

サイバーセキュリティ 演習フレームワークCyTrONE

利用方法

北陸先端科学技術大学院大学

Razvan Beuran

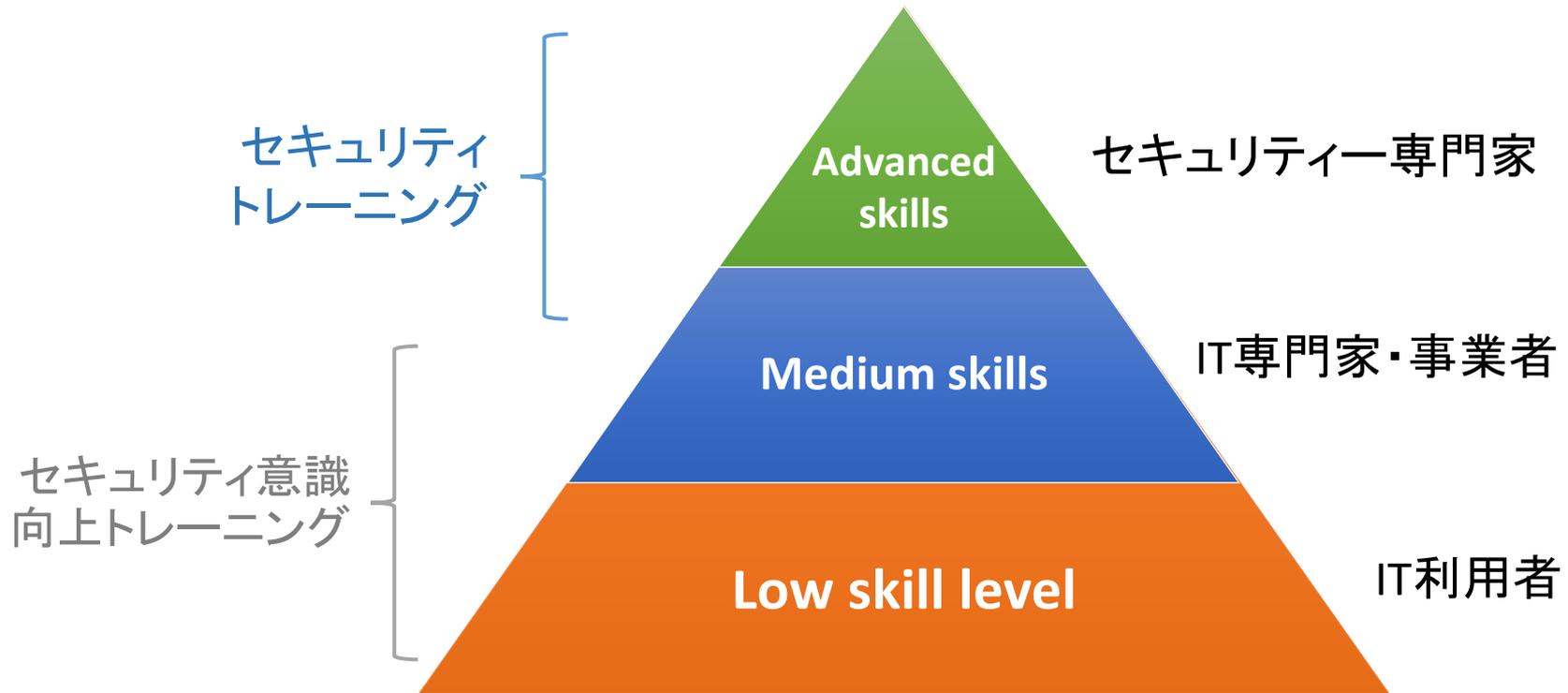
概要

1. サイバーレンジ構成学
2. CyTrONEの概要
3. CyTrONEの利用
4. まとめ

1. サイバーレンジ構成学

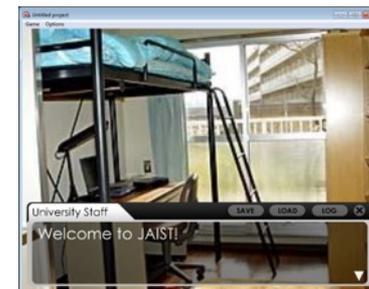
- 北陸先端科学技術大学院大学 NEC寄附講座
 - 2015年4月～2021年3月
 - 日本語名 : サイバーレンジ構成学
 - 英語名 : Cyber Range Organization and Design (CROND)
- 目的 : サイバーセキュリティ人材育成の改善
 - 多種多様なサイバーレンジを誰でも容易に構築できるための基盤技術を研究開発
 - 教育プログラムの設計および教材開発

サイバー演習の必要性

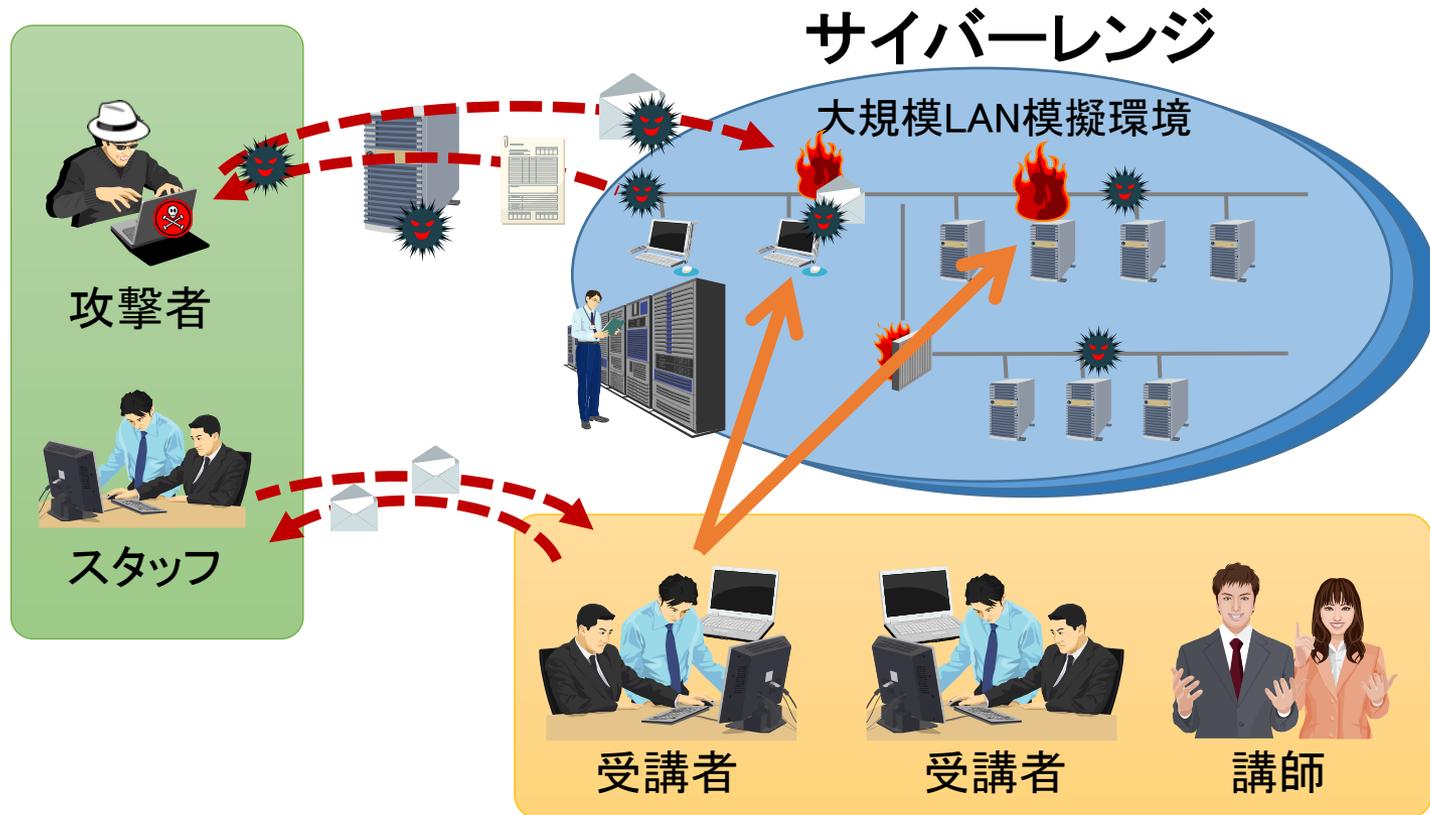


CRONDの活動

- セキュリティトレーニングを中心に
 - サイバー演習統合フレームワークCyTrONEをGitHubで公開
<https://github.com/crond-jaist>
 - **演習支援システム**
 1. 簡単に演習コンテンツの編集・追加が可能
 2. 演習環境の自動生成と管理
- セキュリティ意識向上トレーニングの研究
 - シリアスゲームのプロトタイプ
 - 演習コンテンツの自動生成
 - 適応学習

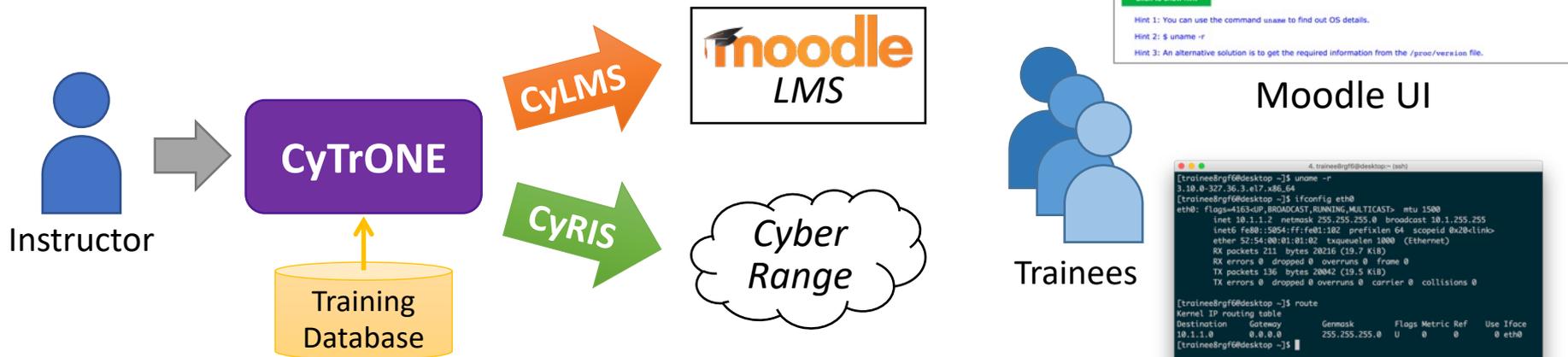


サイバーレンジとは



サイバーレンジ = サイバー攻撃や防御の演習を行うために電子計算機上に特別に構築される仮想空間

2. CyTrONEの概要



CyTrONE Web UI: Door

Training Content		Active Sessions		
<input type="checkbox"/> Scenario Name Information Security Testing and Assessment <input type="checkbox"/> Level 1 (sample) NIST Guide Inspired Training <input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 CTF Style Training Questions <input type="checkbox"/> Binary <input type="checkbox"/> Cryptography <input type="checkbox"/> Network <input type="checkbox"/> OS <input type="checkbox"/> Web	<input type="checkbox"/> End Session <input type="checkbox"/> Refresh List	<input type="checkbox"/> ID <input type="checkbox"/> Session Name <input type="checkbox"/> Inst. Count <input type="checkbox"/> Creation Time	<input type="checkbox"/> 2 <input type="checkbox"/> Level 1 (sample) 1 <input type="checkbox"/> Wed Feb 2 18:55 2022	<input type="checkbox"/> 3 <input type="checkbox"/> Level 1 (sample) 2 <input type="checkbox"/> Wed Feb 2 19:16:43 2022

Last refreshed on Thu Feb 03 2022 11:52:03 GMT+0900 (Japan Standard Time)

CLI/Web UI

```

[traineer@desktop ~]$ uname -r
3.10.0-327.el7.x86_64
[traineer@desktop ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.2 netmask 255.255.255.0 broadcast 10.1.255.255
    inet6 fe80::5854:fff:fe01:202 prefixlen 64 scopeid 0x2<link-ether>
    ether 52:54:00:01:01:02 txqueuelen 1000 (Ethernet)
    RX packets 211 bytes 20216 (19.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 136 bytes 20042 (19.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[traineer@desktop ~]$ route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
10.1.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
[traineer@desktop ~]$
    
```

SSH/VNCでアクセス

サイバーレンジ生成の機能



演習コンテンツ公開

- サンプル演習コンテンツはGitHubで公開
- 他の演習コンテンツはCRONDのウェブサイトで公開
 - <https://www.jaist.ac.jp/misc/crond/achievements-ja.html>

1) CTF型演習コンテンツ

バイナリ解析	バイナリファイル (画像, 音声等データ, 実行可能なプログラム等) を調べる
暗号解読	与えられた暗号を解読する
ネットワーク	キャプチャされたパケットを解析する
OS	OS のリソース (CPU の使用状況やメモリの占有状態等) 管理機能を使用する
ウェブ	SQL インジェクション, クロスサイトスクリプティングを利用する

2) NISTの「Technical Guide to Information Security Testing and Assessment」を参考にした演習コンテンツ

CyTrONEの特長

- 自由性を持ち、大規模な環境生成が可能で、コストが低く、効果的な演習ができる
 - プロプライエタリのシステムと違って拡張が可能



	他のレンジ	CyTrONE
自由性	無	∞
大規模	×	○
コスト*	高	0円+ α

* ソフト + コンテンツ + インフラ

3. CyTrONEの利用

- CyTrONEはインストール済みの想定
- 講師用の操作
 - CyTrONEの操作
 - 演習の操作
 - アカウントの管理
- 受講者用の操作
 - Moodleへのアクセス
 - 問題へのアクセス
 - 解答の登録

講師用の操作

CyTrONEの操作

- CyTrONEの起動
 - `$./start_cytrone.sh`
 - ログファイルが「/tmp」に保存される
- CyTrONEの終了
 - `$./stop_cytrone.sh`
- Moodle VMの起動・終了
 - `$ virsh start moodle`
 - `$ virsh shutdown moodle`

演習の操作 (CLIの場合)

- 演習の起動
 - `$./create_training.sh`
 - 演習のIDとレンジのログイン情報が表示される
 - その後に、レンジのログイン情報を表示したい場合
 - `$./get_notification.sh`
- 演習の終了
 - `./end_training.sh 1` ← 演習のID

演習の操作 (Web UIの場合)

演習の起動

演習の終了

CyTrONE Web UI: Door

Training Content

Create Session Refresh Content

Scenario Name

① 情報セキュリティテスト&評価

レベル 1 (サンプル)

NISTのガイドラインを参考にした演習

レベル 1

レベル 2

CTF型演習問題セット

バイナリ解析

暗号解読

ネットワーク

オペレーティングシステム

ウェブ

Active Sessions

End Session Refresh List

①

ID	Session Name	Inst. Count	Creation Time
<input type="checkbox"/> 2	Level 1 (sample) 1	1	Wed Feb 2 18:18:55 2022
<input type="checkbox"/> 3	Level 1 (sample) 2	2	Wed Feb 2 19:16:43 2022

Last refreshed on Thu Feb 03 2022 11:25:01 GMT+0900 (Japan Standard Time)

レンジのログイン情報の例

Dear user,

Thank you very much for using our cybersecurity training framework. We would like to inform you that Training Session #1 is ready to use. Please find below detailed information about how to access the created cyber range instances:

- Total number of cyber range instances: 2

- Cyber range instance #1:

Login: ssh trainee01@127.0.0.1 -p 63476

Password: 86y35m9bka

- Cyber range instance #2:

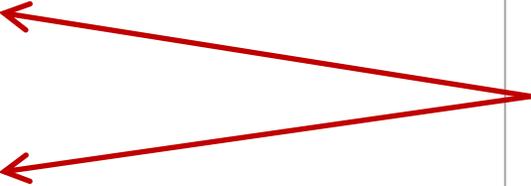
Login: ssh trainee02@127.0.0.1 -p 60243

Password: 0lgx3pn3pk7

We hope you will gain valuable knowledge about cybersecurity through this training. Feel free to contact us if you want to share with us what you think about our training framework.

Best of luck,
The Administration Team

受講者に配布



アカウントの管理

- Moodle関係
 - 受講者用のユーザアカウントを作成し、情報を配布
- サイバーレンジ関係
 - 受講者にサイバーレンジのログイン情報を配布

受講者用の操作

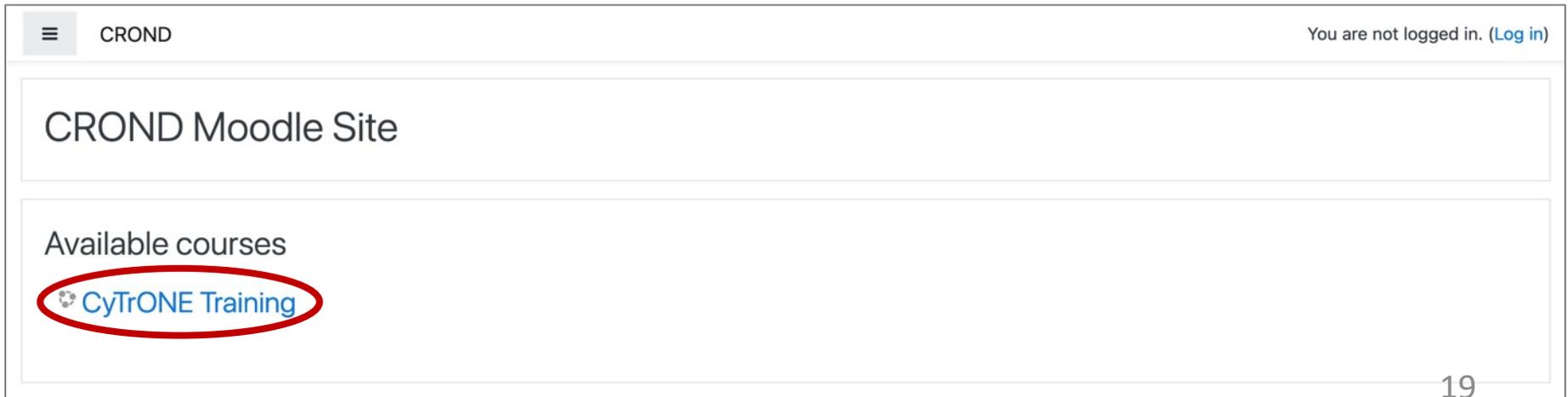
Moodleへのアクセス(1)

- Webブラウザ上で

<https://○○○○○.○○:8081>

と入力してアクセス

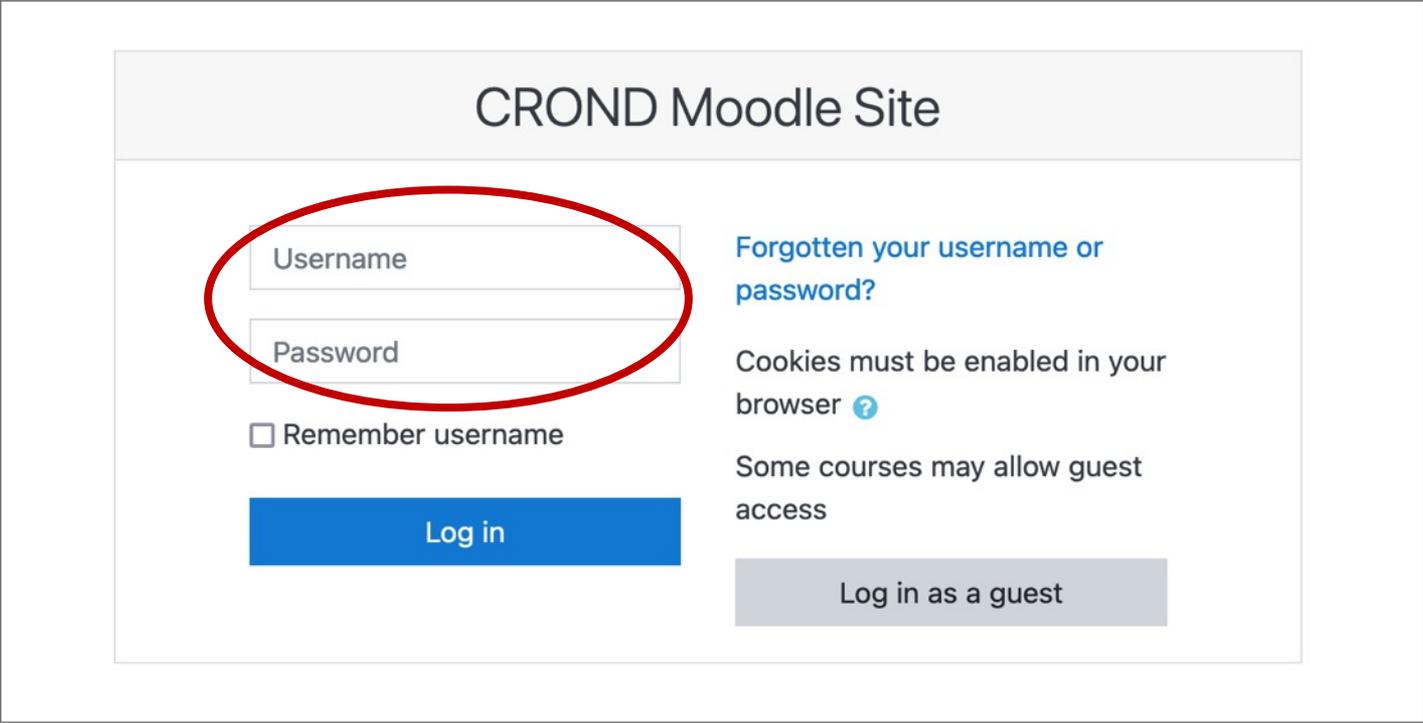
- 青文字の「[CyTrONE Training](#)」をクリック



The screenshot shows a Moodle site interface. At the top left, there is a hamburger menu icon and the text 'CROND'. At the top right, it says 'You are not logged in. (Log in)'. Below the header, there is a section titled 'CROND Moodle Site'. Underneath, there is a section titled 'Available courses'. In this section, the text 'CyTrONE Training' is highlighted with a red circle.

Moodleへのアクセス(2)

- 受講者のMoodle用のユーザ名とパスワードを入力してログイン



CROND Moodle Site

Username

Password

Remember username

Log in

[Forgotten your username or password?](#)

Cookies must be enabled in your browser [?](#)

Some courses may allow guest access

Log in as a guest

問題へのアクセス(1)

- 青文字の「Activity #〇: 〇〇〇」を選択

The screenshot displays the CyTrONE Training interface. On the left is a navigation sidebar with the following items: CyTrONE Training (header), Participants, Badges, Competencies, Grades, Training Activities, and Dashboard. The main content area shows the title 'CyTrONE Training' and a breadcrumb trail: Dashboard / My courses / CyTrONE Training. Below this is a section titled 'Training Activities' with the subtitle 'List of cybersecurity training activities created via CyTrONE'. A single activity is listed: 'Activity #1: I465S Cybersecurity Training', which is circled in red. Below the activity name, it says 'Added on: 2021-09-02 09:35:22'.

問題へのアクセス(2)

- 「Enter」ボタンを押す

The screenshot displays the CyTrONE Training user interface. On the left is a navigation sidebar with the following items: CyTrONE Training, Participants, Badges, Competencies, Grades, Training Activities (highlighted in blue), Dashboard, Site home, Calendar, Private files, and My courses. The main content area shows the breadcrumb path: Dashboard / My courses / CyTrONE Training / Training Activities / Activity #1: I465S Cybersecurity Training. Below this, the title 'Activity #1: I465S Cybersecurity Training' is displayed. The activity details include: Added on: 2021-09-02 09:35:22, Number of attempts allowed: Unlimited, Number of attempts you have made: 1, Grade for attempt 1: 0, Grading method: Highest attempt, and Grade reported: 0. At the bottom, the mode is set to 'Normal' (selected with a radio button). A blue 'Enter' button is circled in red, indicating the next step in the process.

演習画面の例

Information Security Testing and Assessment

Level 1: Investigate the security of a desktop computer

Today is your first day on the job as a sysadmin. Your boss tells you that he suspects somebody tried to hack into your company's network, and asks you to investigate a possible cyber attack that may have happened when the system administrator was a guy called Daniel Craig. The boss sits you in front of the previous sysadmin's computer, and wishes you good luck.

You glance at the machine and reluctantly get to work.

OPEN TERMINAL



Click to show hint

サイバーレンジ内の調査例

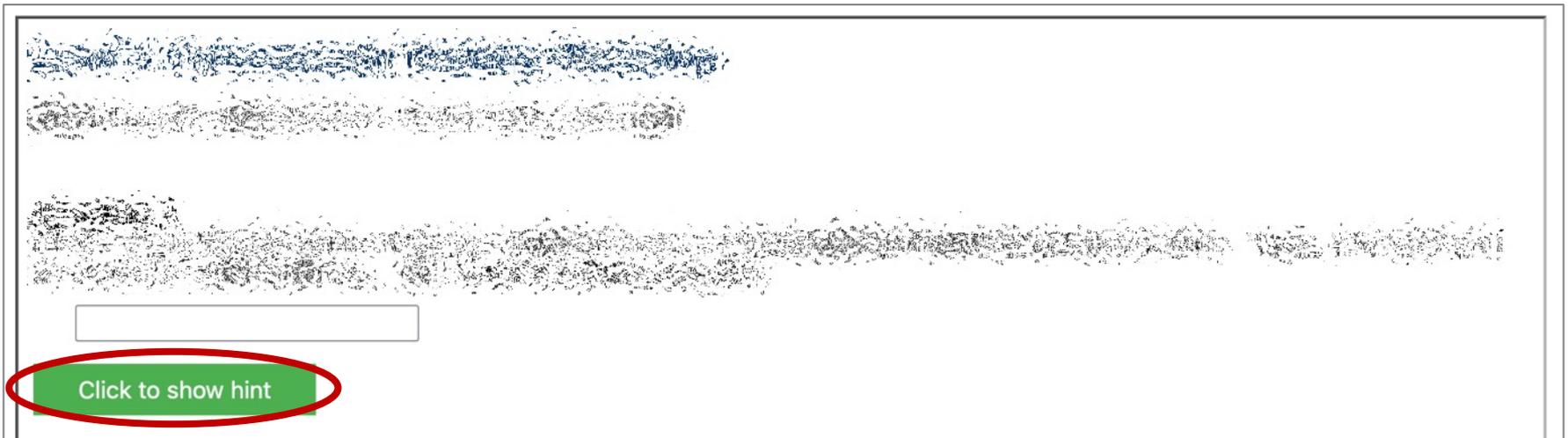
```
$ ssh trainee01@127.0.0.1 -p 63476
The authenticity of host '[127.0.0.1]:63476 ([127.0.0.1]:63476)' can't be established.
ECDSA key fingerprint is SHA256:Y+ukVDq09KKJHtF7o9P/Wc3M6xxPBJr4p5Fy9uNpBtd.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[127.0.0.1]:63476' (ECDSA) to the list of known hosts.
trainee01@127.0.0.1's password:
[trainee01@desktop ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 3.1.1.2  netmask 255.255.255.0  broadcast 3.255.255.255
    inet6 fe80::5054:1ff:fe01:102  prefixlen 64  scopeid 0x20<link>
    ether 52:54:01:01:01:02  txqueuelen 1000  (Ethernet)
    RX packets 133  bytes 19164 (18.7 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 525  bytes 51218 (50.0 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

演習に行き詰まったら

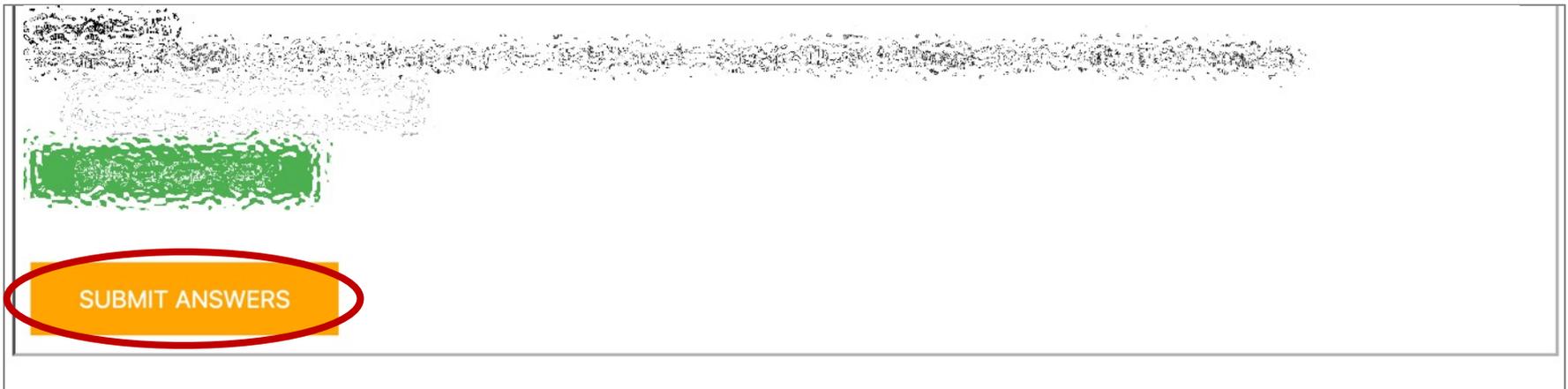
- ヒントの活用

- 「Click to show hint」ボタンを押すとヒントが表示される
- 複数回押すと複数のヒントが表示される場合がある



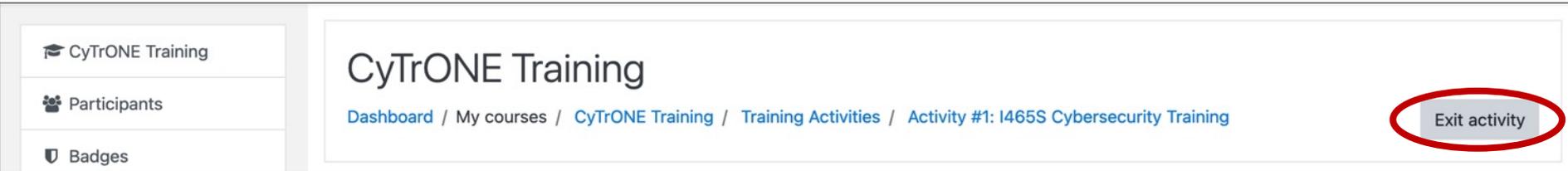
解答の提出

- 各問題の解答を記入して「SUBMIT ANSWERS」をクリック
- 解答が正しいかどうか表示される



解答の登録

- 「Exit activity」ボタンをクリック



The screenshot shows the CyTrONE Training interface. On the left is a sidebar with navigation options: 'CyTrONE Training', 'Participants', and 'Badges'. The main content area displays the title 'CyTrONE Training' and a breadcrumb trail: 'Dashboard / My courses / CyTrONE Training / Training Activities / Activity #1: I465S Cybersecurity Training'. In the top right corner, there is a button labeled 'Exit activity', which is circled in red.

- 何度解答しても可能なので、最後まで諦めない



The screenshot shows the 'Training Activities' page. On the left is a sidebar with navigation options: 'Competencies', 'Grades', 'Training Activities', and 'Dashboard'. The main content area displays the title 'Training Activities' and the subtitle 'List of cybersecurity training activities created via CyTrONE'. Below this, there is a list of activities. The first activity, 'Activity #1: I465S Cybersecurity Training', is circled in red. Below the activity name, it says 'Added on: 2021-09-02 09:35:22'.

4. まとめ

- サイバーレンジ構成学 (CROND) がサイバー演習統合フレームワークCyTrONEを研究開発
 - 様々なサイバーレンジ生成機能が含まれている
- CyTrONEに関する操作
 - 講師用の操作
 - CyTrONE自体と演習の操作
 - アカウントの管理
 - 受講者用の操作
 - Moodleへのアクセス
 - 問題へのアクセス、解答の登録