ペネトレーションテスターより愛を込めてSE ～攻撃視点からの提案～

NTTデータ先端技術株式会社
辻 伸弘

まずは、自己紹介から

辻 伸弘(つじ のぶひろ)

大阪生まれ、大阪育ち。

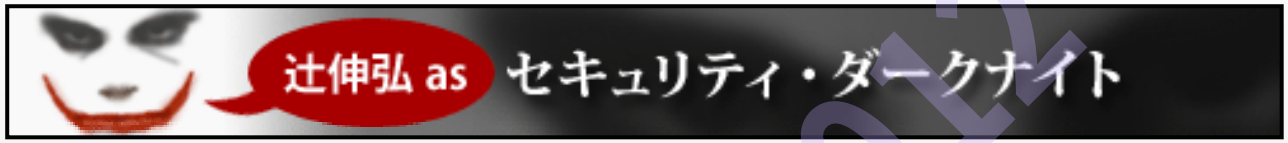
ペネトレをしたくて上京。現在、たしか10年目。

普段の業務はペネトレがメイン。

IDS、ハニポ、フォレンジックなども趣味で。

宣伝

連載記事



http://bit.ly/4mZZxF

http://bit.ly/2xFga

宣伝

その他、雑誌とか色々

おだいもく

0x01. 昨今のセキュリティ界隈
0x02. 予防という考え方
0x03. ペネトレの現場から
0x04. 盛り上がりを見せる対策
0x05. さいごに

0x01. 昨今のセキュリティ界隈

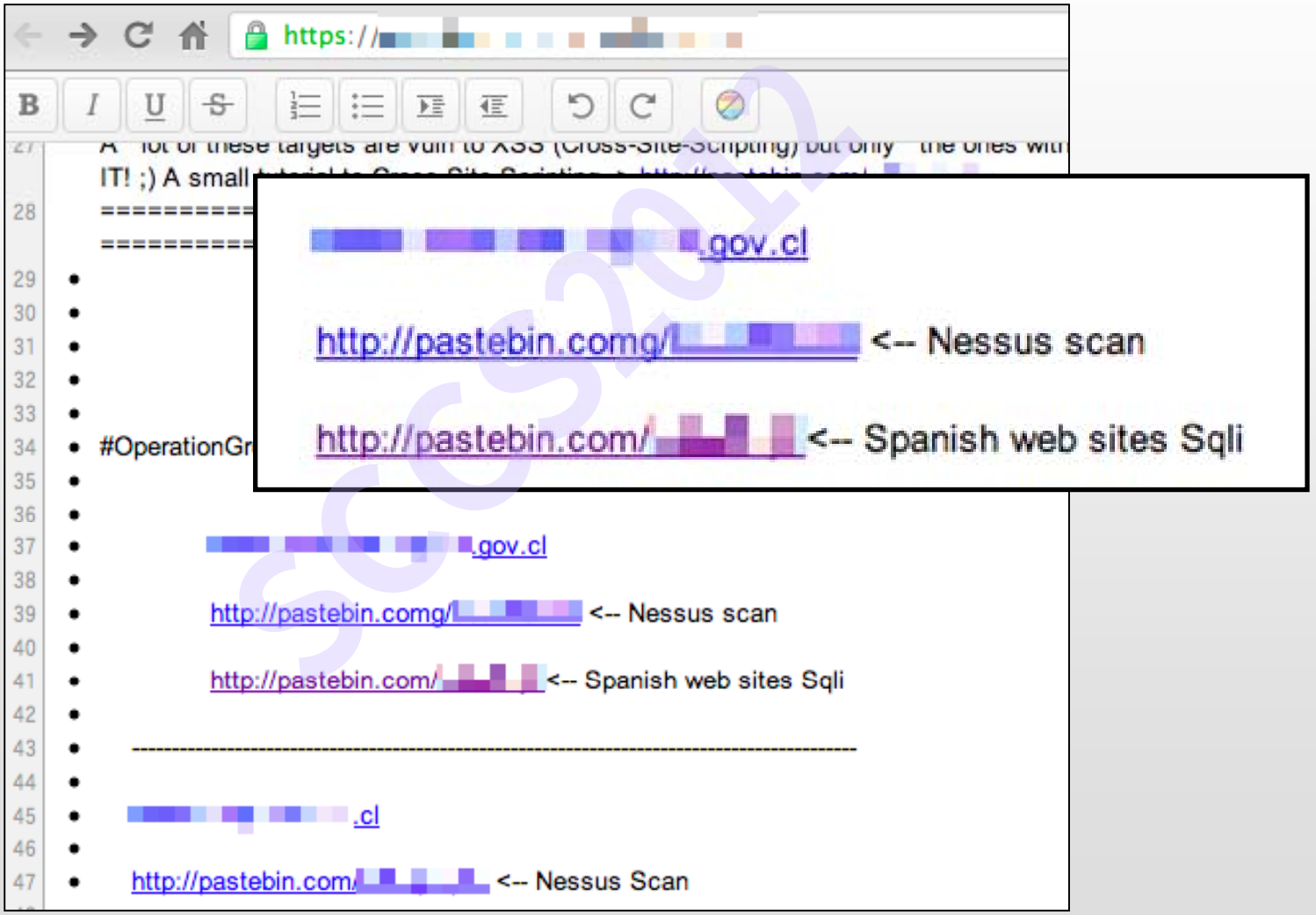
0x01. 昨今のセキュリティ界隈

0x01. 昨今のセキュリティ界隈

ま～ 目まぐるしい。

ちょっと絵で見てみましょう。

0x01. 昨今のセキュリティ界隈

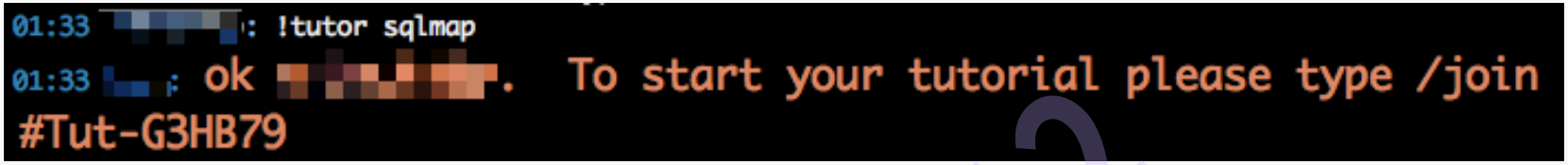


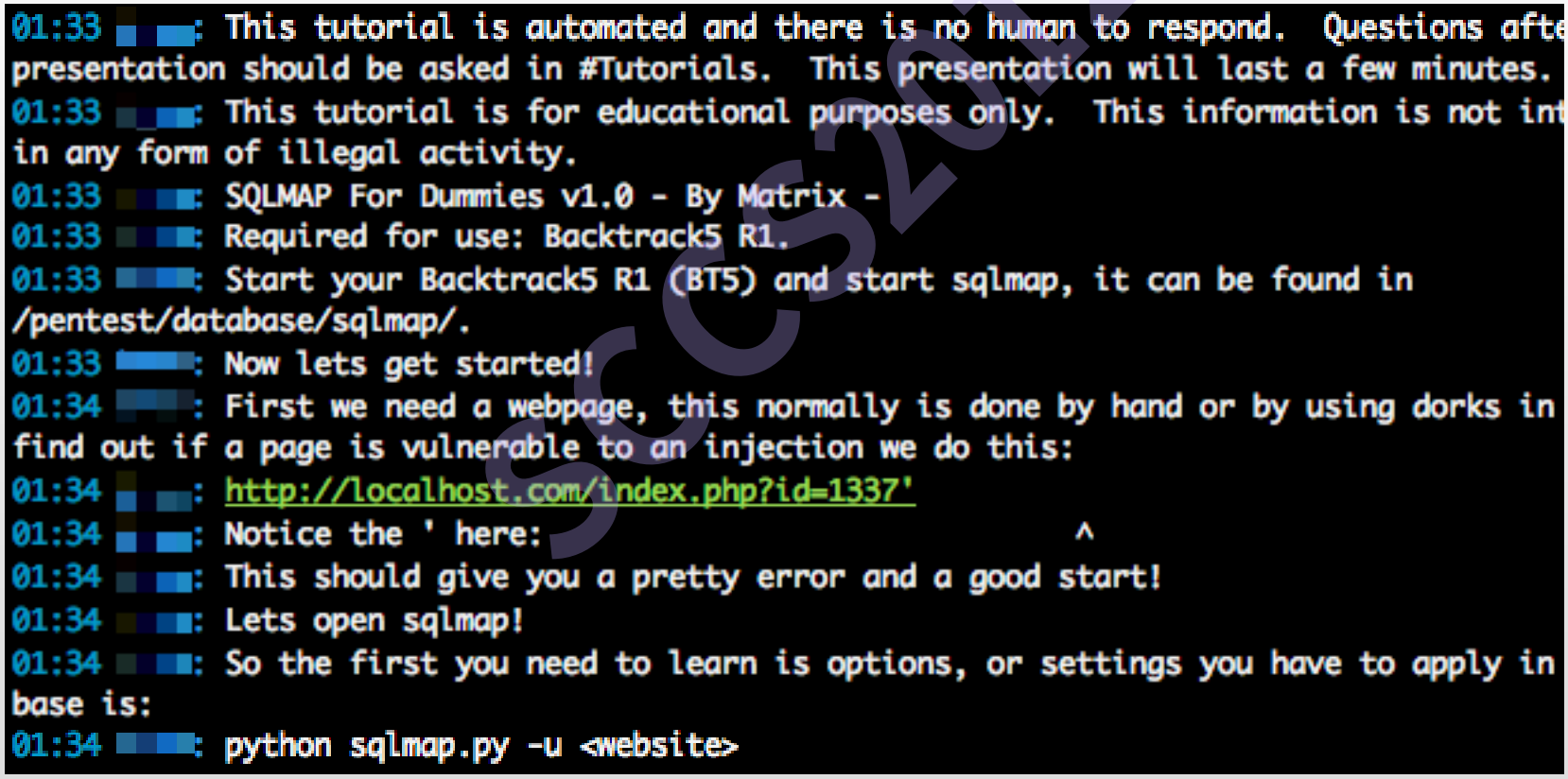
0x01. 昨今のセキュリティ界隈

```
1.  [redacted].cl Nessus scan:
7.
8.  The following plugin IDs have problems associated with them. Select the ID to review more detai
9.  Plugin id#arrow # of issuesarrow        Plugin namearrow        Severityarrow
10. 57792   1       Apache HTTP Server httpOnly Cookie Information Disclosure       Medium Severity
    problem(s) found
11. 10302   1       Web Server robots.txt Information Disclosure    Low Severity problem(s) found
12. 11419   1       Web Server Office File Inventory        Low Severity problem(s) found
13. 11032   1       Web Server Directory Enumeration        Low Severity problem(s) found
```

```
13. 11032   1       Web Server Directory Enumeration        Low Severity problem(s) found
14. 10662   1       Web mirroring   Low Severity problem(s) found
15. 10287   1       Traceroute Information  Low Severity problem(s) found
16. 25220   1       TCP/IP Timestamps Supported     Low Severity problem(s) found
17. 22964   1       Service Detection       Low Severity problem(s) found
18. 11936   1       OS Identification       Low Severity problem(s) found
19. 19506   1       Nessus Scan Information         Low Severity problem(s) found
20. 24260   1       HyperText Transfer Protocol (HTTP) Information  Low Severity problem(s) found
21. 10107   1       HTTP Server Type and Version    Low Severity problem(s) found
22. 43111   1       HTTP Methods Allowed (per directory)    Low Severity problem(s) found
23. 12053   1       Host Fully Qualified Domain Name (FQDN) Resolution      Low Severity problem(s) found
24. 49704   1       External URLs   Low Severity problem(s) found
```

0x01. 昨今のセキュリティ界隈



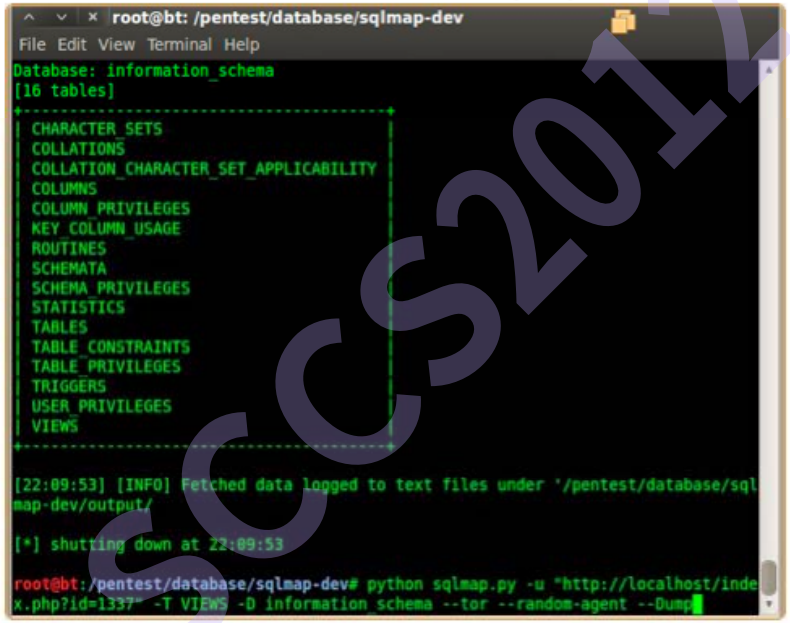


0x01. 昨今のセキュリティ界隈

SQLMAP For Dummies v2 -

[redacted]@gmail.com

Feel free to comment the doc and post questions.

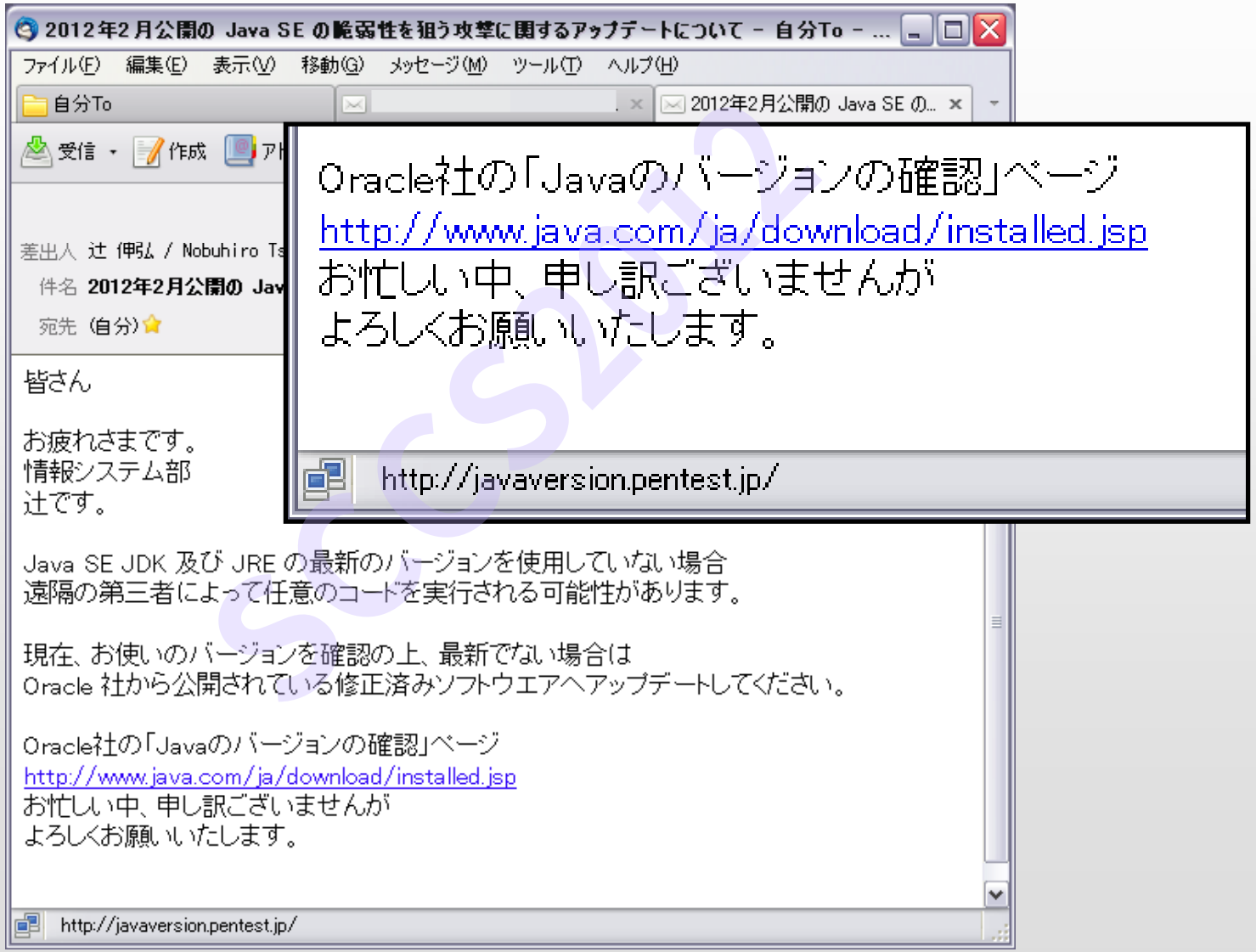


As you can see above we got the tables inside the database information_schema. Nothing to interesting, but i guess we wanna see closer on the table "VIEW". Thus we select the database (-D information_schema) and the table we wanna see (-T VIEWS). using -T we need to add a option telling SQLMAP we wanna dump it all to a text file, thus we use --dump.

and the result:

0x01. 昨今のセキュリティ界隈

0x01. 昨今のセキュリティ界隈



0x01. 昨今のセキュリティ界隈

0x01. 昨今のセキュリティ界隈

しっかり、準備

ちゃっかり、巧妙

0x01. 昨今のセキュリティ界隈

「意識高い」です。

で、一方、、、

0x01. 昨今のセキュリティ界隈

標的型攻撃メールの訓練

開く率を低下させる？

開封率 1% VS 10%では？

0x01. 昨今のセキュリティ界隈

100人を対象にした場合

10人（一般社員）

1人（役員クラス、シス管）

0x01. 昨今のセキュリティ界隈

やられない。はもう捨てて。

弱点発見や意識の底上げ

0%にするというのは…

0x01. 昨今のセキュリティ界隈

しっかり、準備

ちゃっかり、巧妙

0x02. 予防という考え方

そんな中でまず変えないといけない。

「予防」への認識

0x02. 予防という考え方

0x02. 予防という考え方

予防医学という考え方

0x02. 予防という考え方

予防医学という考え方

第1次予防

病気の発生を未然に防ぐ行為。
健康増進と特異的予防
健康増進 → 生活習慣の改善
特異的予防 → 予防接種

0x02. 予防という考え方

予防医学という考え方

第2次予防

病気を早期に発見・処置する行為。
早期発見 → 定期健診・人間ドック
早期処置 → 臨床的治療
治療困難・コスト増を防ぐ

0x02. 予防という考え方

予防医学という考え方

第3次予防

社会復帰するための行為。
機能低下防止、治療、リハビリ
機能回復と再発防止

0x02. 予防という考え方

今までの認識を捨ててください。

100%未然に防ぐことは不可能
世の中にそんな物はありません。

0x02. 予防という考え方

今までの認識を捨ててください。

コンピュータはいくつ？
コンピュータに脆弱性はいくつ？

社員は何人？
社員のリテラシーは？

0x02. 予防という考え方

今までの認識を捨ててください。

何か1つ・・・
破ることができれば…

何か1つ・・・
破られてしまえば…

0x02. 予防という考え方

予防というのは

健康に生きていく

通常の運用を継続させる

0x02. 予防という考え方

では、どうするか

段階的な予防を用いた多層防御の仕組み

0x03. ペネトレの現場から

0x03. ペネトレの現場から

と、その前に

ペネトレってなんですかの話を

0x03. ペネトレの現場から

penetration

→ 貫通、挿入
浸透(力)、洞察力, 眼識.

0x03. ペネトレの現場から

penetration

貫通、挿入
浸透(力)、洞察力, 眼識.

penetration pricing

【商業】
浸透価格設定 新製品が早く市場に浸透するように当初は安く価格を設定すること

0x03. ペネトレの現場から

penetration test

→ 貫通試験・侵入試験

↓

セキュリティ診断、 侵入実験
セキュリティクリニック、 擬似侵入検査サービス

0x03. ペネトレの現場から

言葉の定義（辻版）としては

コンピュータ・ネットワークに内在する弱点を
検出し、実証、評価する行為。

ネットワーク上のコンピュータやNW機器など
に対して、実際の攻撃手法を用いて実証。
対象がどの程度のセキュリティレベルであるのか
ということを判明させること。

0x03. ペネトレの現場から

経路・対象についての誤認

ペネトレーションテストの説明の際に

「外部」からサーバを診断します。

というような文言が多用される

0x03. ペネトレの現場から

経路・対象についての誤認

以下のように誤認

ペネトレは、
インターネットから
DMZ上の公開サーバに実施

0x03. ペネトレの現場から

経路・対象についての誤認

以下のように誤認

~~ペネトレは、
インターネットから
DMZ上の公開サーバに実施~~

0x03. ペネトレの現場から

経路・対象についての誤認

そんな縛りはありません。

0x03. ペネトレの現場から

経路・対象についての誤認

インターネットへの
公開、非公開は全く関係ありません。
DMZ、内部ネットワーク
サーバ、クライアント、ネットワーク機器
どれでもです。

0x03. ペネトレの現場から

経路・対象についての誤認

もっと極端

0x03. ペネトレの現場から

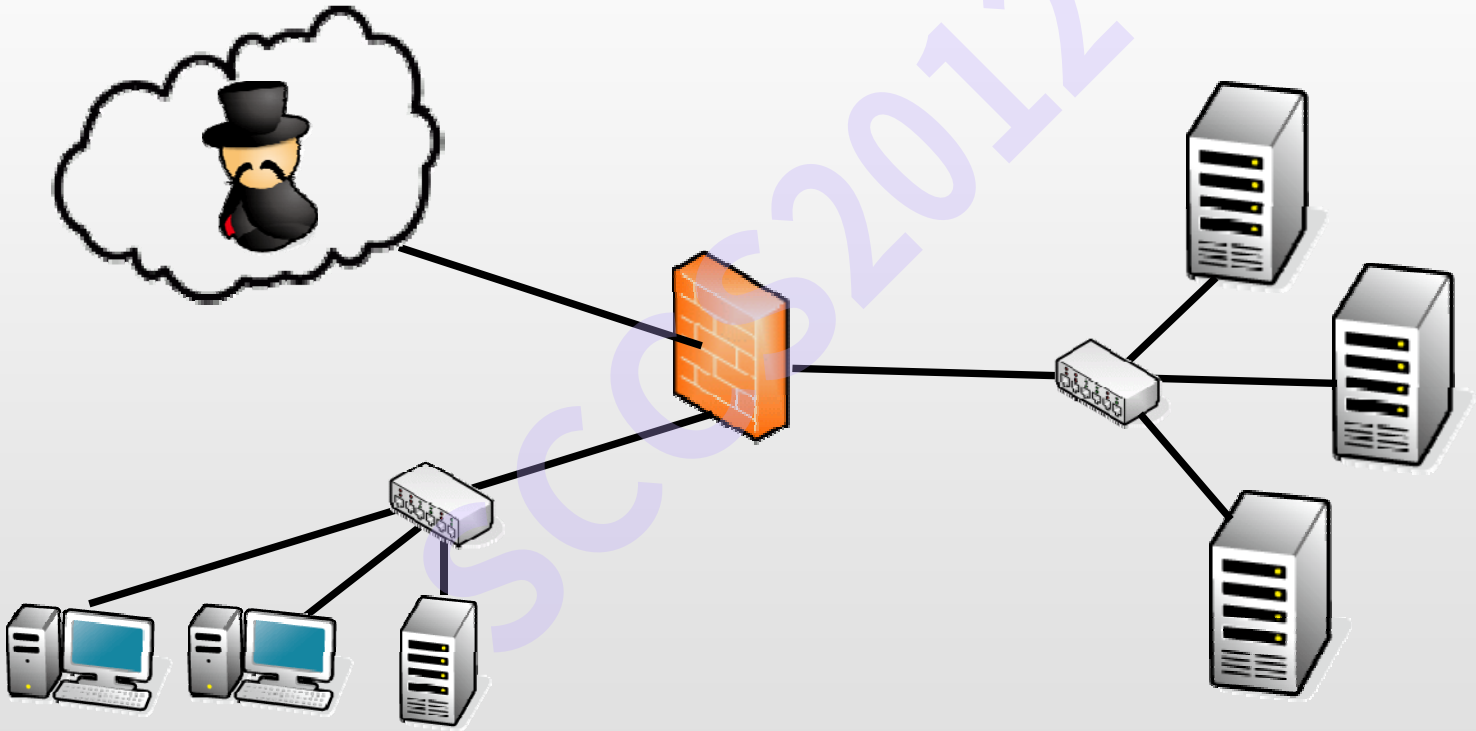
経路・対象についての誤認

IPアドレスを
持っていればOK

プリンタや空調制御装置の検査もしました。

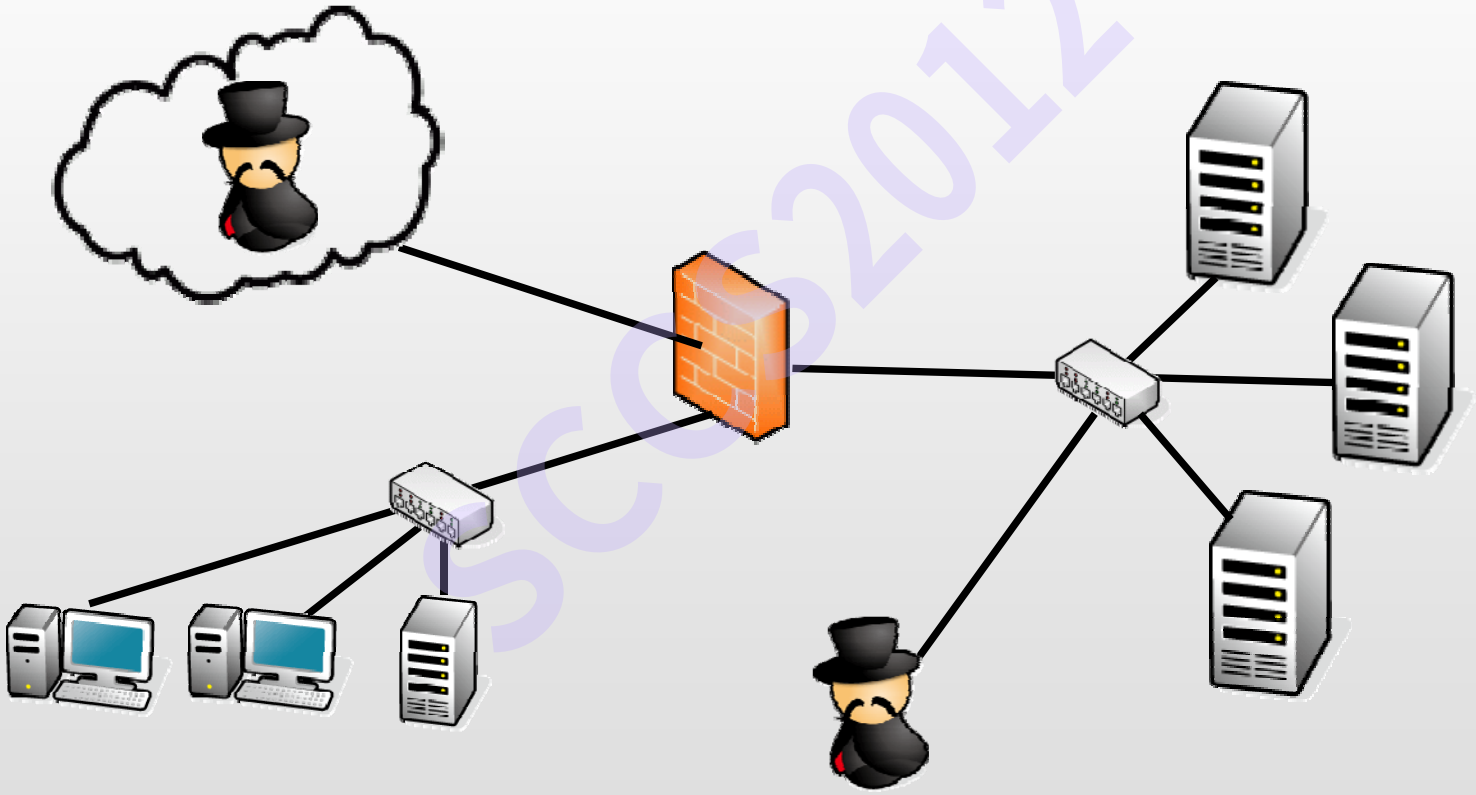
0x03. ペネトレの現場から

攻撃のシュミレーションですから…



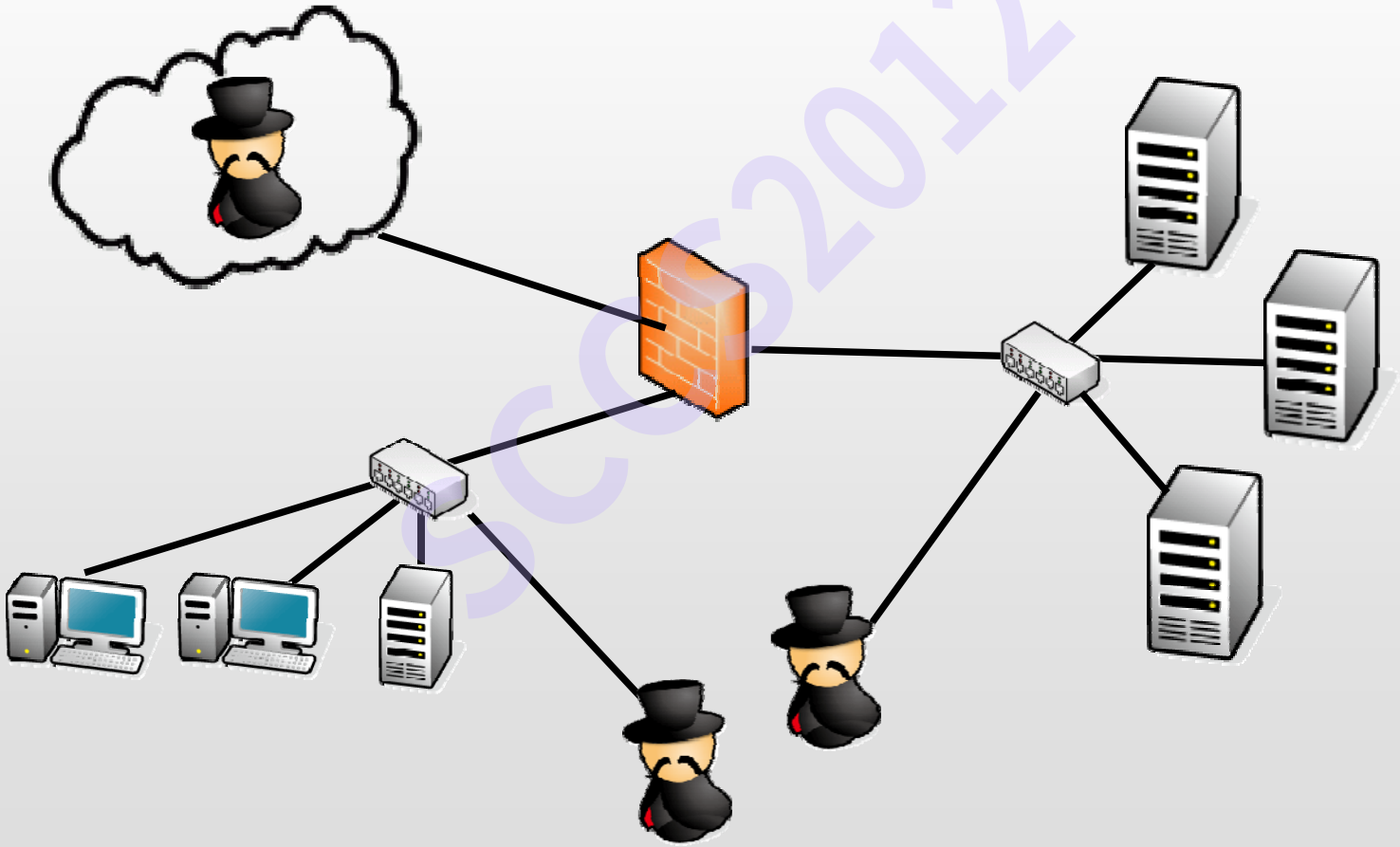
0x03. ペネトレの現場から

攻撃のシュミレーションですから…



0x03. ペネトレの現場から

攻撃のシュミレーションですから…



0x03. ペネトレの現場から

どんなことをするのか。

① 情報の収集

② 攻撃方法選定

③ 攻撃

0x03. ペネトレの現場から

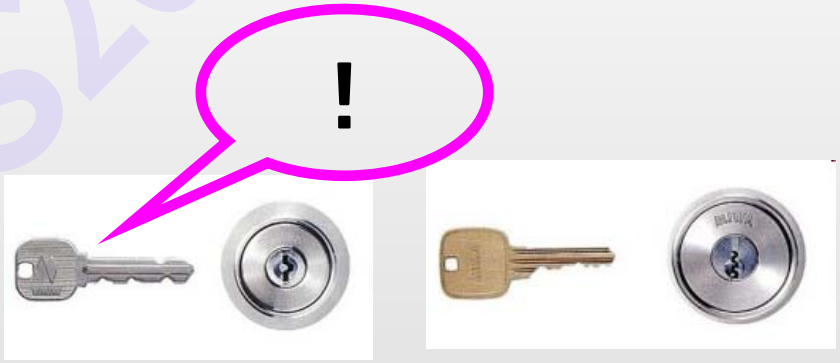
① 情報収集

通信可能な入り口（ポートオープン）の確認
OSやアプリケーションのバージョン推測
脆弱性が存在する可能性チェック

0x03. ペネトレの現場から

② 攻撃方法の考察

①により判明した情報から対象に
存在するであろう脆弱性の攻撃方法を考察



0x03. ペネトレの現場から

攻撃

②の考察により導き出された方法を用いて
対象の制御や機密情報の奪取を試みる。

0x03. ペネトレの現場から

奪取後は？

0x03. ペネトレの現場から

場合によっては終わり。

場合によっては始まり。

0x03. ペネトレの現場から

何が始まるのか？

0x03. ペネトレの現場から

範囲の拡大

① 下地の構築

② 権限の昇格

③ 情報の窃取

0x03. ペネトレの現場から

① 下地の構築

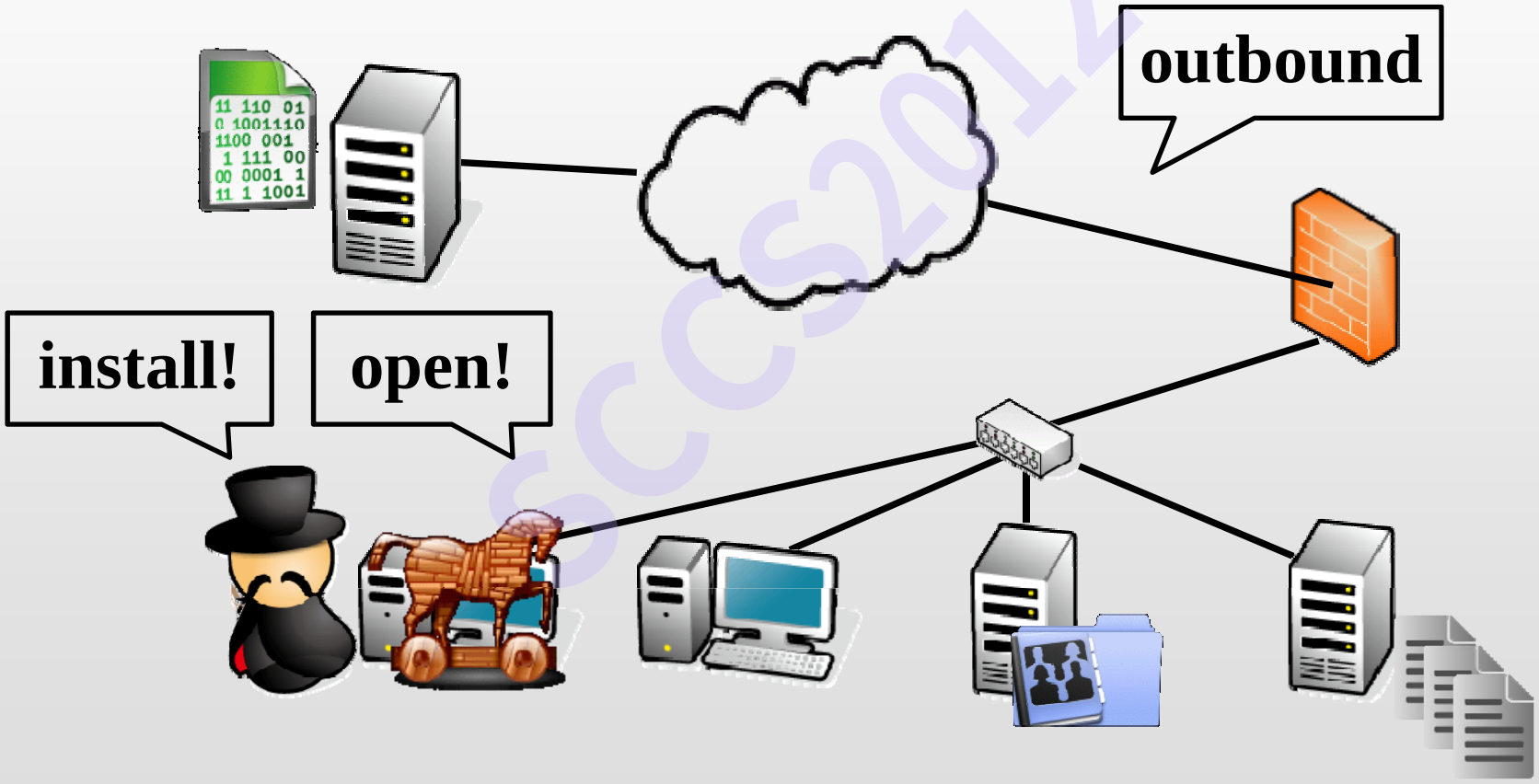
外部との通信

攻撃ツール設置

バックドア設置

0x03. ペネトレの現場から

下地の構築



0x03. ペネトレの現場から

外部との通信

- 最小限にしてる？
- プロクシ入ってる？
- ネットワーク監視してる？

0x03. ペネトレの現場から

攻撃ツール/バックドア設置

- 検知/blockの性能は？
- ネットワーク制御は？
- ソフトウェアは最新？

0x03. ペネトレの現場から

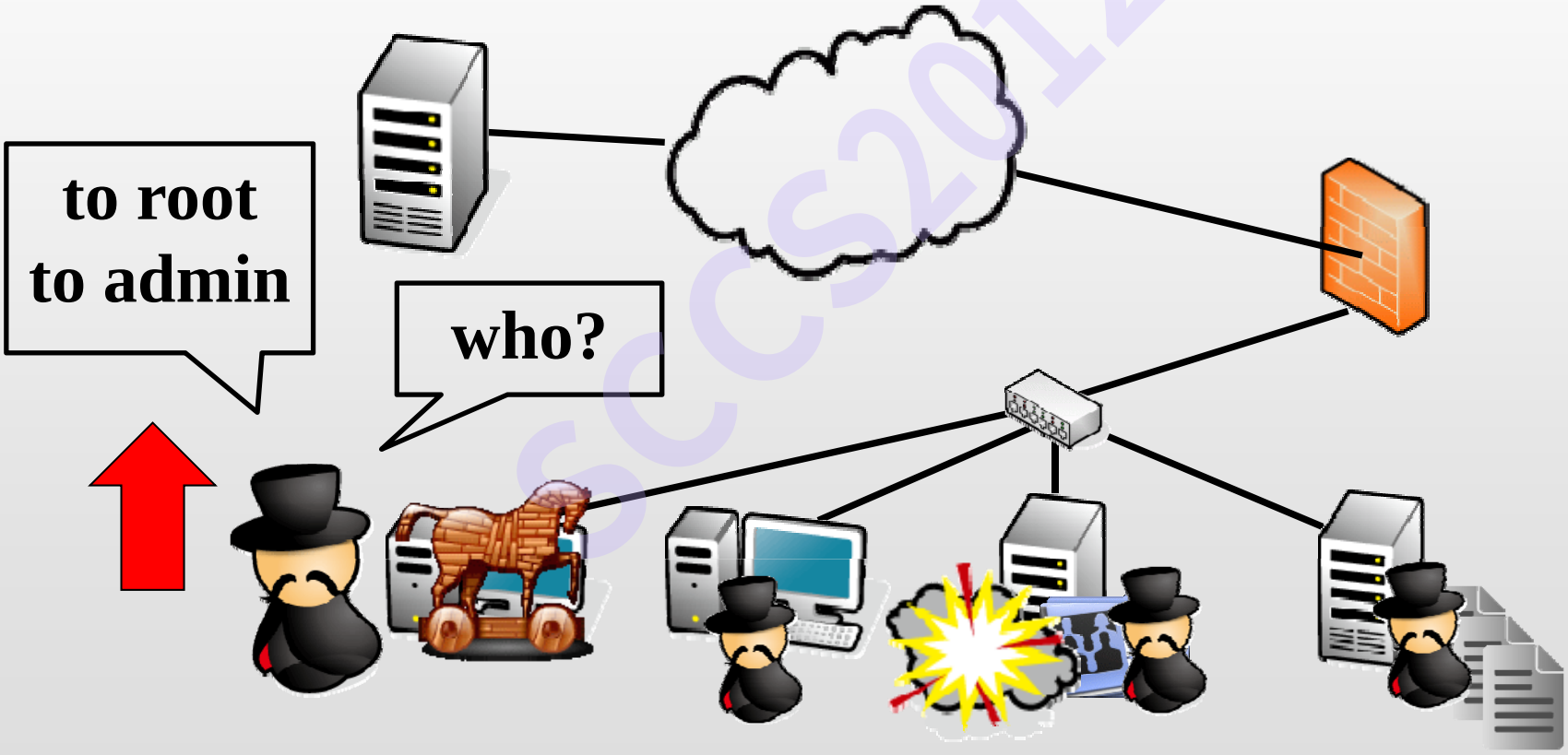
② 権限の昇格

奪取環境の確認

管理者権限/ADの奪取

0x03. ペネトレの現場から

② 権限の昇格



0x03. ペネトレの現場から

奪取環境の確認

- 実行コマンドの監視
- ログの保存設定は？

0x03. ペネトレの現場から

管理者権限/ADの奪取

- パスワードは？
- 不要なユーザ/権限は？
- ソフトウェアは最新？

0x03. ペネトレの現場から

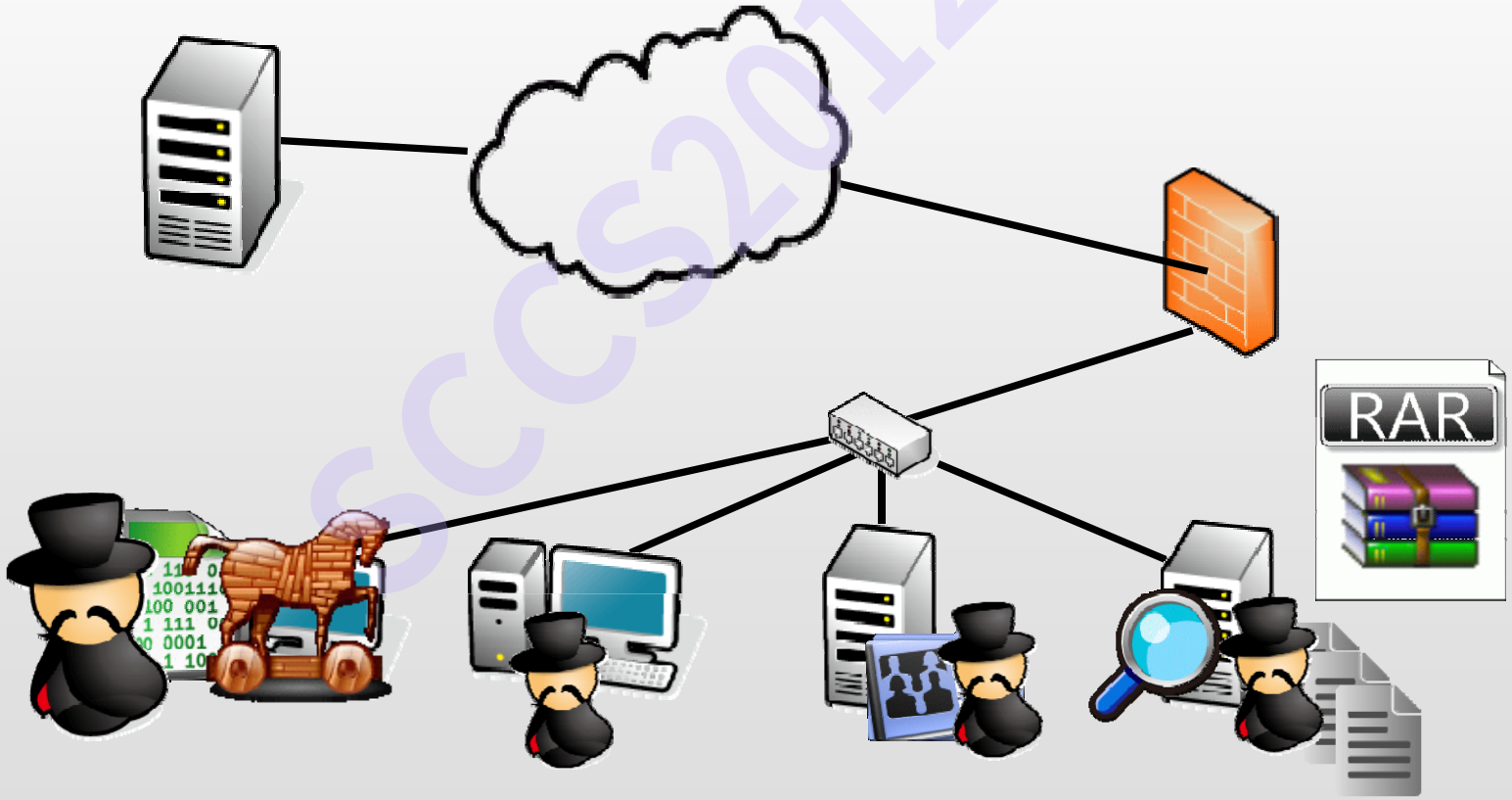
③ 情報の窃取

機密情報へのアクセス

外部への送信

0x03. ペネトレの現場から

③ 情報の窃取



0x03. ペネトレの現場から

機密情報へのアクセス

- 本当にそこにあるべき？
- アクセス権は適切？

0x03. ペネトレの現場から

外部への送信

- インターネットは必要？
- ネットワーク監視は？
- 重要情報の暗号化は？

0x03. ペネトレの現場から

別に真新しくはないですよね？

「新しいタイプの攻撃」

＝

「古いタイプの攻撃」の組合せ

0x03. ペネトレの現場から

別に真新しくはないですよね？

「古いタイプの攻撃」の組合せ

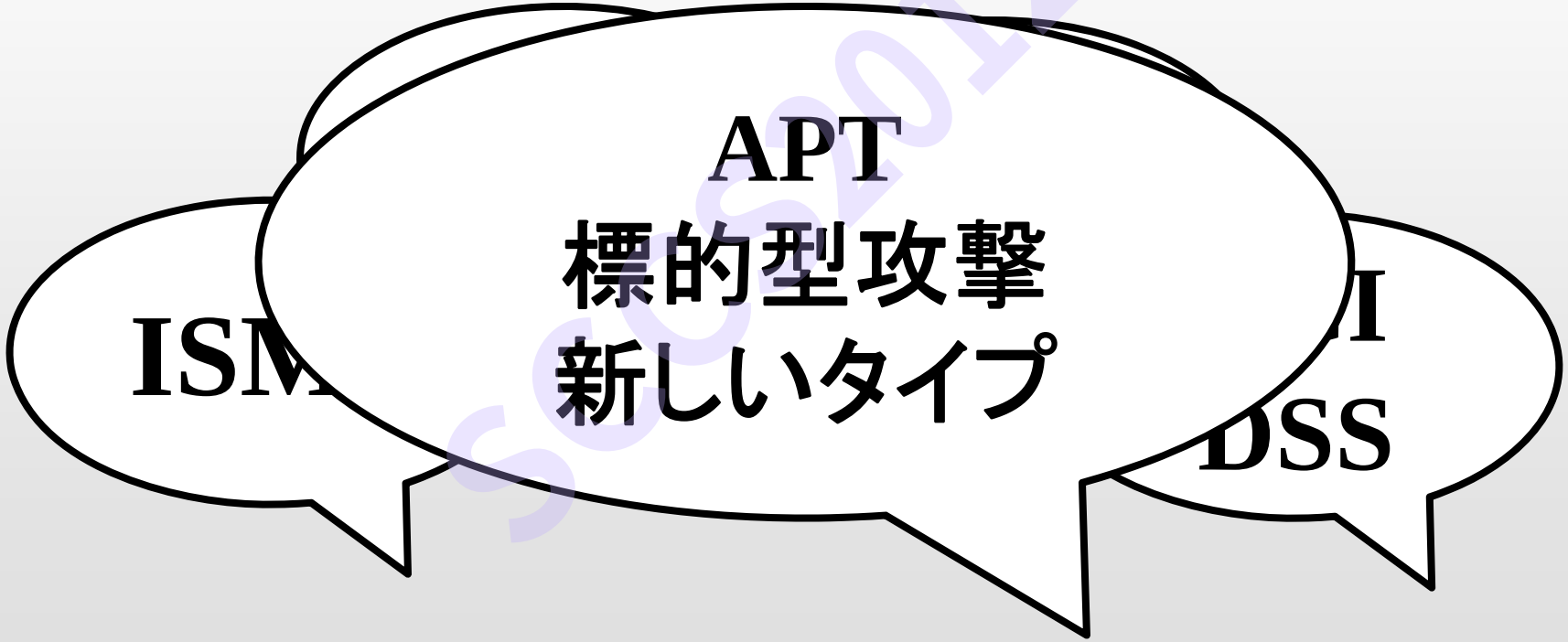
↑

「古いタイプの対策」の組合せ

0x04. 盛り上がりを見せる対策

0x04. 盛り上がりを見せる対策

巷には色々な製品が。



0x04. 盛り上がりを見せる対策

巷には色々な製品が。

同じ製品が看板を変えただけ。

言い換えれば

基本的な対策は同じ。

0x04. 盛り上がりを見せる対策

ただし、製品というのは

装備やサプリメントと同じ。

つまり

基礎、土台が必要。

0x04. 盛り上がりを見せる対策

標的型攻撃(ブーム)は

包括的な攻撃

自身を見直すいい機会。

0x05. さいごに

0x05. さいごに

大切になってくること。

再設計

0x05. さいごに

何が充分なのか？

何が不十分なのか？

0x05. さいごに

何が危ないのか？

どれくらい危ないのか？

0x05. さいごに

どこにある何を守りたいのか？

それはどこから狙われるのか？

0x05. さいごに

その目的は？

0x05. さいごに

汝と汝の敵を
知りましょう

0x05. さいごに

セキュリティ業界に限らず
「嘘・大げさ・紛らわしい」
が沢山あると思います。

0x05. さいごに

在りもしない脅威を
さも、そこに在るかのように
訴求してくるといった
「セキュリティ詐欺」

0x05. さいごに

何事においても
どこから発信されても
誰から発信されても
一考し、自身の目で真偽を。
そして、取捨選択してください。

0x05. さいごに

それが
「安全」を実現し
「安心」を得る
“セキュリティの基本”
だと思います。

0x05. さいごに

そして

0x05. さいごに

怪物と闘う者は
その過程で自らが
怪物と化さぬよう心せよ。

0x05. さいごに

セキュリティの仕事をして
危険を必要以上に
煽らないという点において

0x05. さいごに

怪物と闘う者として
その過程で
自らが怪物と化さぬよう
心しなければならない。

ご清聴ありがとうございました。