Hardening Project から学ぶインシデント対応の勘所

株式会社インターネットイニシアティブ
セキュリティ情報統括室

WASForum Hardening Project
実行委員

根岸 征史 @MasafumiNegishi

IIJ-SECT
IIJ Group Security Coordination Team

Hardening Project 2015

お伝えしたいこと

Hardening Project ってなに?

Hardening Project から得られたものは?

自己紹介

IIJグループの CSIRTチーム所属 (IIJ-SECT, 2001年結成)
https://sect.iij.ad.jp/

SANS JAPAN 公式インストラクター (2007〜)

OWASP Japan アドバイザリーボード (2012〜)

WASForum Hardening Project 実行委員 (2012〜)
http://wasforum.jp/hardening-project/

@ITで動画連載始めました!「セキュリティのアレ」← New!!

Hardening Project とは

Hardening Project

実践的な堅牢化技術の価値を最大化すること

WASForum(通称ワスフォーラム：ウェブアプリケーションセキュリティフォーラム) は、セキュリティ・イベント「Hardening Project」を実施してきました。このイベントは、最高の「守る」技術を持つトップエンジニアを発掘・顕彰するものであり、技術競技(コンペティション)の形式で実施しています。

ビジネスの視点

Focus on prevention techniques and process

最初の2012年４月に開催された「Hardening Zero」、ひき続いて同年10月には、よりチャレンジ力の求められる形として発展した「Hardening One」を実施してきました。

守る技術の顕彰

Engineering awards and talent discovery

2013年7月、さらなるアレンジを施した発展形として「Hardening One Remix」を開催。2014年はさらに進化をめざし、2014年6月、ついにHardening 10 APAC、「Hardening 10 Evolutions」として、競技とともに議論を深める技術交流の機会となりました。

利用者視点の認識向上

Perspective for stakeholder communication

2015年度の活動により、さらに堅牢化技術の価値を最大化することを目指してまいります。

WASForum Hardening Project 実行委員会
実行委員長 門林 雄基

Hardening Project の歴史

2012年　4月 Hardening Zero (東京)

2012年10月 Hardening One (東京)

2013年　7月 Hardening One Remix (東京)

2014年　6月 Hardening 10 APAC (沖縄)

2014年11月 Hardening 10 Evolutions (沖縄)

2015年　6月 Hardening 10 MarketPlace (沖縄)

2015年11月 Hardening 10 ValueChain (沖縄)

Hardening 10 ValueChain

8時間の耐久競技にインターネットの縮図を実現。よりリアルに。

新制度: プロフェッショナルによる
サービスの提供が可能です。
参加者が”オーダー”して出動します。

Eコマースサイトの”売上”と”稼働状況”を
リアルタイム・スコアボードに

参加者（10人 x 6 チーム想定）

参加者は与えられたショッピングサイトの売上を最大化するべく、チームワークを生かして行動していただきます

競技　演習　訓練

CTF (攻防戦形式、クイズ形式など)

重要インフラ事業者 (13分野 18セプター) 分野横断的演習 (NISC)

電力・ガス・ビル・化学分野のサイバーセキュリティ演習 (経済産業省)

実践的サイバー防御演習 CYDER (Cyber Defense Exercise with Recurrence) (総務省)

情報危機管理コンテスト (白浜シンポジウム)

Hardening → Softening

(1) Hardening Day: 実践の場
8時間耐久での堅牢化競技

(2) Softening Day: 学びの場
健闘の振り返り、気づき、学びを深める

(3) WASNight: 共有の場
発表することによる新たな気づき
得られた知見、経験を広める

MINI Hardening Project

過去の Hardening 参加者の中から有志が自主的に立ち上げた、初心者向けの競技イベント

東京、大阪でこれまでに 4回開催

http://minihardening.connpass.com/

https://twitter.com/minihardening

MINI Hardening

Hardening Project から得られたもの

H10VC
競技環境

10.2.xx.0/24
Global Router
.254
グローバルエリア
192.168.xx.0/24
.101
CHECKyy
CentOS 6.6
VPC
ルーター
.254
さくらのクラウドエリア
192.168.3.0/24
dm
CentOS 6.3
.1
win2008
Windows Server 2008
.2
lb
CentOS 6.3
.3
ec1
CentOS 6.3
.4
ec2
CentOS 6.3
.5
ec3
CentOS 6.3
.6
web1
CentOS 6.3
.7
vpn
CentOS 6.3
.8
8つのIPを1対1 NATする
公開サーバエリア
DNAT用にさらにIPアドレスは8つ
.253
Firewall（NICx4）
vyOS 1.1.5
.254
.254
.254
192.168.1.0/24
サポート端末
Window7
.1
サポート端末
Window8.1
.4
サポート端末
Window7
.2
サポート端末
Window10
.5
サポート端末
Window7
.3
サポート端末
CentOS6.7
.6
172.31.xx.0/24
踏み台クライアントエリア
172.30.xx.0/24
SSLVPN ルーター
ESSID：Teamyyaで接続
参加者端末
参加者端末
参加者端末
沖縄会場エリア
192.168.2.0/24
db-m
CentOS 6.3
.1
db-s
CentOS 6.3
.2
log
CentOS 6.3
.3
dns
CentOS 6.3
.4
ad
Windows Server 2008
.5
社内サーバエリア

インシデントへの対応

サービスの
安定稼動

売り上げの
最大化

サイト堅牢化に
必要な技術力

インシデント対応

臨機応変で
的確な対応力

重要な情報/システムの保護

脆弱性の発見、修正

外部サービスの活用

顧客/社外/社内への連絡

コミュニケー
ションカ

マネジメントカ

スコアボード

Hardening10ValueChain
Hardeningショップ売上推移 - 現在の1位は【5:現地集合検知改竄】です
1:ちゅーばーしんか[2637.228]
2:ちゃんぷるー[2639.308]
3:SUNSUNSUN[2585.848]
4:セキュ子の部屋[962.838]
5:現地集合検知改竄[3249.34]
6:秘密結社にんじんしりしり[2517.344]
♥:Kuromame6[4897.504]
5,000
4,000
3,000
2,000
1,000
0
0
20.48
40.96
61.44
81.92
102.4
122.88
143.36
163.84
184.32
204.8
225.28
245.76
#SLA推移#
1,636
1,227
818
409
0
1
2
3
4
5
6
♥
繁盛レベル
1:ちゅーばーしんか
息をしてないのっ！
2:ちゃんぷるー
16
3:SUNSUNSUN
14
Hardening Project 2015
4:セキュ子の部屋
05
5:現地集合検知改竄
20
6:秘密結社にんじんしりしり
14
♥:Kuromame6
10

シナリオ(1) 標的型攻撃

マルウェア感染の疑いがあり、外部に対して不審な通信を行っている可能性あり、とのメールが第三者から届く

そもそもどこの窓口に連絡がくるのか　WHOIS

外部への不審な通信とは何か、どうやって検知したのか

C2サーバ、DNS

何が起こっているのか

で、いったい何をすればよいのか

さあ動け！

社内関係部署への連絡
マルウェア感染端末の特定、調査
- Firewall, Proxy, DNS等のログの調査
- メモリ、ディスク等の証拠保全、調査
- マルウェア検体の保全、調査
感染原因の特定、調査
被害内容、影響範囲の特定
通信遮断、通信監視
社内への注意喚起
警察への被害届、外部への情報提供
外部へのアナウンス、顧客対応

視点と役割

視点：攻撃者、開発者、運用者、経営者、サービス提供者、インフラ事業者、…
(実際にその立場で関わるわけでなくても、その視点で物事がどう見えるか考える)

役割：リーダー、脆弱性対応、インフラ、アプリ、広報、…
(どのように連携して動くことが必要か)

その他のシナリオ例

実際のインシデント事例をもとに、緊迫感と臨場感のある実践的なシナリオを実施

DDoS攻撃による脅迫

広告からのマルウェア感染 (Malvertising)

Webアプリケーションの脆弱性による情報漏洩

ソフツトウェアの既知の脆弱性による Web改ざん

リスト型攻撃による不正ログイン

どうする?

サイトをどう止めるか

問題点をどう見つけるか

顧客にどう伝えるか

社内にどう伝えるか

情報をどう共有するか

準備がすべて！！

頭でわかっていても、いざインシデントが発生すると体が動かない

負荷のかかった状況で冷静に的確な対応をするには何が必要か

あらかじめ起こりうる事を想定して、やるべき事、判断基準、優先順位、役割分担をしっかり決めておくこと

想像力 → それぞれの行動がもたらす結果、影響についてあらかじめ考える

意思決定者はだれなのか

よくハマるポイント

視野狭窄に陥りがち

- 堅牢化した結果、自分達にも影響
- 業務に必要だから安易に止めちゃダメなサービス
- 競技環境として変更してはいけない設定変更

セキュリティサービスへの過信

攻撃者への責任転嫁

- 「脆弱性のあるサイトで買い物なんかしたくない」

まとめ

Hardening Project に興味をもっていただけたでしょうか?

Hardening / MINI Hardening Project にぜひ参加してみてください。お待ちしております！