



Metasploit 3.2

✂ ——— (° ▽ °) ——— ツ!

ყუმიდნო3 <dt> gmail.com



前置き (追加スライド)

- 実は最新のMetasploitを使うためのsvnチュートリアルが予定でした。
- でも、Metasploit 3.2がリリース～ (T-T;
- なので、3.2の内容も含めつつ機能紹介
- ちなみにではブラッディマンディがはやってるようなので、ブラッディマンディごっこ風味をいれてみた。
- 落ちがないですw



このプレゼン

- いまさらのMetasploitの紹介です
- 残念ながら3.2の紹介ではありません
- 一部、検証してないのがあるので突っ込みにしえできませんw(でも、うるかむ)
- ツールは許可された環境で使おう



Metasploitとは

- 誰でも
- 簡単に
- 脆弱性自体を動作テストできる
- 要するに脆弱性テスターにとっては欠かすことができないツールです
- 本格的なことでもできますよ



Metasploitとは

■ こんな感じで"exploit"を選択

Metasploit Framework GUI v3.2-any-day-now

System Window Help

Microsoft Server Service Relative Path Stack Corruption

MSF::Assistant

Review your configuration before clicking the **apply** button

Confirm settings

保存(S)

SMBPIPE : BROWSER
SSL : false
EnableContextEncoding : false
EXITFUNC : thread
ContextInformationFile :
PAYLOAD : windows/reflectivemeterpreter/reverse_tcp
DLL : C:/Documents and Settings/.../Application Data/msf3/data/meterpreter#metsrv.dll
SMB::pipe evasion : false
DCERPC::fake_bind_multi : true
SMBDirect : true
LPORT : 4444
RPORT : 445
RHOST : 1.1.1.1
LHOST : 10.212.197.128
TARGET : 0

キャンセル(C) 戻る(B) 適用(A)

■ こんな感じで"設定して実行



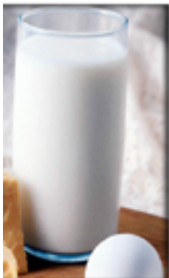
みんな何に使ってる？

- ペネトレテスト
- ブラッディ・マンデイごっこ
- 管理者が失踪したサーバにログイン
- それだけじゃないですよ？



その他の紹介

- まとめて便利なツールがインストール
(Windows版)
 - netcat
 - putty
 - VNC クライアント
 - vi
 - NASM
 - Nmap



Metevpreter

- 攻撃成功後に使うToolです
- 色々コマンドを実行できます
- 使い方
PAYLOADにwindows/meterpreter/bind_tcp等を指定
- コマンド抜粋
cat/cd/download/edit/getwd/ls/mkdir/pwd/rmdir/
upload/ipconfig/portfwd/route/getpid/getuid/kill/ps
詳しくはhelpと入力してね♪



Met ev pr et ev

■ 便利なコマンド

execute = コマンド実行-hで隠して実行もできます

use priv = 認証情報の取得

hashdump = 認証情報を表示 ⇒ C:\inに放り込む

timestamp = ファイルのタイムスタンプ(MACE)を変更

migrate <pid> = pidを書き換え(他のプロセスと同じにできる)

ほかにもスクリプトを作って実行とかもできます

参考デモ :

<http://jp.youtube.com/watch?v=TMkLUqfxSjs>

<http://www.learnsecurityonline.com/vid/MSF3-met/MSF3-met.html>



MITMツールとAutopwn

- MITMツール `Auxiliary>server>capture`
- `http/smtp/pop3/smb`などに対応

ettercapもある？さがし方がまずいのか見当たらないです

- Autopwn = Browser攻撃ツール
- `Auxiliary>server>browser_autopwn`
- 接続してきたクライアントのブラウザ/OS/パッチを判断 (javascript)
- 受動攻撃もテストできます。



Karmat+Metasploit

- Wifiアクセスポイントとして動作
- 正常な接続を乗っ取ります
- MITMツールと統合されています
- Aircrack-ngと一緒に使えます
(WEPキーの解析もやってくれます)

<http://blog.metasploit.com/2008/08/karmetasploit-wireless-fun.html>

<http://metasploit.com/dev/trac/wiki/Karmetasploit>



他にもあるんだけど

時間がないので調べきれってません・・・
仮眠好攻撃もできます。ポート固定です。

面白きうなの

- vdtproxyをパッチして使うWebエキテナ
- 白眼 (WinDBGの拡張モジュール)
- ペイロード作成ツール

3.2で追加されたものには触れてません(涙
みんなでいじってレポートしてください



最後に

- MetasploitはRubyです。
- Pythonじゃないので"ブラッディ・マンデイ"ズ
っここには不向きです
- なので、Rubyを使いましょう

- でも、私はPerlしか使えませぬorz

追記：

たとえば、perlを使った回もあったね
あと、バイナリを扱うにはpythonが楽チンみたいですよ