



MWS Cup 2020 事前課題

岡山大学 セキュリティ讃歌
市岡, 伊藤, 白石, 大谷, 川島, 芝

目的・動機(1/2)

- 新しい脆弱性やPoCコードが公表されたとき、
実際にサーバを立てて試したい
- 既存のハニーポット
 - 外にハニーポットを公開し、攻撃者から多くの攻撃を受けることでログを収集

第三者からの
攻撃が必要

脆弱性の検証に
時間がかかる

目的・動機(2/2)

●本成果物では、PoCコードや脆弱性を試すことのできる「やられ環境」を気軽に作成

●実際に受けた攻撃や脆弱性に迅速に対応可能

●「やられ環境」への願望

●サーバのバージョンを自由に変更したい

●実環境に近いサーバを構築したい

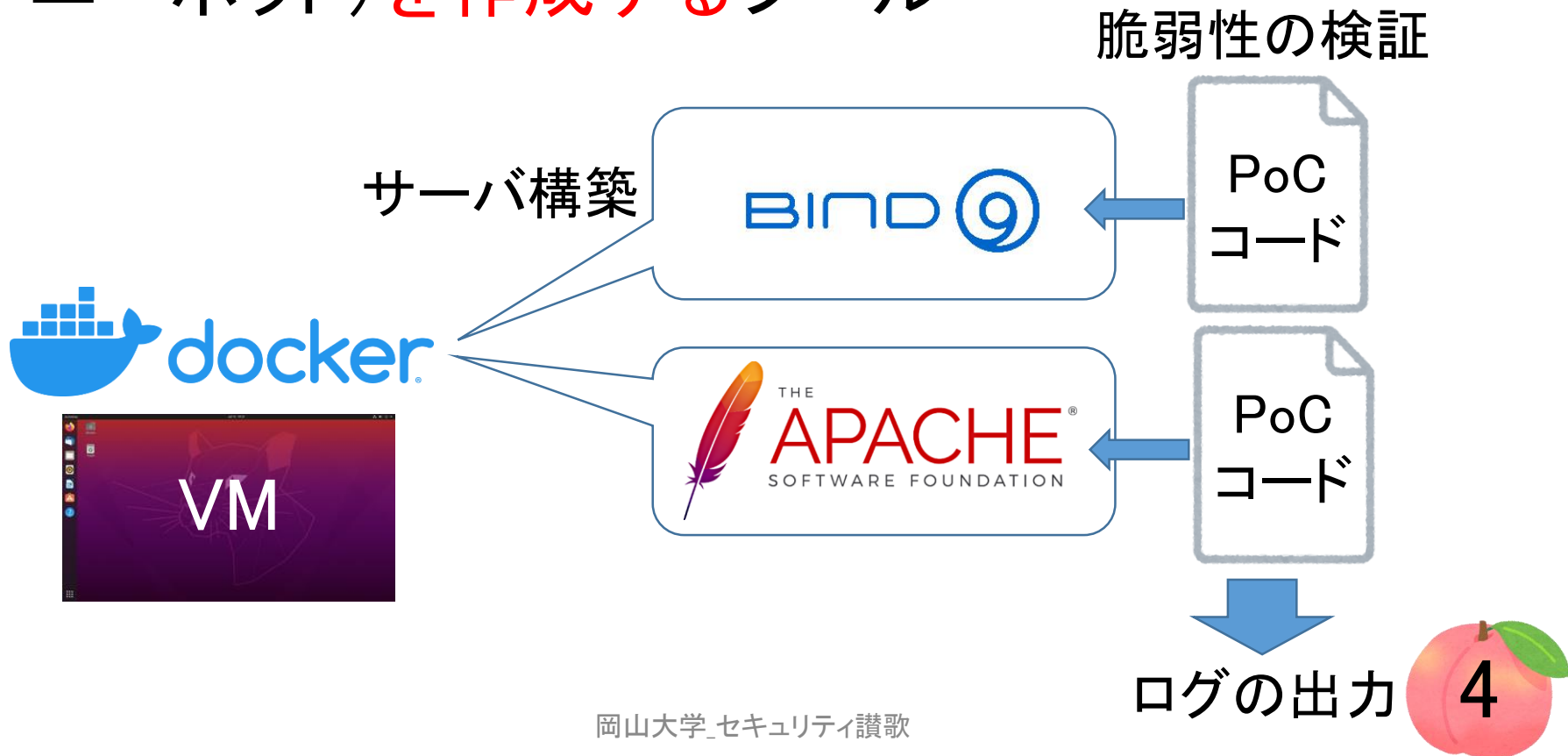
●攻撃内容を知ることのできるログを見たい

●新しいサーバを短時間で起動したい

➡ これらに対応

DC-p0t

- Docker Container honeypot
- 気軽に使用できる「**やられ環境**」(高対話型ハニーポット)**を作成するツール**



主な機能

🍎 サーバ構築

- 🍎 BIND9, Apache2, Apache2+php

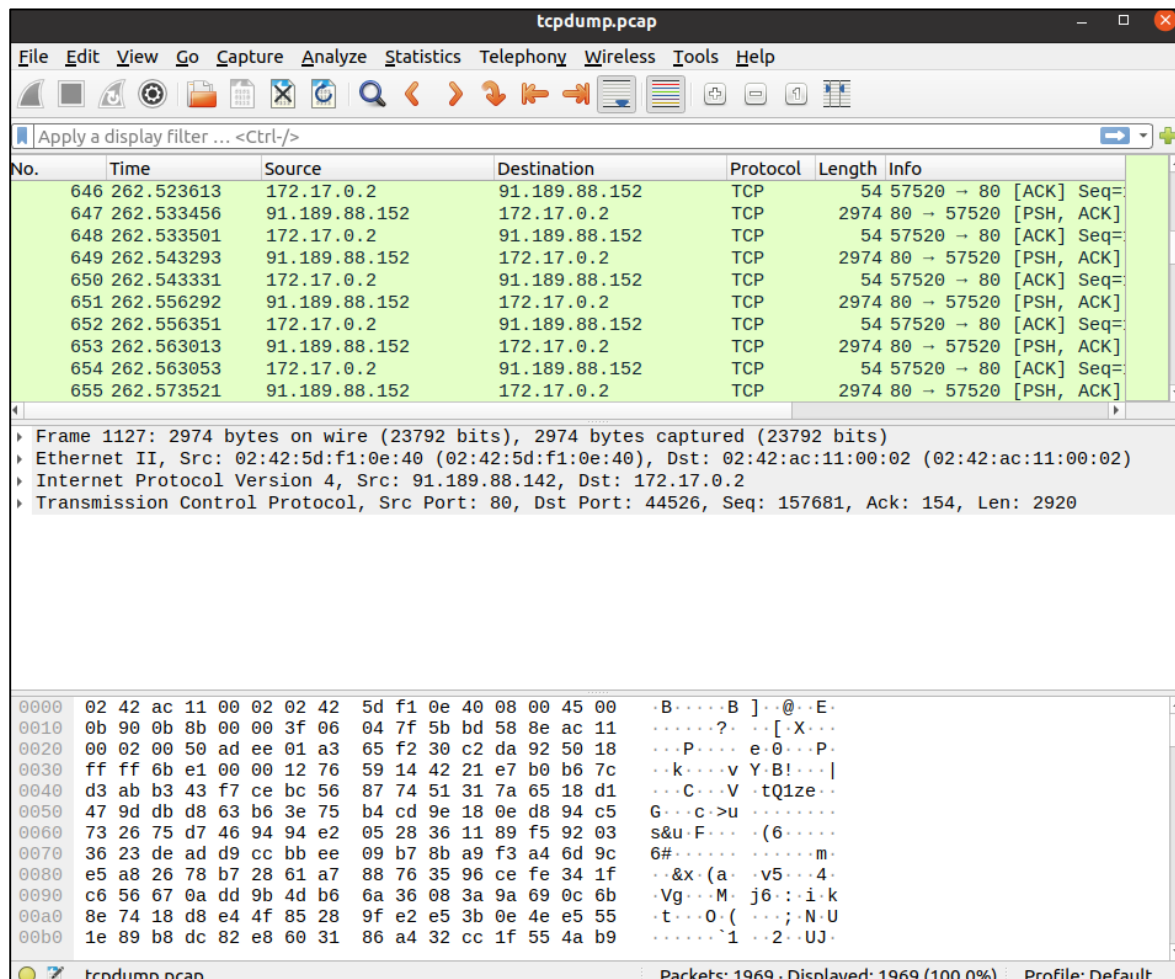
→ 様々なバージョンのサーバを構築可能

🍎 ログの確認

- 🍎 tcpdump, プロセス生成, 追加または修正されたファイル, 標準(エラー)出力メッセージ

ログの確認(1/4)

🍎tcpdumpによる通信のキャプチャ



The screenshot shows the tcpdump.pcap application window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table has columns: No., Time, Source, Destination, Protocol, Length, and Info. It displays 11 packets, all of which are TCP connections from 172.17.0.2 to 91.189.88.152. The details pane for frame 1127 shows the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
646	262.523613	172.17.0.2	91.189.88.152	TCP	54	57520 → 80 [ACK] Seq=
647	262.533456	91.189.88.152	172.17.0.2	TCP	2974	80 → 57520 [PSH, ACK]
648	262.533501	172.17.0.2	91.189.88.152	TCP	54	57520 → 80 [ACK] Seq=
649	262.543293	91.189.88.152	172.17.0.2	TCP	2974	80 → 57520 [PSH, ACK]
650	262.543331	172.17.0.2	91.189.88.152	TCP	54	57520 → 80 [ACK] Seq=
651	262.556292	91.189.88.152	172.17.0.2	TCP	2974	80 → 57520 [PSH, ACK]
652	262.556351	172.17.0.2	91.189.88.152	TCP	54	57520 → 80 [ACK] Seq=
653	262.563013	91.189.88.152	172.17.0.2	TCP	2974	80 → 57520 [PSH, ACK]
654	262.563053	172.17.0.2	91.189.88.152	TCP	54	57520 → 80 [ACK] Seq=
655	262.573521	91.189.88.152	172.17.0.2	TCP	2974	80 → 57520 [PSH, ACK]

Frame 1127: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits)
Ethernet II, Src: 02:42:5d:f1:0e:40 (02:42:5d:f1:0e:40), Dst: 02:42:ac:11:00:02 (02:42:ac:11:00:02)
Internet Protocol Version 4, Src: 91.189.88.142, Dst: 172.17.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 44526, Seq: 157681, Ack: 154, Len: 2920

0000 02 42 ac 11 00 02 02 42 5d f1 0e 40 08 00 45 00 ·B····B·]·@··E·
0010 0b 90 0b 8b 00 00 3f 06 04 7f 5b bd 58 8e ac 11 ····?· ··[·X·
0020 00 02 00 50 ad ee 01 a3 65 f2 30 c2 da 92 50 18 ···P··· e·0···P·
0030 ff ff 6b e1 00 00 12 76 59 14 42 21 e7 b0 b6 7c ··k···v·Y·B!···|
0040 d3 ab b3 43 f7 ce bc 56 87 74 51 31 7a 65 18 d1 ···C··V·tQ1ze··
0050 47 9d db d8 63 b6 3e 75 b4 cd 9e 18 0e d8 94 c5 G··c>u····
0060 73 26 75 d7 46 94 9a e2 05 28 36 11 89 f5 92 03 s&u·F··· ·(6····
0070 36 23 de ad d9 cc bb ee 09 b7 8b a9 f3 a4 6d 9c 6#····· ·····m·
0080 e5 a8 26 78 b7 28 61 a7 88 76 35 96 ce fe 34 1f ··&x·(a· ·v5··4·
0090 c6 56 67 0a dd 9b 4d b6 6a 36 08 3a 9a 69 0c 6b ·Vg· ·M· j6··i·k·
00a0 8e 74 18 d8 e4 4f 85 28 9f e2 e5 3b 0e 4e e5 55 ·t···0·(···;·N·U·
00b0 1e 89 b8 dc 82 e8 60 31 86 a4 32 cc 1f 55 4a b9 ·····1· ·2·UJ·

CVE-2011-3192を
利用したexploit code
を用いたDoS攻撃の
通信キャプチャ



ログの確認(2/4)

🍑 コンテナで起動したプロセスのPIDとプロセス名

ps_monitor.txt [読み取り専用]									
ファイル"/home/kawashima/dc-p0t/ps_monitor.txt"を開くときにエラーが発生しました。									
開いたファイルに不正な文字が含まれています。このファイルを編集し続けると、この文書が壊れてしまうかもしれません。									
メニューから文字エンコーディングを選択して再試行してください。									
文字エンコーディング(A): 現在のロケール (UTF-8) ▼									
1	UID	EVENT	COMM	PID	TID	PPID	RET	ARGS	
2	0	execve	runc:[2:INIT]	20	20	147769	0	/usr/bin/ls	00 [ls, -l, /usr]
3	0	execve	runc:[2:INIT]	25	25	147806	0	/usr/bin/ls	00 [ls, -l, /usr/local]
4	0	execve	runc:[2:INIT]	30	30	147841	0	/usr/bin/ls	00 [ls, -l, /usr/local/apache2]
5	0	execve	runc:[2:INIT]	36	36	147877	0	/usr/bin/ls	00 [ls, -l, /usr/local/apache2/logs]
6	0	execve	runc:[2:INIT]	42	42	147914	0	/usr/bin/ls	00 [ls, -l, /usr/local/apache2/logs/access_log]
7	0	execve	runc:[2:INIT]	47	47	147972	0	/usr/bin/ls	00 [ls, -l, /usr/local/apache2/logs/error_log]
8	0	execve	runc:[2:INIT]	52	52	148028	0	/usr/bin/ls	00 [ls, -l, /usr/local/apache2/logs/httpd.pid]

ログの確認(3/4)

🍎 コンテナ起動中に追加・修正されたファイルの一覧

```
docker_diff_result.txt [読み取り専用]
~/dc-p0t

1 C /usr
2 C /usr/local
3 C /usr/local/apache2
4 C /usr/local/apache2/logs
5 A /usr/local/apache2/logs/httpd.pid
6 A /usr/local/apache2/logs/access_log
7 A /usr/local/apache2/logs/error_log
```

🍎 追加・修正されたファイルの内容

```
docker_log  usr  local  apache2  logs
最近開いたファイル
★ 星付き
🏠 ホーム
🖥 デスクトップ
📄 ダウンロード
📁 ドキュメント
📺 ビデオ
🖼️ ピクチャ
🎵 ミュージック
🗑️ ゴミ箱
+ 他の場所

access_log  error_log  httpd.pid

access_log [読...
~/dc-p0t/docker_l...

access_log x  error_log x  httpd.pid x
1 172.17.0.1 - - [19/Oct/2020:14:31:52 +0900] "GET / HTTP/1.1" 200 44
2 172.17.0.1 - - [19/Oct/2020:14:31:52 +0900] "GET / favicon.ico HTTP/1.1" 404 209

なし ▾ タブ幅: 8 ▾ (2行、80列) ▾ [挿入]
```


ログの確認(4/4)

●標準出力および標準エラー出力



The screenshot shows a text editor window titled "docker_logs_result.txt [読み取り専用]" with a file path of "~/dc-p0t". The window contains a single line of log output: "1 httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2 for ServerName". The status bar at the bottom indicates "なし", "タブ幅: 8", "(1行、110列)", and "[挿入]".

```
1 httpd: Could not reliably determine the server's fully qualified domain  
name, using 172.17.0.2 for ServerName
```

メンバーの担当箇所

- 市岡・・・Docker上のApache, BINDの環境構築
- 伊藤・・・ログ取得モジュールの作成
- 白石・・・攻撃実験の実施・性能評価
- 大谷・・・関連研究の調査
- 川島・・・README, スライドの作成
- 芝・・・Docker上のphpの環境構築, UIの実装

継続性と貢献

🍎 継続性

- 🍎 対応する「やられ環境」の拡張
 - 🍎 WordPressの導入を検討中
- 🍎 ソースコードの公開

🍎 貢献

- 🍎 実際に攻撃を手軽に試すことが可能
- 🍎 プロセスログの取得などを簡単にできる

まとめ

- 気軽に使用できる「やられ環境」(高対話型ハニーポット)を作成するツール「DC-p0t」
- 機能は大きく2つ
 - サーバ構築
 - ログの確認
- 実際に受けた攻撃や脆弱性に迅速に対応可能

🍎 ご清聴ありがとうございました