

# **Phishing: Going from Recon to Creds**

by Adam Compton and Eric Gershman

# Agenda

- Who Are We?
- What is Phishing?
- Standard Phishing Process
- New Tool - Yay!
  - Demo

# Who am I?

Adam Compton

- Father - 5 yrs
- Husband -15 yrs
- Pentester - 15 yrs
- Programmer - 34 yrs
- Hillbilly - 38 yrs

@tatanus

[adam.compton@gmail.com](mailto:adam.compton@gmail.com)

<https://github.com/tatanus>

<http://blog.seedsofepiphany.com/>

# Eric Gershman

- Husband - 2 years
- Security Hobbyist - 14 years
- SysAdmin - 10 years
- Security - 2 years

# Why Present on Phishing?

- Phishing is cool
- To say thank you to the community
- Present my phishing project

# What is Phishing?

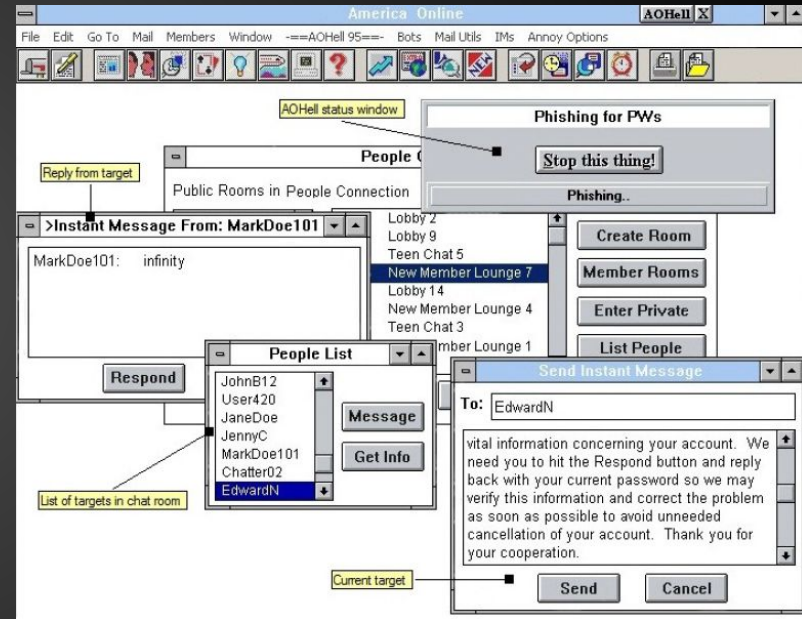
"Phishing is the attempt to acquire sensitive information...by masquerading as a trustworthy entity in an electronic communication." - Wikipedia (Phishing)

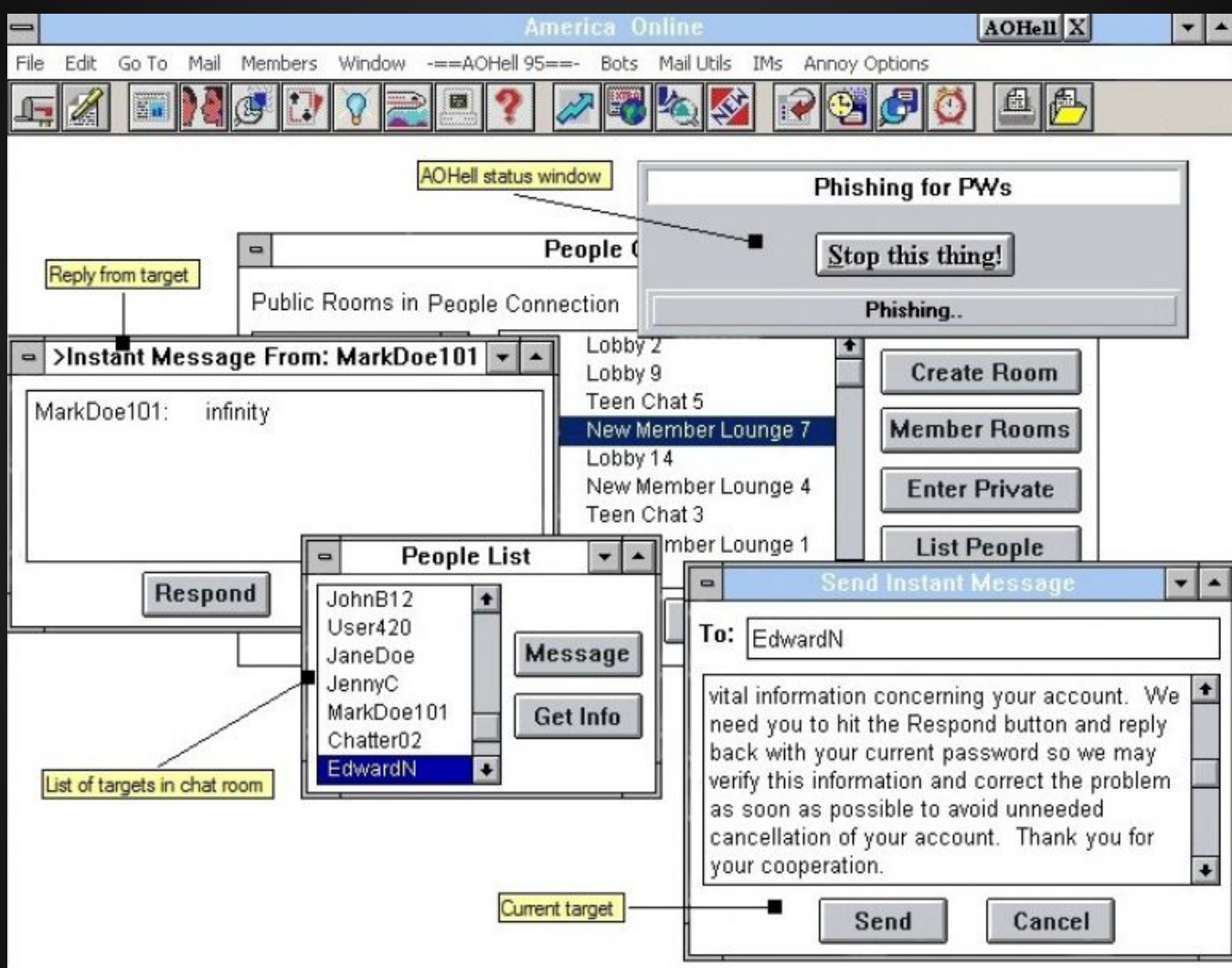
<http://en.wikipedia.org/wiki/Phishing>



# Phishing Like it's 1995

- Goes back to AOL
- Script Kiddies running AOL Progs
- Attackers Posing as AOL Admins via IM and Email







# What kind of sensitive info?

- Credentials - User/Pass
- Credit Cards
- Identity - PII
- Health Information
- Steam Games, Bitcoin Wallets

# Types of Attacks

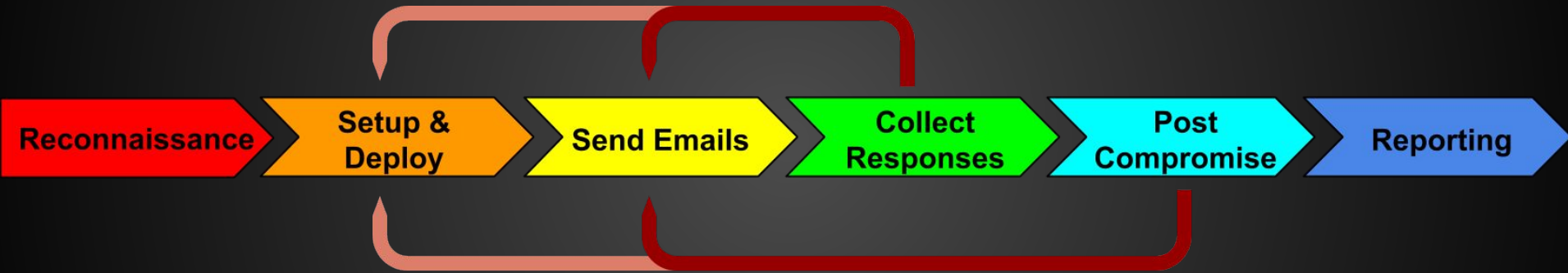
- Phishing - Usually no specific targets and for monetary gain
- Spear Phishing - specific individuals or groups
- Whaling - targeting executives

# Why Phish?

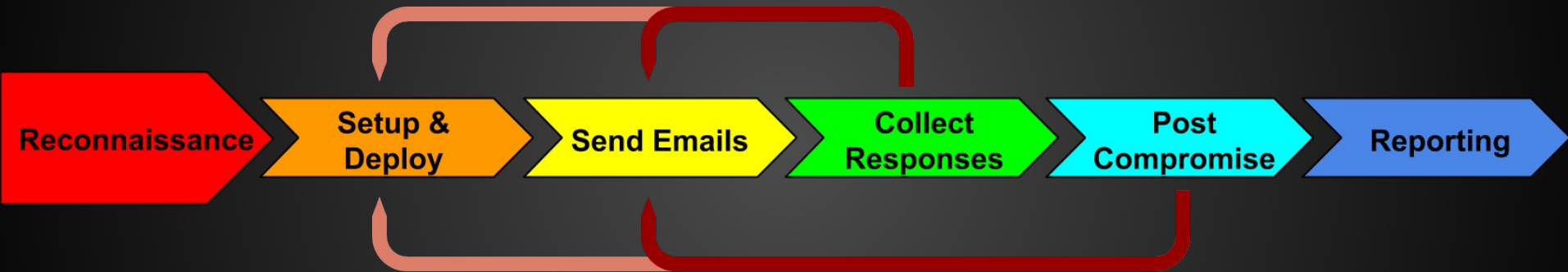
Q: Why phish when there are other attack vectors?

A: Because it works! Attack the people, not the computers.

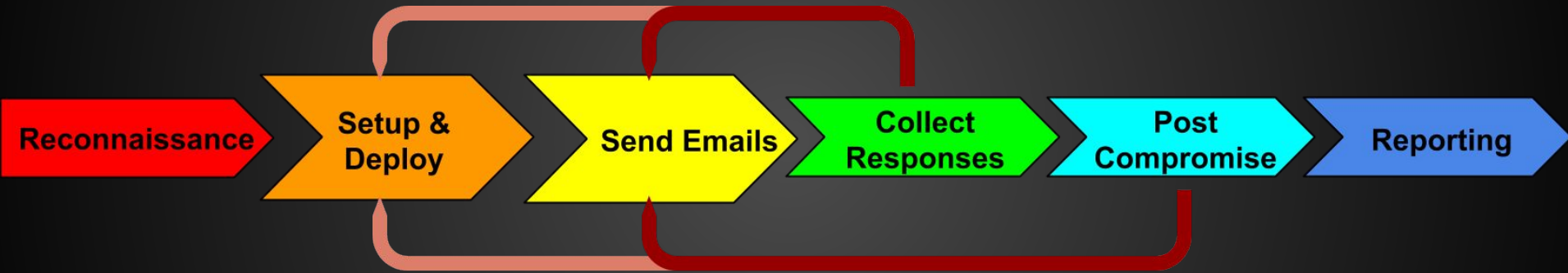
# Standard Phishing Process



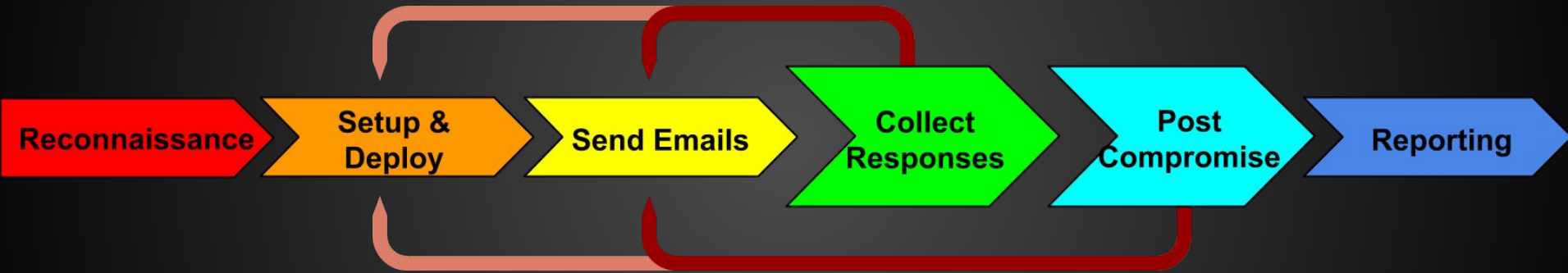
# Recon



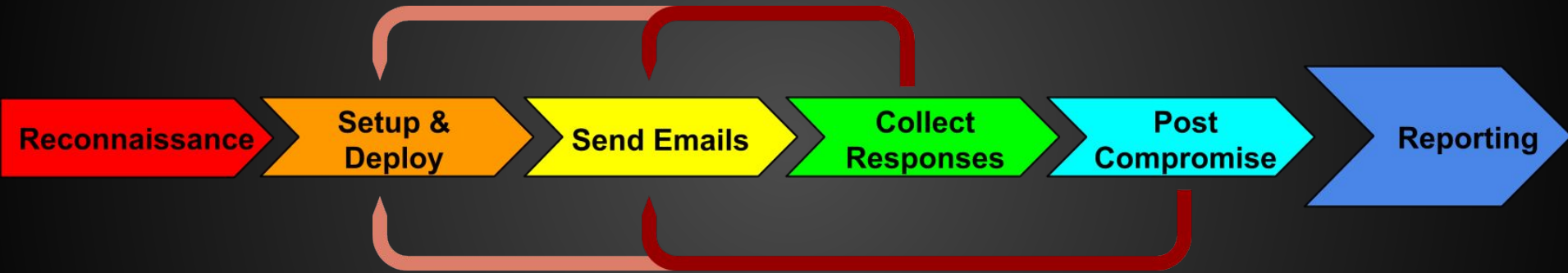
# Setup, Deploy & Send Emails



# Collect Responses & Post Compromise



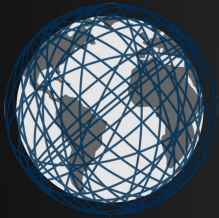
# Reporting





# Phishing Tools - Recon

MetaGoofil

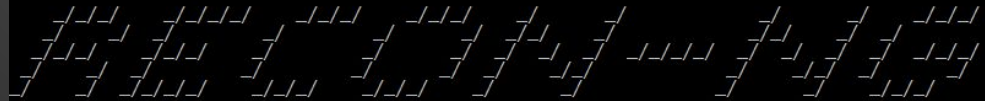


netglub

Really Open Source  
Information Gathering



```
$ python recon-ng.py
```



```
[recon-ng v1.00 Copyright (c) 2013, Tim Tomes (@LaNMaSteR53)]
```



# Phishing Tools - Attack

- SET
- Phishing Frenzy
- BeEF



# I am lazy - Can we make this even easier?

Yes...Automation!

- Program APIs
  - BeEF RESTFul API
  - Recon-cli
  - SET - seautomate
- Parse Commandline Tool Output
- Python, Perl, & Bash

# SpeedPhishing Framework - SPF

- Automates common tasks needed to perform a phishing exercise
- Written in Python
- Minimal external dependencies

Download source from:

<https://github.com/tatanus/SPF>

# Current Features

- Harvests Email Address
- Setups & Hosts Websites
- Sends phishing emails to targets
- Records Creds and Keystrokes
- Creates Simple Report

# SPF - Usage Statement / Options

```
usage: spf.py [-h] [-f <list.txt>] [-C <config.txt>] [--all] [--test]
              [--recon] [-e] [--dns] [-g] [-s] [--simulate] [-w] [-W] [--adv]
              [--profile] [--pillage] [-d <domain>] [-p <domain>]
              [-c <company's name>] [--ip <IP address>] [-v] [-y]
```

## optional arguments:

-h, --help	show this help message and exit
-d <domain>	domain name to phish
-p <domain>	newly registered 'phish' domain name
-c <company's name>	name of company to phish
--ip <IP address>	IP of webserver defaults to [192.168.1.123]
-v, --verbosity	increase output verbosity

## input files:

-f <list.txt>	file containing list of email addresses
-C <config.txt>	config file

# SPF - Config File

```
[MISC]
PHISHING_DOMAIN: example.com
DOMAIN_NAME:
EMAILS_MAX: 100
EMAIL_DELAY: 1
DATABASE: spf.sqlite

[TEMPLATES]
WEB_TEMPLATE_PATH: templates/web/
EMAIL_TEMPLATE_PATH: templates/email/

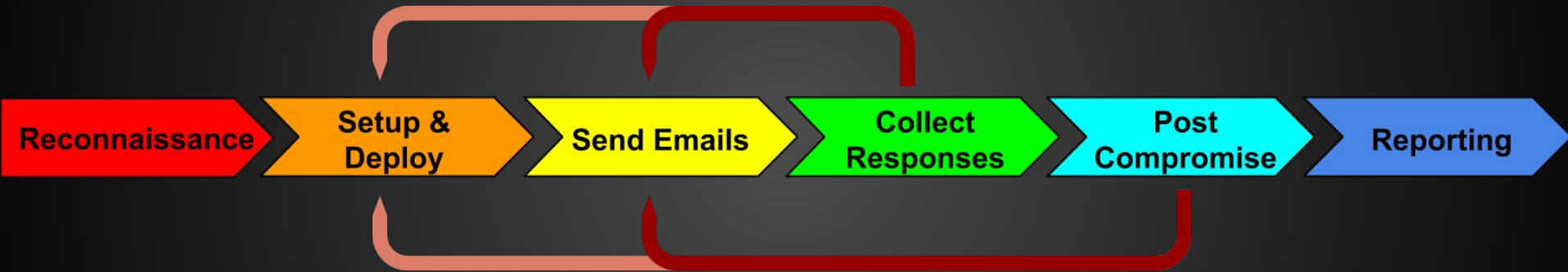
[SMTP]
DETERMINE_SMTP: 1
USE_SPECIFIC_SMTP: 0
SMTP_SERVER: smtp.gmail.com
SMTP_USER: XXXX
SMTP_PASS: XXXX
SMTP_FROMADDR: XXXX
SMTP_PORT: 25
```

```
[EXTERNAL_TOOL_PATHS]
THEHARVESTER_PATH: /usr/bin/theharvester
BEEF_PATH: /usr/bin/beef-xss

[ADDITIONAL_ATTACKS]
ENABLE_KEYLOGGING: 1

[WEB]
ENABLE_HOST_BASED_VHOSTS: 1
DEFAULT_WEB_PORT: 80
VHOST_PORT_MIN: 8000
VHOST_PORT_MAX: 9000
```

# SPF - Standard Phishing Process





# SPF - Reconnaissance

- Searches online search engines like Google, Bing, and DuckDuckGo
- Can use external tools such as:
  - theHarvester

# SPF - Identifying Potential Targets

```
[*] Obtaining list of email targets
[*] [VERBOSE] Gathering emails via built-in methods
[*] [VERBOSE] Currently searching [google, bing, ask, dogpile, yan
[*] [VERBOSE] [Processing: /] Google
[*] [VERBOSE] [Processing: -] Bing
[*] [VERBOSE] [Processing: /] Ask
[*] [VERBOSE] [Processing: /] Dogpile
[*] [VERBOSE] [Processing: -] Yandex
[*] [VERBOSE] [Processing: /] Baidu
[*] [VERBOSE] [Processing: /] Yahoo
[*] [VERBOSE] [Processing: |] DuckDuckGo
[*] [VERBOSE] Gathered [67] email addresses from the Internet

[*] [VERBOSE] Collected [64] unique email addresses
[*] -----
[*] EMAIL LIST
[*] -----
[*] -555-555-0199@example
[*] .com.me@example
[*] 20someone@example
[*] 555-555-0199@example
[*] GTUBE1.1010101@example
[*] MyEmailAddress@example
[*] Myname@example
[*] Someone@example
[*] _qhw@example
[*] account@example
[*] accounts@example
[*] admin@example
[*] another.person@example
[*] anotherperson4@example
[*] anotheruser@example
[*] aric-kunde@example
[*] bob@example
[*] clark.kent@example
[*] def@example
[*] demo@example
[*] description@example
[*] email2@example
[*] email3@example
[*] email@example
[*] escaped@example
[*] example@example
[*] fern-block@example
[*] fred-smith@example
```

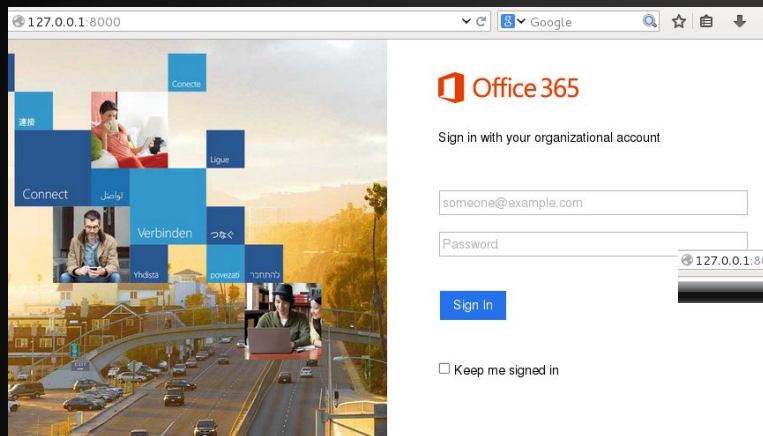
# SPF - Setup and Deploy

- Builtin web server based on Twisted python library
- Templated sample web sites with accompanying email templates
- Ability to dynamically clone additional login portals as needed

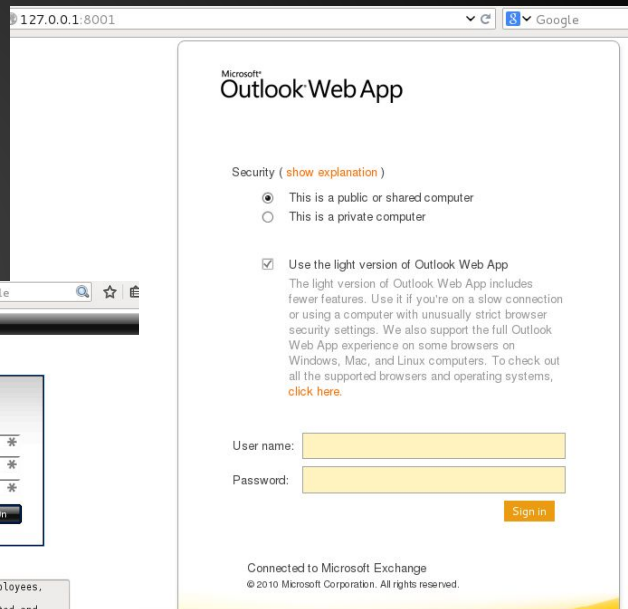
# SPF - Loading Web Sites

```
[*] Starting phishing webserver
[*] [VERBOSE] Found the following web sites: [templates/web/owa/CONFIG]
[*] [VERBOSE] Found the following web sites: [templates/web/citrix/CONFIG]
[*] [VERBOSE] Found the following web sites: [templates/web/office365/CONFIG]
[*] [VERBOSE] Started website [office365] on [http://192.168.59.128:8000]
[*] [VERBOSE] Started website [owa      ] on [http://192.168.59.128:8001]
[*] [VERBOSE] Started website [citrix   ] on [http://192.168.59.128:8002]
[*] [VERBOSE] Created VH0ST [office365.example.com] -> [http://192.168.59.128:8000]
[*] [VERBOSE] Created VH0ST [owa.example.com      ] -> [http://192.168.59.128:8001]
[*] [VERBOSE] Created VH0ST [citrix.example.com    ] -> [http://192.168.59.128:8002]
[*] [VERBOSE] Started WebServer with pid = [4181]
```

# SPF - Web Sites



**\*\*NOTICE\*\*:** These systems are solely for the use of authorized employees, consultants and/or agents of the target company and its worldwide subsidiaries and affiliates. Unauthorized use is strictly prohibited and subject to civil and criminal penalties. All usage of the systems must be in compliance with the Code of Ethics, Employee Handbook(s), and consultant/agency agreements, as applicable. All persons accessing these systems hereby consent to the monitoring, recording, disclosure, retention (as required by law and/or document retention standards in place at the company) and transfer (to other countries other than where the user is based) of all system usage information. System usage information includes, but is not limited to, system ID, LAN ID, all electronic content produced by the user, email account, instant messaging account, mainframe ID, and system passwords. System usage information may be used for managing the workforce, communications and emergencies, business operations, compliance and other legal, regulatory, audit and business purposes. By accessing these systems, the user consents to all terms as described above. (C2)



# SPF - Sending Emails

- Can simulate sending of emails
- Sends emails in a round robin style alternating across all phishing sites
- Sends emails via 3rd party SMTP server or by connecting directly to the target's mail server



# SPF - Sending Emails

```
[*] [VERBOSE] Locating phishing email templates
[*] [DEBUG] Found the following email template: [templates/email/owa.txt]
[*] [DEBUG] Found the following email template: [templates/email/citrix.txt]
[*] [DEBUG] Found the following email template: [templates/email/office365.txt]
```

```
[*] Sending phishing emails
[*] Would have sent an email to [0199@example.com] with subject of [Webmail - Office 365], but this was just a test.
[*] Would have sent an email to [555-555-0199@example.com] with subject of [New OWA Server], but this was just a test.
[*] Would have sent an email to [Abc..123@example.com] with subject of [New Login Portal], but this was just a test.
[*] Would have sent an email to [Abc.@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [COMMITTEE@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [MyEmailAddress@example.com] with subject of [Webmail - Office 365], but this was just a test.
[*] Would have sent an email to [Someone@example.com] with subject of [New OWA Server], but this was just a test.
[*] Would have sent an email to [abarnes@example.com] with subject of [New Login Portal], but this was just a test.
[*] Would have sent an email to [account@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [admin@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [alguien@example.com] with subject of [Webmail - Office 365], but this was just a test.
[*] Would have sent an email to [alias@example.com] with subject of [New OWA Server], but this was just a test.
[*] Would have sent an email to [anna@example.com] with subject of [New Login Portal], but this was just a test.
[*] Would have sent an email to [ayticcc@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [b@atlanta.example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [bar@example.com] with subject of [Webmail - Office 365], but this was just a test.
[*] Would have sent an email to [ceo@example.com] with subject of [New OWA Server], but this was just a test.
[*] Would have sent an email to [contact@example.com] with subject of [New Login Portal], but this was just a test.
[*] Would have sent an email to [cris@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [dbmaster@example.com] with subject of [Updated Citrix Server], but this was just a test.
[*] Would have sent an email to [email@example.com] with subject of [Webmail - Office 365], but this was just a test.
```

# SPF - Collect Responses & Post Exploitation

- Logs all access to the web sites
- Logs all form submissions
- Logs all key strokes
- Has ability to pillage email accounts (via pillage module)




# SPF - Collecting Results

```
[*] ::citrix2:: 2015.07.23-11.35.32,[KEYLOGGING],127.0.0.1,keylog=['u']
[*] ::citrix2:: 2015.07.23-11.35.32,[KEYLOGGING],127.0.0.1,keylog=['s']
[*] ::citrix2:: 2015.07.23-11.35.32,[KEYLOGGING],127.0.0.1,keylog=['e']
[*] ::citrix2:: 2015.07.23-11.35.32,[KEYLOGGING],127.0.0.1,keylog=['r']
[*] ::citrix2:: 2015.07.23-11.35.33,[KEYLOGGING],127.0.0.1,keylog=['2']
[*] ::citrix2:: 2015.07.23-11.35.33,[KEYLOGGING],127.0.0.1,keylog=['[TAB]']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['p']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['a']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['s']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['s']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['w']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['o']
[*] ::citrix2:: 2015.07.23-11.35.34,[KEYLOGGING],127.0.0.1,keylog=['r']
[*] ::citrix2:: 2015.07.23-11.35.35,[KEYLOGGING],127.0.0.1,keylog=['d']
[*] ::citrix2:: 2015.07.23-11.35.35,[KEYLOGGING],127.0.0.1,keylog=['2']
[*] ::citrix2:: 2015.07.23-11.35.35,[KEYLOGGING],127.0.0.1,keylog=['[ENTER]']
[*] ::citrix2:: 2015.07.23-11.35.35,[KEYLOGGING],127.0.0.1,keylog=['\r']
[*] ::citrix2:: 2015.07.23-11.35.35,[CREDENTIALS],127.0.0.1,password=['password2'], user=['user2'],
```

# Reports

- Saves all data and activity logs to assessment specific directory structure
- Generates simple HTML report

  
**INITECH**

**T.P.S REPORT**  
COVER SHEET

Prepared By: \_\_\_\_\_ Date: \_\_\_\_\_  
System: \_\_\_\_\_ Program Language: \_\_\_\_\_ Platform: \_\_\_\_\_ OS: \_\_\_\_\_  
Unit Code: \_\_\_\_\_ Customer: \_\_\_\_\_  
Unit Code Tested: \_\_\_\_\_  
  
Due Date: \_\_\_\_\_ Approved By: \_\_\_\_\_  
Test Date: \_\_\_\_\_ Tested By: \_\_\_\_\_  
Total Run Time: \_\_\_\_\_ Total Error Count: \_\_\_\_\_  
Error Reference: \_\_\_\_\_  
Errors Logged: \_\_\_\_\_ Log Location: \_\_\_\_\_  
Passed: \_\_\_\_\_ Moved to Production: \_\_\_\_\_  
Comments: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

CONFIDENTIAL

# SPF - Simple Report

## Report for Phishing Exercise against [example ]

The phishing engagement was started on [2015/05/14 20:24:13 ] and ran through [2015/05/14 20:37:52 ].

For this exercise, the domain [example.com ] was registered and used for the phishing attacks.

### Phishing Campaign : citrix

#### SAMPLE EMAIL:

TO:  
FROM: XXXX  
SUBJECT: Updated Citrix Server

Due to recent issues with the Citrix gateway and growing Internet based threats, we have deployed an updated access server.

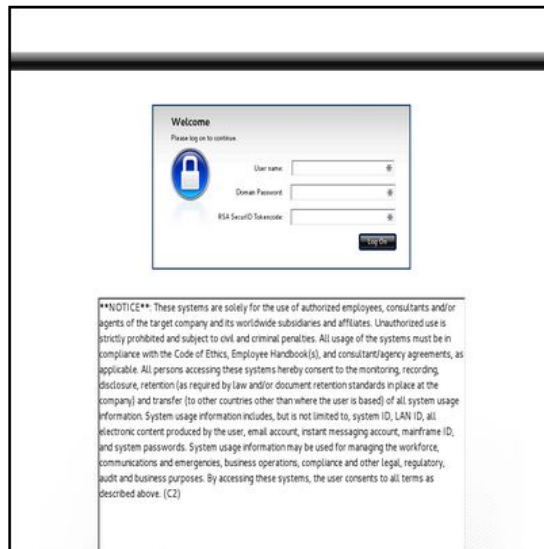
<http://citrix.example.com>

Please verify that you can access the site.

Service Desk, Information Technology

#### TARGET EMAIL ADDRESS(es):

20someone@example



<http://192.168.59.128:8002>

#### CAPTURED CREDENTIALS:

```
2015.05.14-20.34.51,[CREDENTIALS],127.0.0.1,username=['user1'], token=['123456'], password=['passw0rd']
2015.05.14-20.35.01,[CREDENTIALS],127.0.0.1,username=['test'], token=['1232'], password=['bob']
```

# Advanced/Experimental Features

- Company Profiler
  - Identify which if any templates should be used
  - Dynamically generate new "target-specific" phishing sites
- Pillage
  - Verify credentials
  - Download attachments
  - Search for "SSN, password, login, etc...)

# SPF Demo

We shall all now pray to the demo gods

# Future Work/Features

- Unique Ids to track specific emails
  - More external tools
  - Better Profiling/Pillaging
  - Fancy Reports
  - Incorporate SSL (possibly via <https://letsencrypt.org/>).
- 
- Suggestions?

Download SPF tool from: <https://github.com/tatanus/SPF>

# 411

@tatanus

[adam.compton@gmail.com](mailto:adam.compton@gmail.com)

<https://github.com/tatanus>

<http://blog.seedsofepiphany.com/>

@EricGershman

[eric@ericgershman.com](mailto:eric@ericgershman.com)

<https://github.com/EricGershman>

Download SPF tool from:

<https://github.com/tatanus/SPF>

# A HUGE Thank You to:

Recon-ng - Tim Tomes (lanmaster53)

BeEF - Wade Alcorn

theHarvester - Christian Martorella

Social Engineering Toolkit - Dave Kennedy

...



# Thank You!

