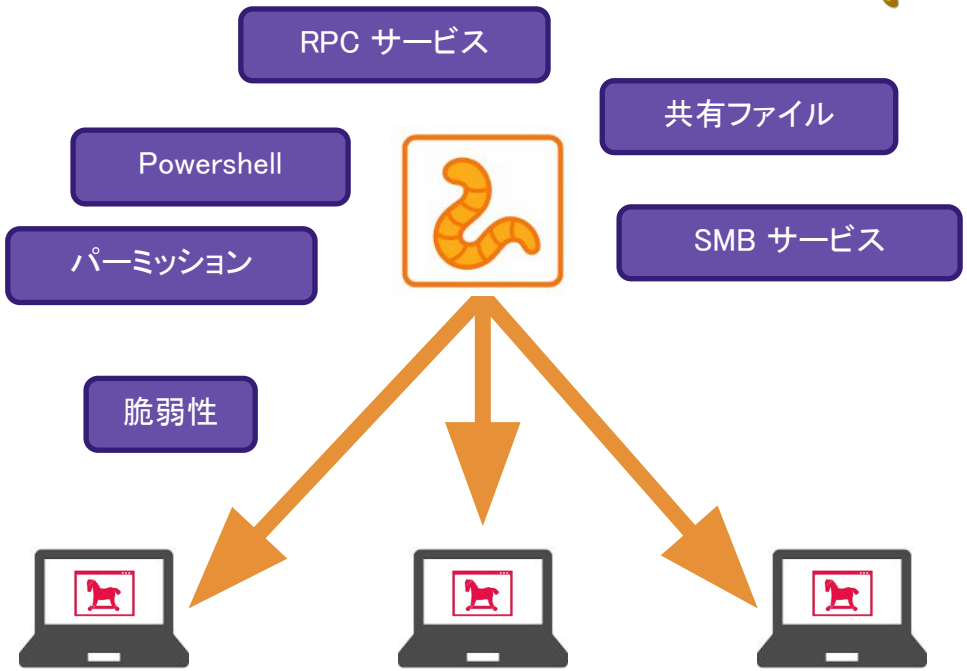
防御側

- 資格情報の防護。パスワードの複雑化。使いまわし禁止。短い有効期間。
- 最小権限化。サービス/アカウントに最小権限を適用。

EDRなどを使用した認証挙動の監視と分離 – ログ監視

内部偵察＆水平展開

攻撃側



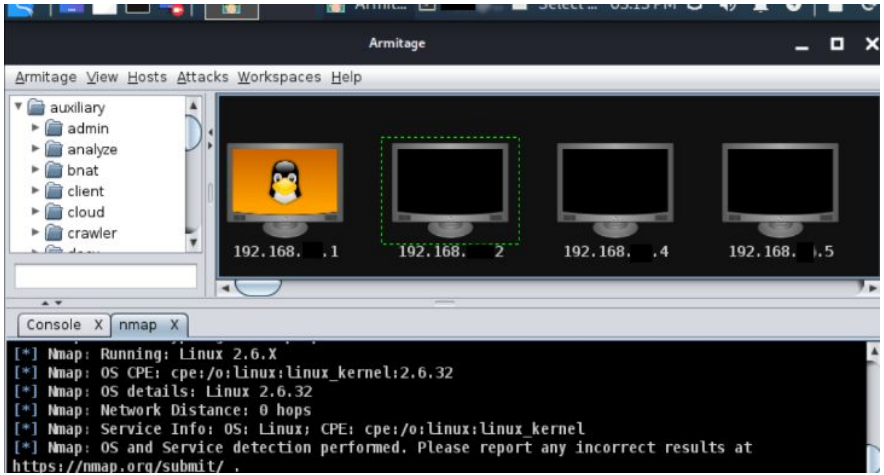
防御側

- ネットワーク分割（マイクロセグメンテーション）。
- 管理プロトコルの制限（RDP/SMBの利用制御・踏み台制限）

EDRで水平展開の挙動検出

永続化

攻撃側



防御側

- システムの構成変更の監視とアラート。解放ポート、常駐プロセス、デーモン、ユーザー等

EDRでシステムの構成変更の検出

目標達成

攻撃側

防御側

- 重要データの把握と不正持ち出しのブロック＆アラート。DLP。
- 通信の監視と異常検知 。大量の転送や不審なエンドポイントへの接続を検知。
- 暗号化バックアップとオフライン保管。

資産とリスクの棚卸とバックアップ。

“チームで守る”

防御側

- SOC（Security Operation Center）
- 専門の外部サービスに任せる
- 何を守るべきか？の大切な資産の棚卸から始める
- まずは一番大切なものから小さく始めていく
- 継続的な社員教育と訓練