Inspired-Sec

Penetration Testing tips and tricks that will hopefully make your struggles at least a little bit better :)

Spear Phishing 101

MAY 7, 2017

TAGS: PHISHING, SERVER-SETUP

Spear phishing is one of the most useful tools available to gain initial access in an environment. At its core Phishing is essentially a form of social engineering designed to entice a user to reveal sensitive information, or run a payload to compromise their system. Running a successful Phishing campaign requires a few different resources and some

setup. In this post I will go over the process I use to setup and run a successful Phishing campaign.

Target Identification

The first step in a successful phishing campaign is to know your target. For the purpose of this post, our target will be the fictitious organization ACME LLC.

There are a few things that we need to know about ACME to conduct the campaign.

1. Is this a Linux or Windows Based environment?
2. How are their email addresses formatted?
3. Is there a public login portal for the organization?
4. Does the organization implement email filtering?

The answers to these questions will help establish a good baseline and give us the information we need to start setting up the campaign. However, these questions are not all inclusive, and the more time you spend researching the target organization, the better; enumeration is critical.

I usually start by searching through Linkedin. I have found a lot of information by looking through employee Linkedin profiles and job postings. By determining the skills required

for a new employee, and the skills of their current employees, you can learn a lot about the organization's infrastructure.

For example, if the there is a job available for a Splunk Engineer, C# Developer, and a SOC operator. We can reasonably assume that they are using Splunk, have a SOC to respond to threats, and are primarily a Windows environment.

Another great source of OSINT can be the corporate website. These websites often have a lot of information, such as email addresses, job postings, and background information on the organization that can be useful when crafting a template.

To identify email addresses, I prefer to use a tool called SimplyEmail, made by @Killswitch_GUI. This tool was built to be an expansion of the popular tool "The Harvester."

Another tool used to conduct reconnaissance is recon-ng. Recon-ng is a full-featured Web Reconnaissance framework written in Python. It comes loaded with independent modules and useful built-in functions. Null-Byte did an excellent overview of the tool that is available here.

Infrastructure Setup

After identifying the target and some information about the target environment, I start to setup infrastructure. The first thing needed to set up infrastructure is a few domain names. To find good domain names, I turn to expireddomains.net. Here, you can search through a list of domains that have expired to buy one that is categorized already and similar to your target.

Expired Domains.net

Expired Domain Name Search Engine

Search for Domain Names

Expired Domains | Deleted Domains | Domain Lists | Links

Domain Name Search

acme.com

Show Filter (About **8,013** Domains)

Next Page »

Domain	BL	DP	ABY	ACR	SimilarWeb	STC	Dmoz	C	N	O	D	TLDs Reg	SG	CO	List	Status	RL
Atop**Acme**.com	0	0	-	0	0	-	-					0	0	0	Expired	Available	
hv**acme**ridian.com	1	1	2015	4	0	-	-					1	0	0	Name.com	Backorder	
AcmeCelebs.com	547	20	2002	423	0	-	-					1	10	0	Dynadot	Make Offer	
AcmeRecording.com	15	3	1999	66	0	-	-					3	20	4	Dynadot	Make Offer	
AcmeMaterials.com	11	2	1998	31	0	-	-					2	50	10	Dynadot	Make Offer	
hv**acme**chanicaltraining.com	0	0	2007	16	0	-	-					1	0	0	SnapNames	Backorder	
Go**Acme**Plumbing.com	0	0	-	0	0	-	-					1	0	0	SnapNames	Backorder	
AcmeEmergency.com	0	0	2012	7	0	-	-					1	0	0	SnapNames	Backorder	
aahv**acme**chanicalllc.com	0	0	-	0	0	-	-					1	0	0	SnapNames	Backorder	
acmemorials.com	7	2	2008	16	0	-	-					1	0	0	GoDaddy	5 USD	
fabio**acme**107.com	16	5	2007	69	0	-	-					0	0	0	GoDaddy	5 USD	
AcmeBeerBox.com	0	0	2013	9	0	-	-					1	10	26	GoDaddy	11 USD	
acmeledoutdoormovies.com	0	0	-	0	0	-	-					1	0	0	GoDaddy	5 USD	
Mackin**acMe**moriesPhoto.com	0	0	-	0	0	-	-					4	0	0	GoDaddy	9 USD	
acmedu.com	95	1	2013	9	0	-	-					2	0	0	Expired	Available	
m**acme**dicals.com	0	0	-	0	0	-	-					0	0	0	Expired	Available	
acmebarandgrillmyrtlebeach.com	13	1	2013	5	0	-	-					0	0	0	Expired	Available	
AcmeTechnoSoft.com	847	4	2007	6	0	-	-					0	0	0	Expired	Available	
AcmeAbatementContractor.com	1	0	-	0	0	-	-					0	0	0	Expired	Available	
AcmeArtAndFraming.com	0	0	2011	7	0	-	-					0	0	0	Expired	Available	
AcmeBargainClub.com	13	0	2013	9	0	-	-					0	0	0	Expired	Available	
AcmeBud.com	2	0	-	0	0	-	-					0	0	0	Expired	Available	
AcmeGlassTulsa.com	0	0	2012	4	0	-	-					0	0	0	Expired	Available	
AcmeMils.com	0	0	-	0	0	-	-					0	0	0	Expired	Available	
AcmePrintConcepts.com	0	0	-	0	0	-	-					0	0	0	Expired	Available	

Next Page »

Domainhunter is a great tool that searches through Expireddomains.net for any expired domains with a previous history of use. It can optionally query for domain reputation against services like BlueCoat and IBM X-Force.

After selecting your domain name, it's time to begin setup. Each operator tackles infrastructure differently, but here is how I prefer to do it.

For each engagement, I set up three servers. They are as follows:

1. Payload Host, and Command and Control Server
2. SMTP Server
3. Redirection Server

I prefer to use Cobalt Strike to host payloads and manage C2 channels.

For an SMTP Server, I prefer to use a combination of Postfix and Dovecot. This combination allows for the segregation from the C2 server and supports IMAP to handle user responses. I made a script to automate most of the setup process. For detailed instructions, you can refer to this post.

To use this server with GoPhish, follow these instructions.

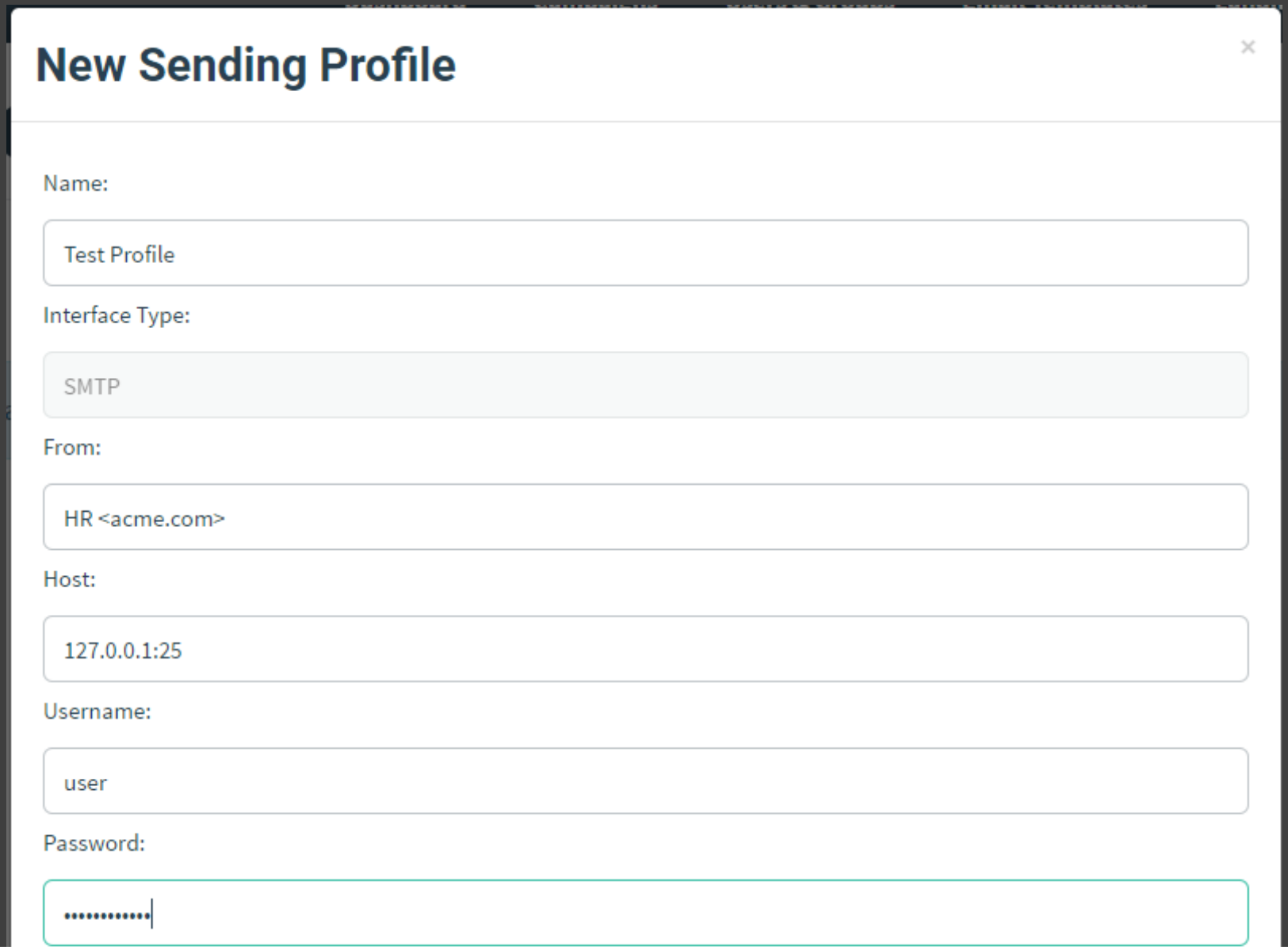
1. Install GoPhish by downloading and extracting the lastest release.
2. After extraction, edit the configuration file "config.json."

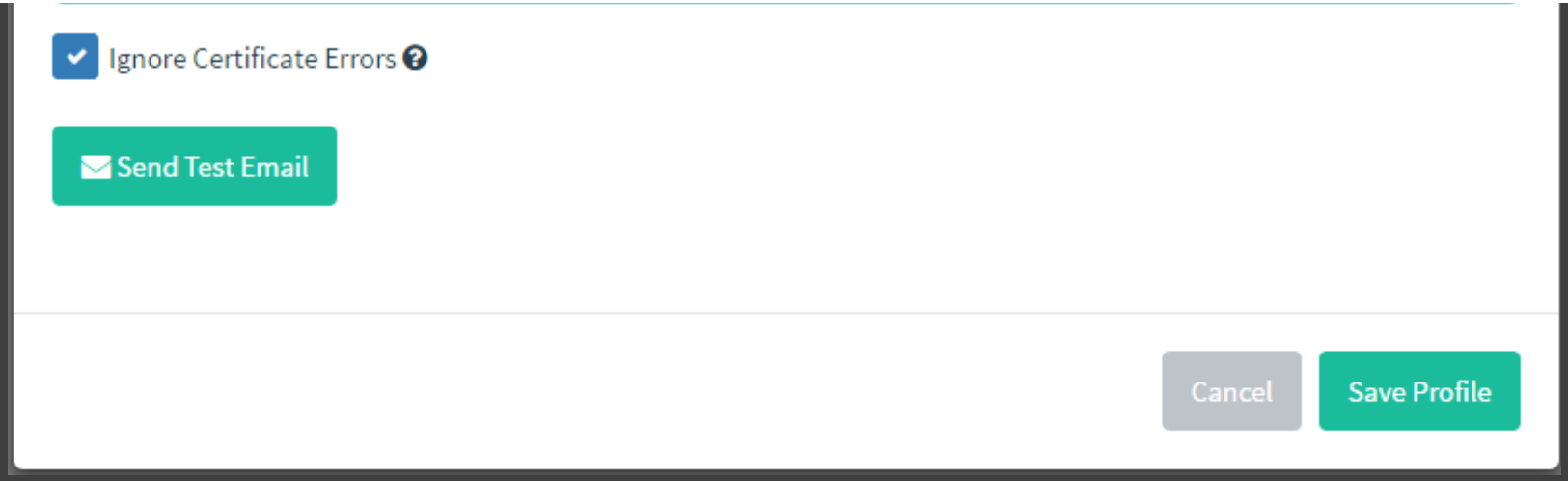
3. If you are running the mail server locally, change “host: stmp.example.com:25” to “host: localhost:25”, and the username/password appropriately.
4. If you are running the mail server on another server; Set the mail server to accept the GoPhish server as a relay, and set “host: stmp.example.com:25” to “host: Mail Server IP:25”, and the username/password appropriately.

Here is an example configuration:

```
{
        "admin_server" : {
                "listen_url" : "0.0.0.0:3333",
                "use_tls" : false,
                "cert_path" : "example.crt",
                "key_path" : "example.key"
        },
        "phish_server" : {
                "listen_url" : "0.0.0.0:80",
                "use_tls" : false,
                "cert_path" : "example.crt",
                "key_path": "example.key"
        },
        "smtp" : {
                "host" : "127.0.0.1:25",
                "user" : "user",
                "pass" : "P@ssword123!"
        },
        "db_path" : "gophish.db",
        "migrations_path" : "db/migrations/"
}
```

After setting the configuration file, we need to add a sending profile. Here is the sending profile configuration associated with the configuration shown above.





Finally, the last server will handle payload redirection. This server will proxy our payload to the user, or redirect them away from the server. This server serves a few primary functions.

1. Allow live hot swapping of payloads
2. Protect the location of our Command and Control Server
3. Deliver operating system specific payloads, and handles mobile users

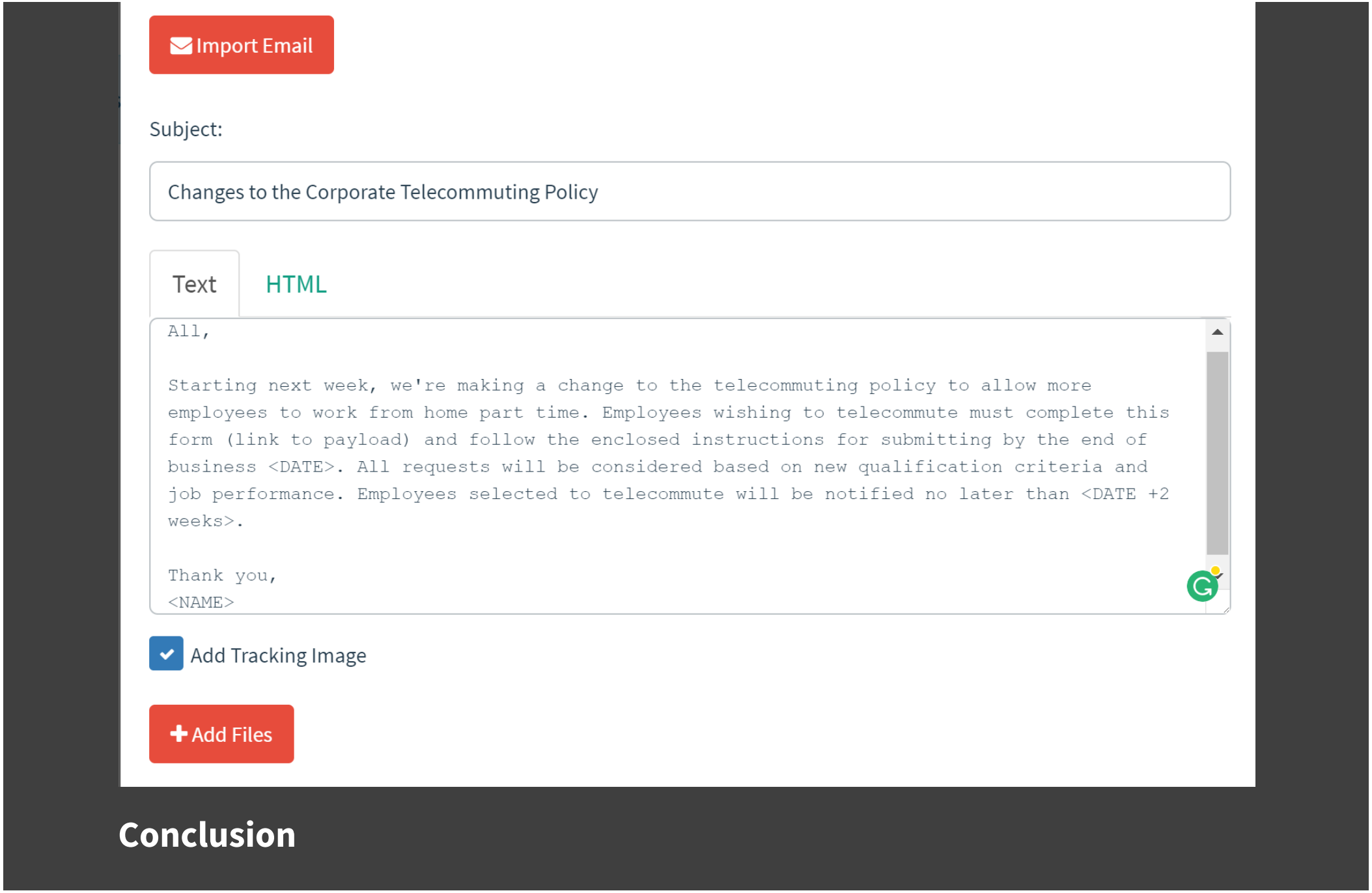
I made a script to automate most of the setup process. For detailed instructions, you can refer to this post. For more information of Mod_Rewrite, Jeff Dimmock has done a lot of excellent research on this topic and it can all be found on his here

Template Creation

A template can single-handedly make or break a campaign. The template is what entices the user to reveal sensitive information or run a payload and compromise their system. Templates can be simple or complex, but the best appeal to the user's emotions. Fear, greed, curiosity, desire and sex are some of the topics I found to be especially potent.

Let's make a template for the ACME organization. Our template will be informing employees of a change in the telework policy.

Here is the template:



Conclusion

By now we have conducted OSINT on our target, created the backend infrastructure required to support the engagement, and created some templates to send. These are great first steps in carrying out a successful phishing campaign. Remember, this guide is not perfect, and neither am I. I wanted to share the process I go through during a phishing engagement to help others and learn more myself.

If you have any suggestions to add to the post, or issues with any of the content posted here, feel free to let me know, and I will make changes accordingly. :)

« Mod_Rewrite Automatic Setup

Inspired-Sec

jcatrambone94
nOpe_sled

Penetration Testing tips and tricks that will hopefully make your struggles at least a little bit better :)