Gophish Phishing Simulation Tool

Janice Mitchell

We covered a lot of different tools in this class, but one area we didn't really get into includes the tools used to keep all employees within an organization educated and mindful about their company's security.

Given that, I wanted to take this opportunity to test out a phishing email simulator and see what goes into crafting an email as well as what the reporting structure looks like on the back end and how that data can be effectively put to use.

The program I worked with was gophish, installed on a Kali Linux VM. It's based on the go programming language.

Background & Topics Covered Today

- Research and Preparation
- Installation and Setup
- Deploying Campaign
- Dashboard and Results
- Benefits for the Organization

In determining what tool I would work with, I looked at several industry lists ranking different simulators and then, when I had it narrowed down, viewed the user guides available for each one as well as youtube tutorials that were available, which helped me with my final decision to move forward with gophish. And, as I came up against issues while working with the program, the gophish github repository was extremely helpful in identifying solutions.

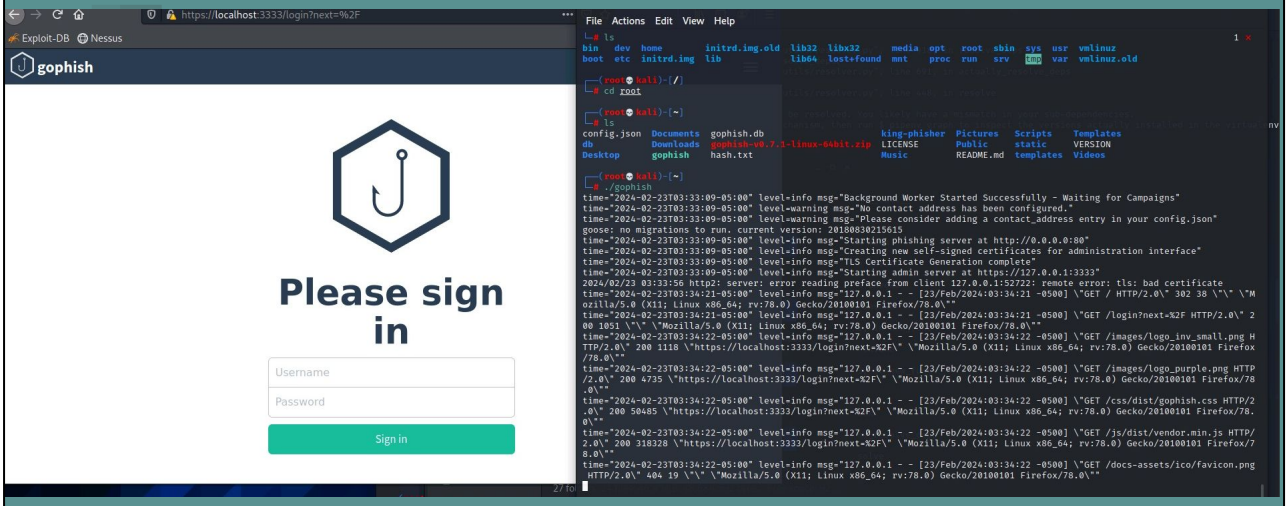
So today I'll cover the initial installation and setup, the details of deploying a phishing campaign, an overview of the dashboard to view and interpret campaign results, and finally, discuss the cybersecurity concepts at play, and the benefits to an organization using this tool and type of testing.

Installation/Setup

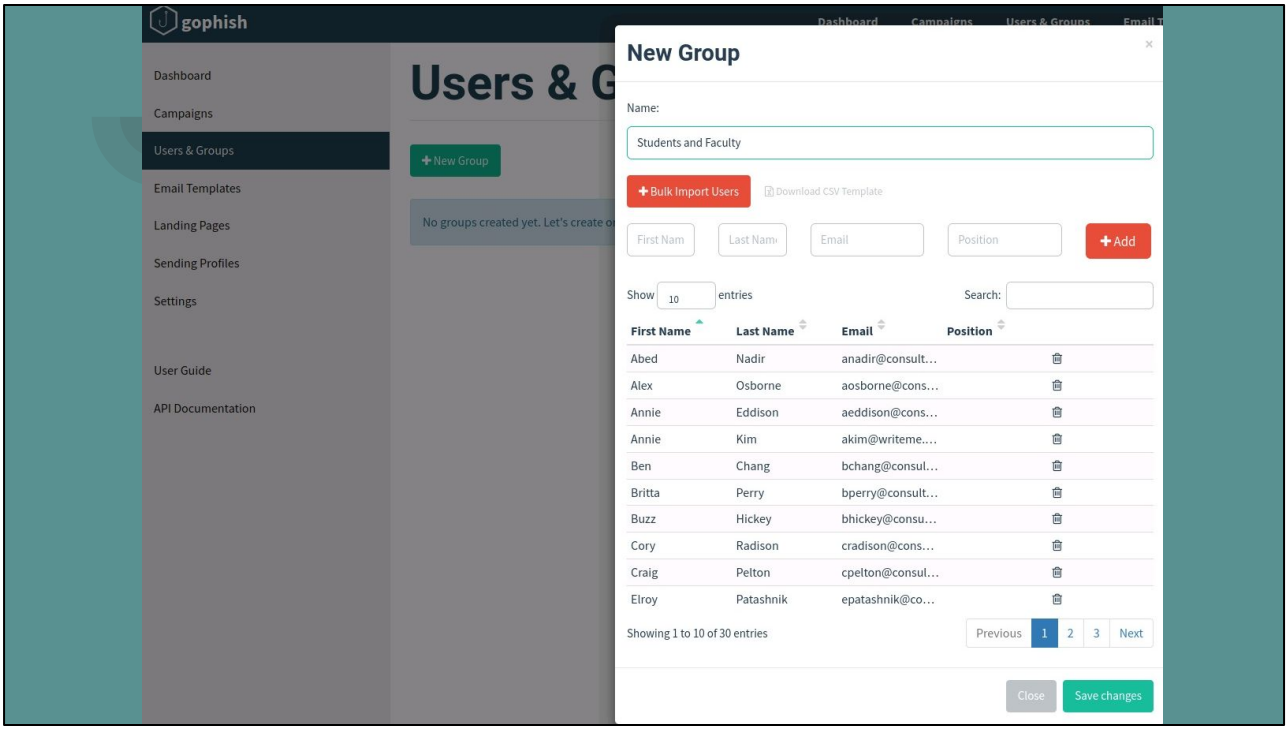
We'll start off with installation and setup

From here on out, use cursor to point out specific fields/buttons/etc as we go through the slides

Root# go get github.com/gophish/gophish

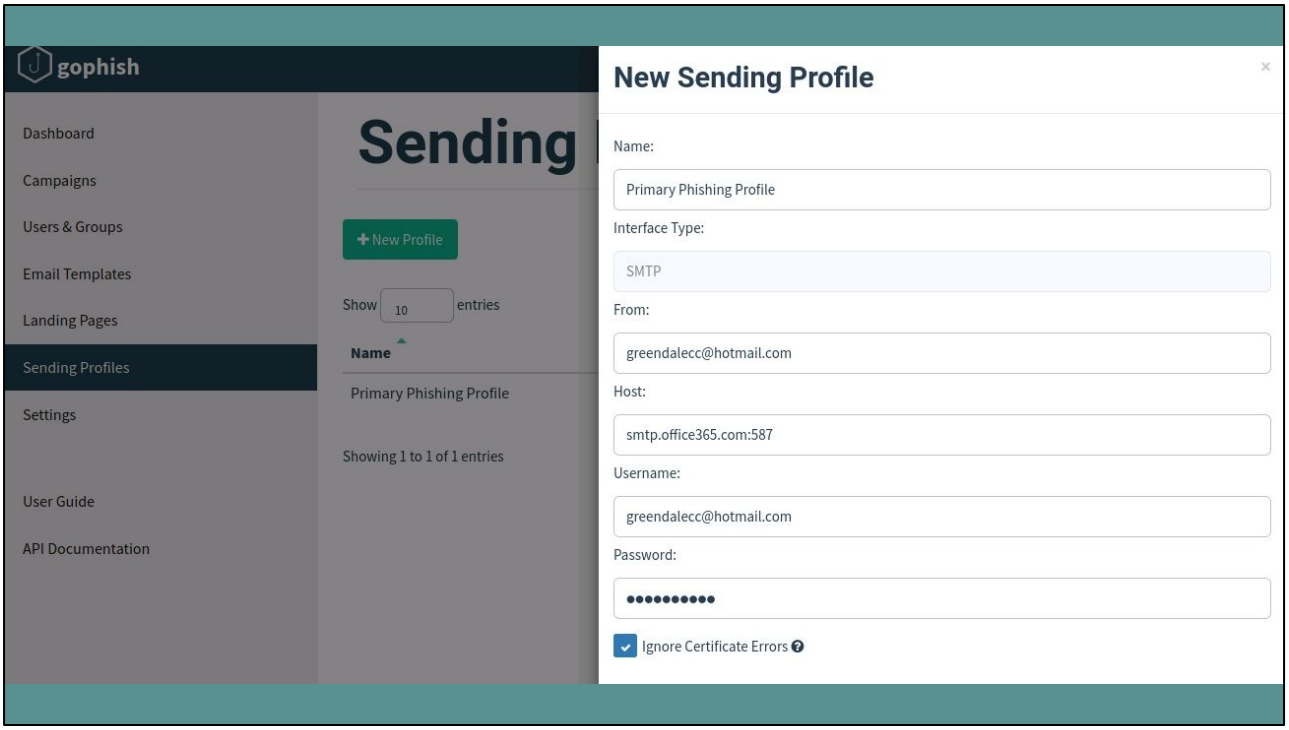


After confirming the system has the go programing language installed, use the go get github command to download the program. Once completed, gophish will appear in the selected directory - here you can see it's in the home directory. Launch gophish and it will start the phishing server, create self signed certificates and load the admin server. Once complete, navigate to the address for the admin server in your web browser and you will be taken to the sign in page. Default credentials are admin/gophish and can be changed after your first sign-in.



Once signed in as the admin, you can begin to load in your email addresses through the Users and Groups page. Using the bulk import option, you can upload an entire database of users quickly via .csv file versus keying in users individually.

If you want to send targeted campaigns to different departments, you can create multiple groups here instead of one like I have. When you are creating your campaign to be sent later, you can choose as many of the created groups as you'd like for the recipients list.

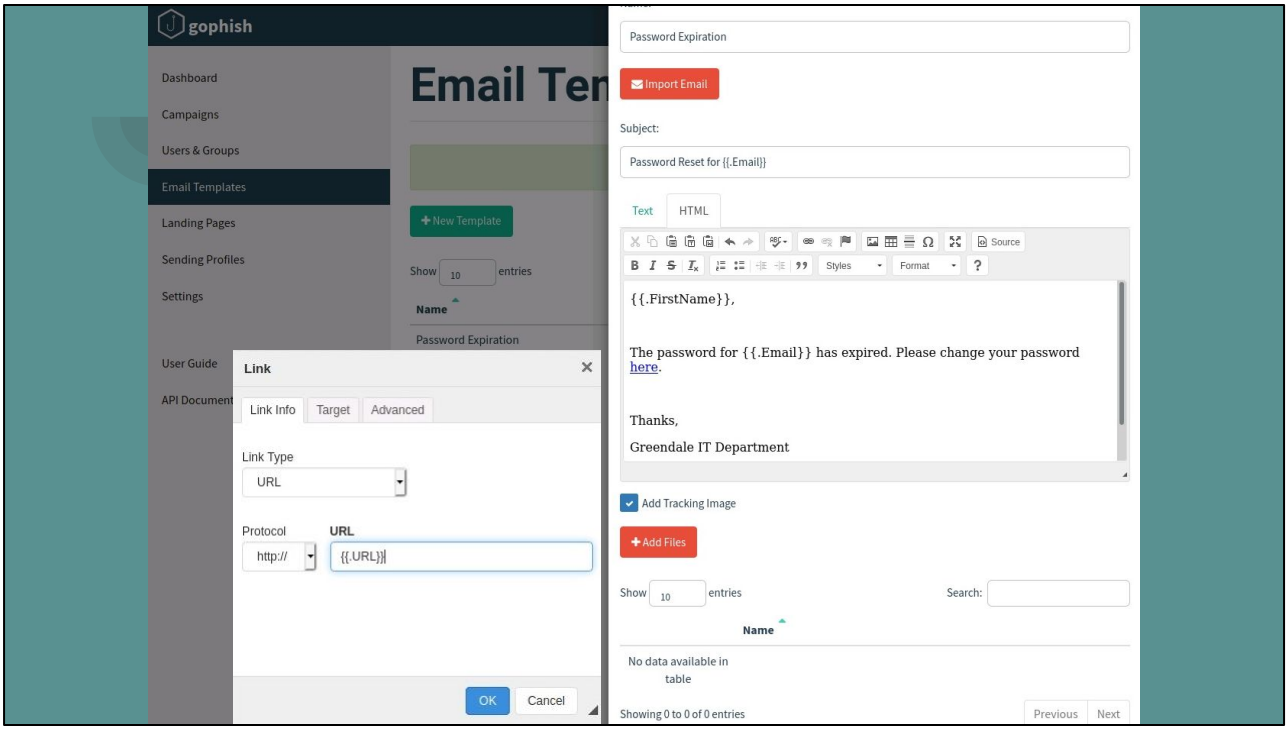


Next, you will set up your Sending Profile. This is the information for the email address your messages will be sent from. You do need to use a real email address and have the SMTP server details for the associated email host. In this case I used a hotmail address, and hotmail uses smtp.office365.com through port 587.

If you want to change the displayed name on the final emails to something different, you can edit the "from" field, so long as the username and password are filled in properly for your sending email address.

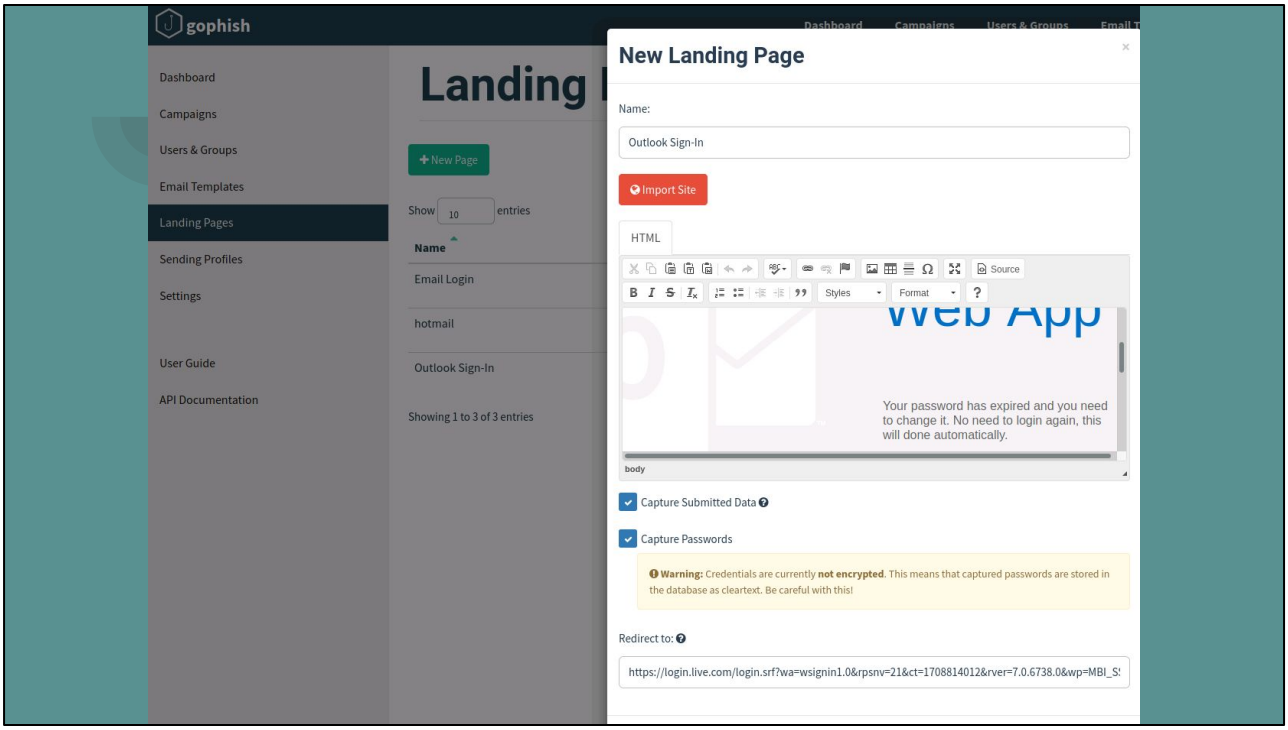
Campaign Creation

From here we can move to the details for what will be sent out with a campaign.



Email Templates is the section that allows you to specify what the email received by your targets will look like. To personalize with details from the .csv file already uploaded for your recipients, you just reference the desired field like this (point out Firstname& email sections w/ cursor). We'll see what this ends up looking like in a few slides.

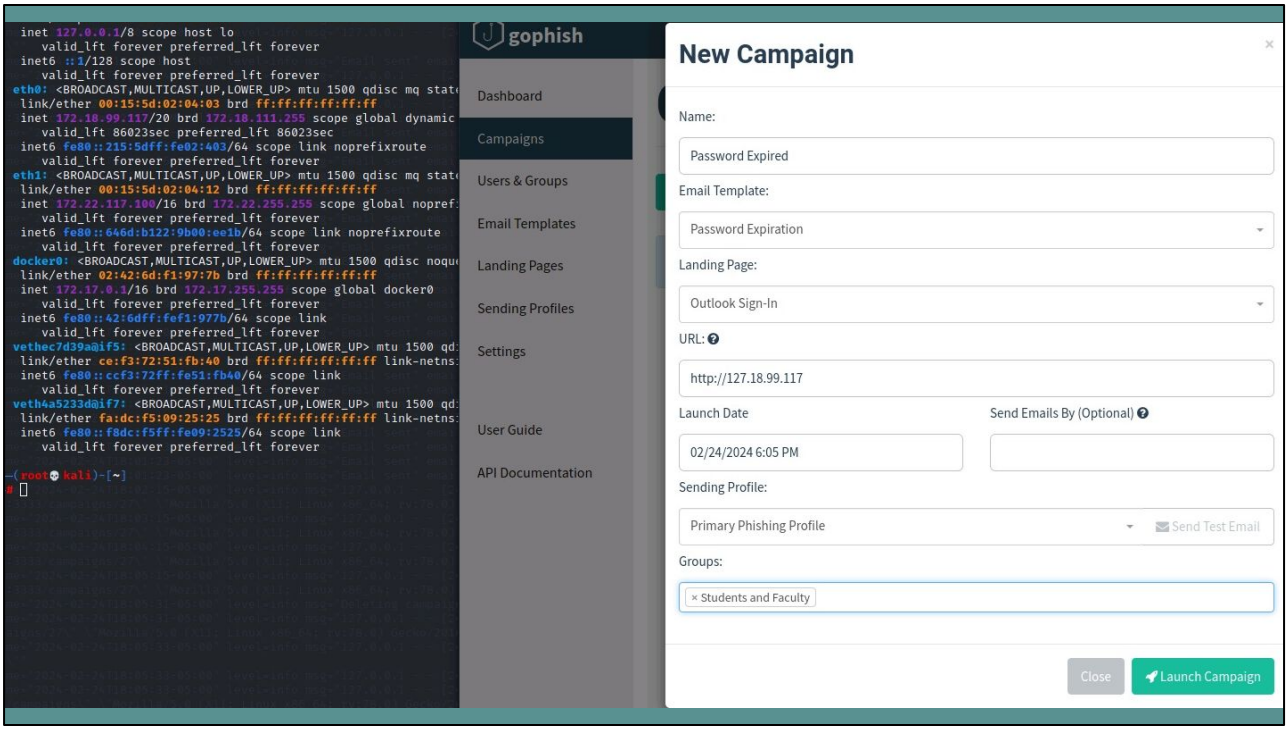
For my demo, I've kept things simple, but your options here are fairly open. You can create and customize and email from scratch, or import an existing email to use it's HTML coding as the starting framework (layout/images/headers/footers/etc). For either option, you just need to ensure the link to your landing page is properly specified. To do that, you add in the link as {{.URL}} displayed here (point out w/ cursor); this is how recipients will be directed to your campaign's associated landing page, which is created next.



Landing page. This is where recipients will be taken if they click your link. If you are spoofing an existing service, gophish gives you the option to import that page and use the code as the basis for the false page which makes it easy for a user to mistake it for the real thing. The source button lets you switch between the HTML code and the visual.

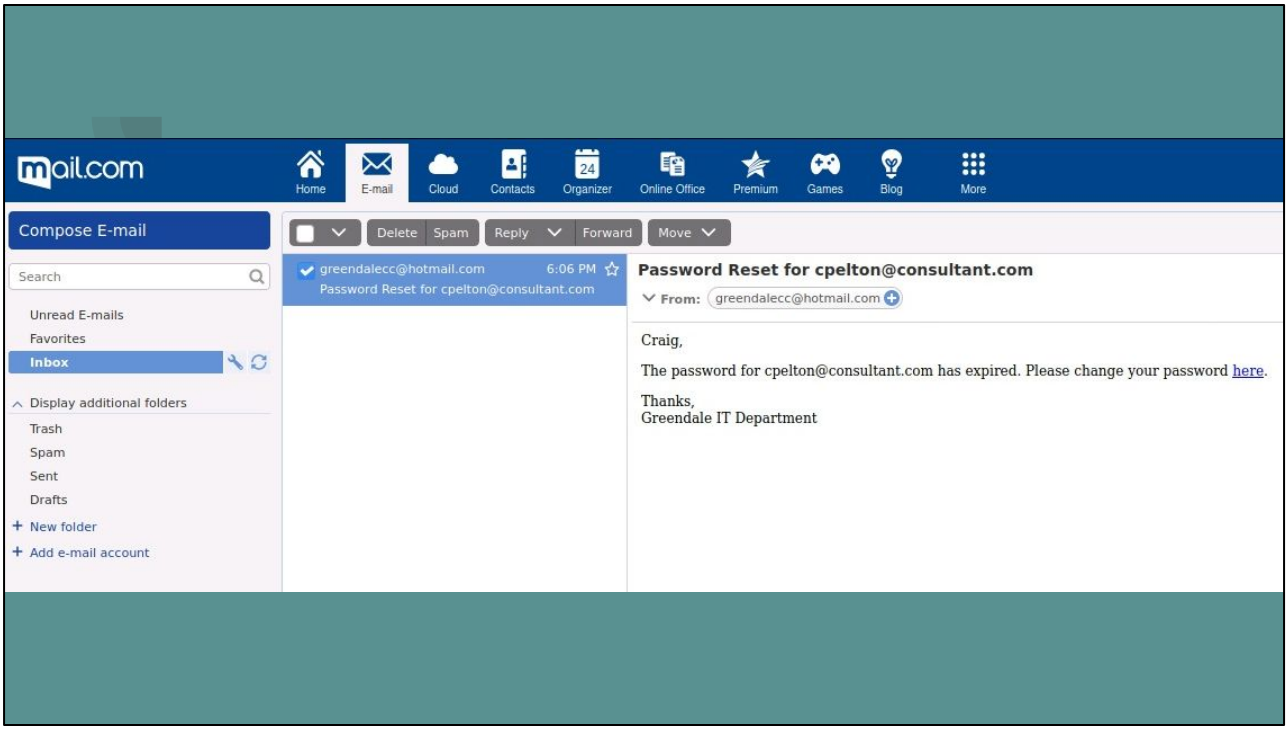
Checking the boxes for capture submitted data and capture password allow you to see what was keyed in by the visiting user, not just that they did or did not key in credentials on the landing page.

The redirect link is where they will be taken after submitting from your landing page, usually this will be the real site being spoofed so the user is less likely to become suspicious.

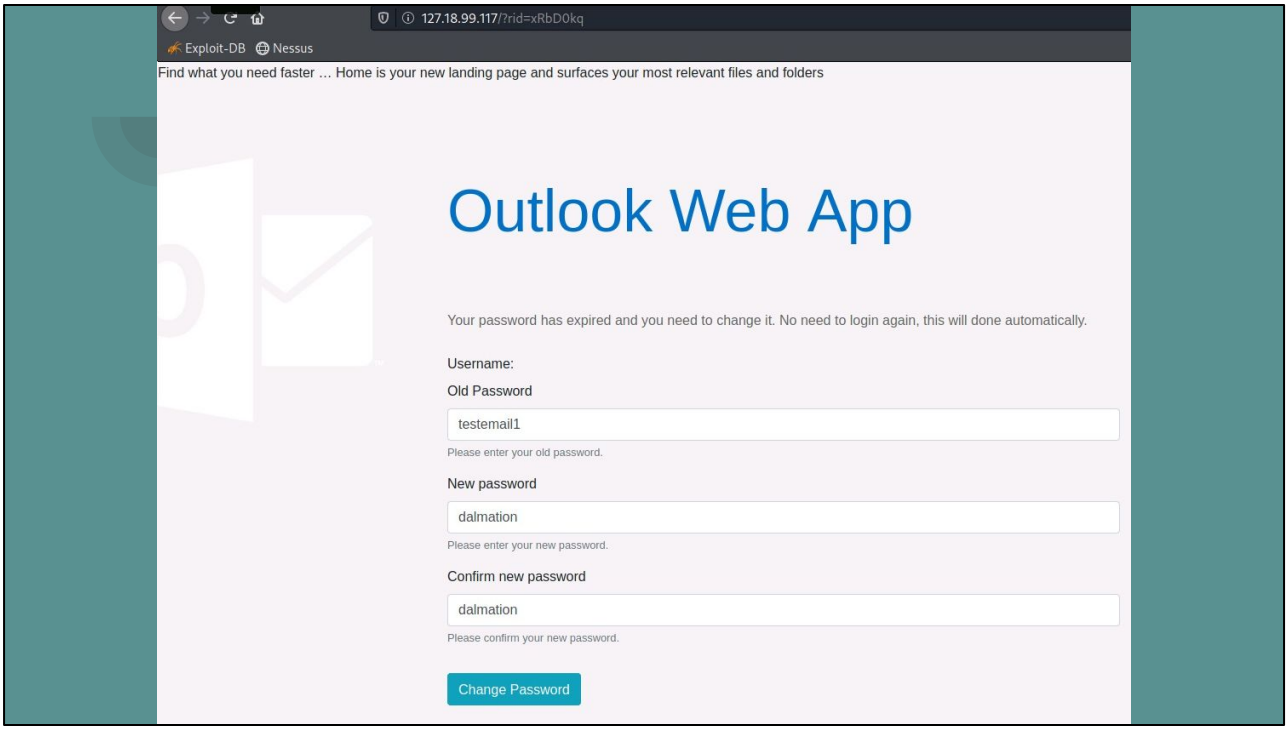


Once you have set up all the previous sections, you can create your campaign. Title it, then choose your template email, the landing page to use, the sending profile, and the groups/users who will be receiving the emails. Your URL will need to match your external IP in order for the links to properly direct the recipient to your landing page and subsequently update your reports in the dashboard.

Once you click launch campaign, gophish sends out the messages as configured.



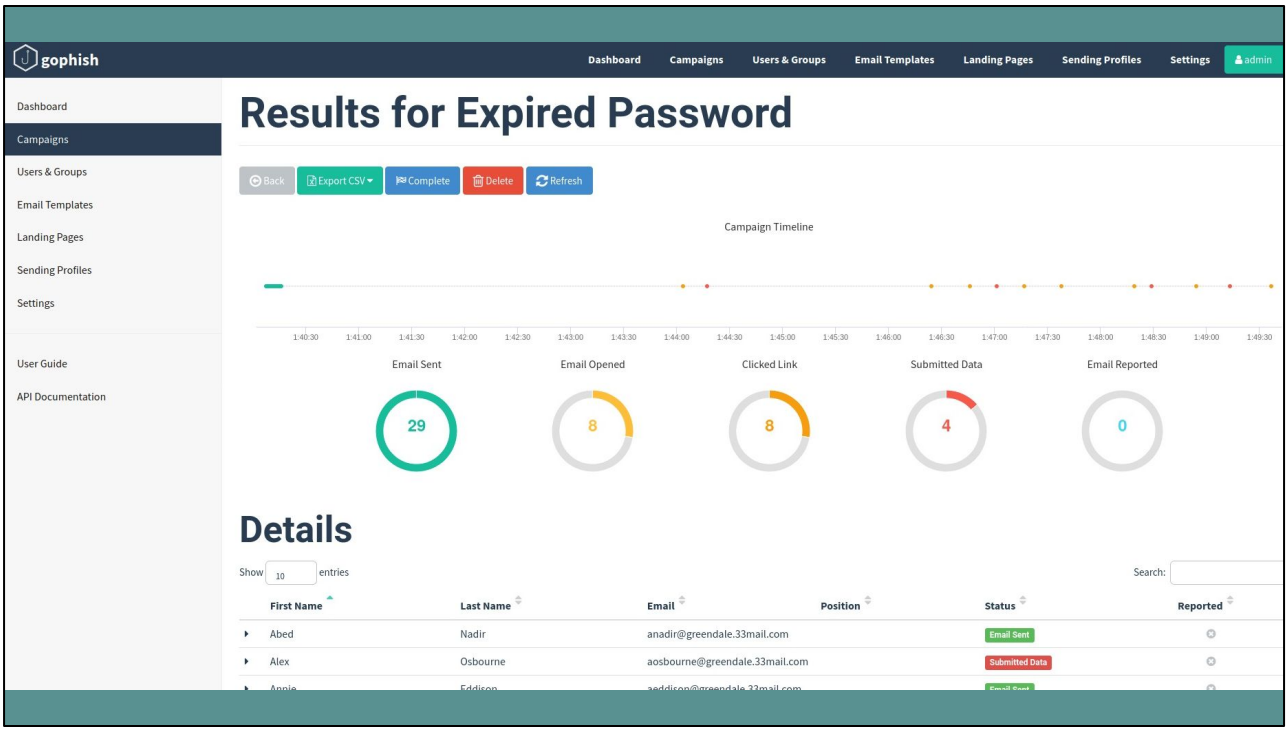
Once sent, here is what the email looks like to the recipient. You can see it has filled in the first name and email address for this specific user so it's more personalized. And if you click the link, …



They are brought to your landing page. As you can see in the address bar, this is where the IP address we looked up for the URL comes into play. If they're paying attention, this would be a clue to users that the site is not legit and they should leave/report the phishing email.
Any credentials keyed here are captured and sent back to gophish for reporting. And the user is redirected to the outlook sign in page after submitting (leading them to believe they have completed the password change and are good to sign in).

Dashboard/Results

Speaking of reporting, let's take a look at what the dashboard looks like once users have interacted with the emails.



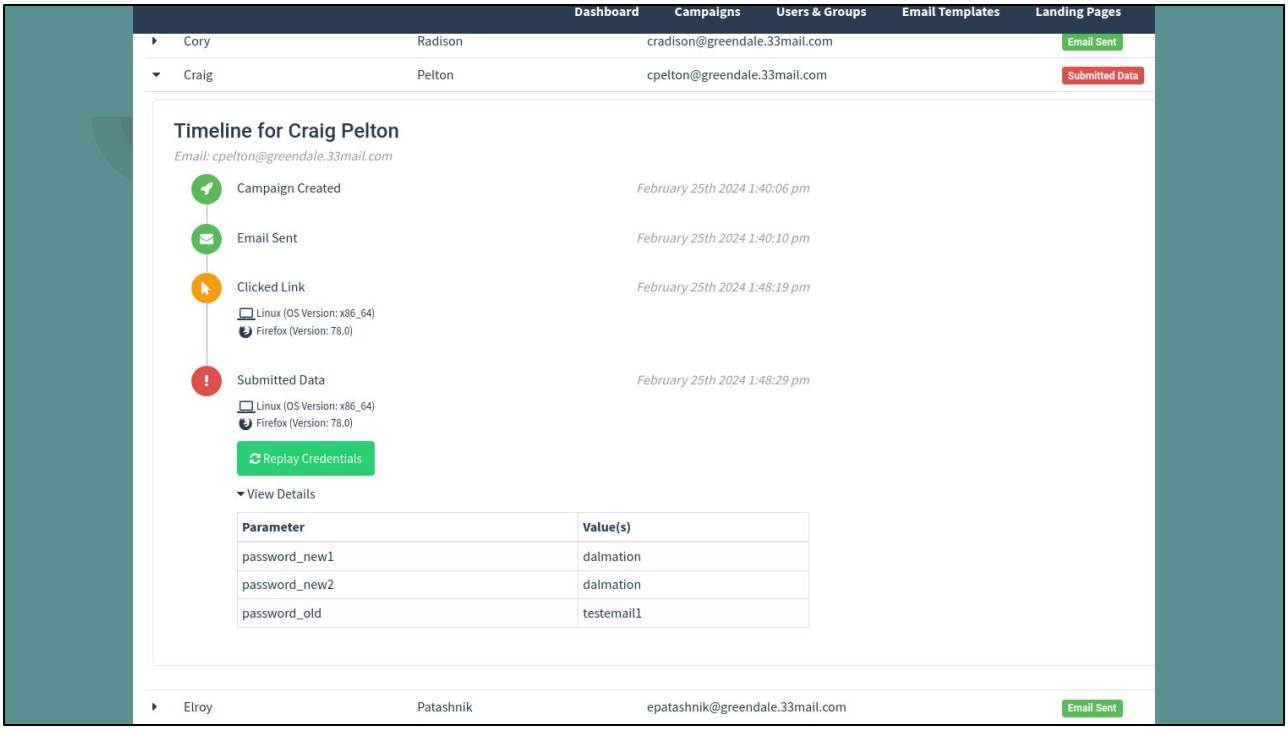
As your campaign progresses, you can view details on the campaign page or the dashboard (The dashboard will combine all active campaigns, so if you have more than one running, you can drill down into each one individually on the campaigns tab).The dashboard will update to show the portion of users who have opened/clicked/submitted/reported and these are color coded for different levels of concerning interaction (clicked orange, data submitted red, etc).

Now, because of the email client I used (tested both with mail.com and temporary emails routed through gmail), the "email opened" did not report back for this demo b/c of some default security features that are in place and cannot be changed; However, an organization's own mail server/client may or may not have those security features built in, so having access to that data can be useful situationally to see initial engagement for those who may not have clicked the link or reported the email. Either way, the most concerning behaviors of clicking the link and submitting credentials, are always going to be reported back.

Additionally, for the purposes of my demo, because I was not working from an email server I had admin controls over and access to a phishing reports box, I was unable to activate logging of the reporting tracker. This would be done within an organization by updating gophish with the IMAP details of where reported emails are forwarded once a user flags them. And using those credentials, gophish will check the reporting inbox and update this portion of the dashboard accordingly.

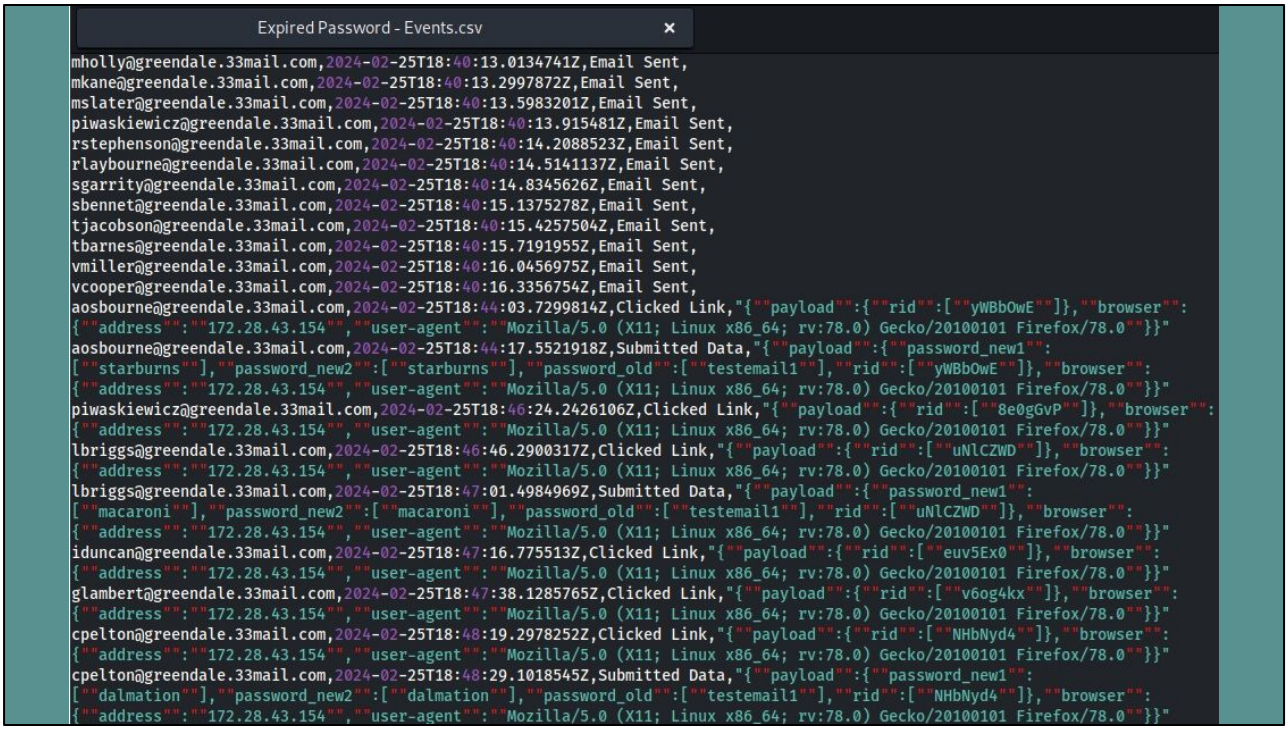
You can hover over data points on the timeline to see who took what action at a given

time. And…



Individual users can be expanded to show activity and timestamps each step of the way. If they keyed in credentials, you can even replay those credentials, which will pup up a box where you can enter a real website of your choosing to plug in and test out the credentials they submitted in case it's been reused for other logins.

At the top of the campaign details pictured on the prior slide, there is an option to export the dashboard data to a .csv file…

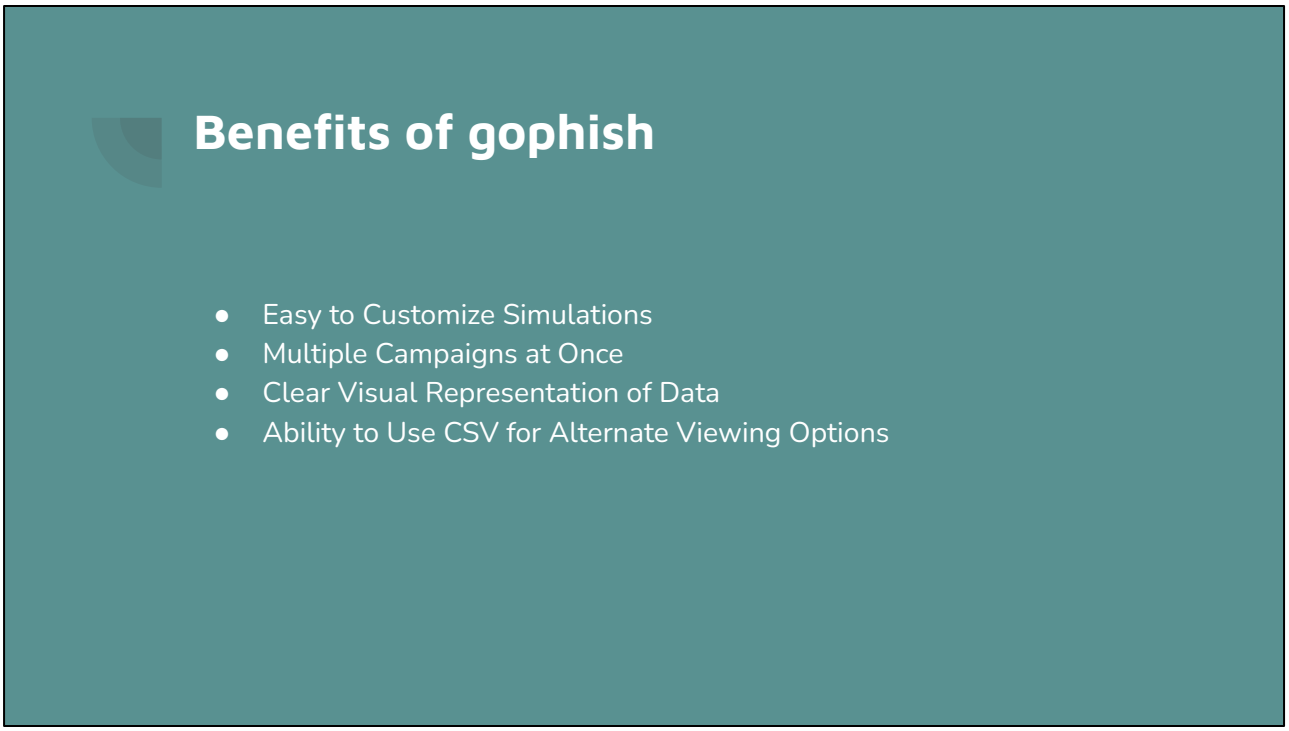


…That will give you an output in this format if you want to drill down a little further. This report contains the user info, when the phishing email was sent, status of link clicked or not, timestamps of interactions, what browser was used to access the link, what IP address they are coming from, and if data was submitted, what was keyed into those fields.

It's worth noting that, while not part of today's presentation, there are a few open source viewers out there that have been created to take this data and display additional visuals, such as a map of the IP address locations or a breakdown of access methods (browser, mail app, etc).

Organizational Benefits

So, why simulate phishing emails and why use this simulator?



Gophish has
-easy to customize simulations that allow incorporation of emerging trends in social engineering, or make adjustments so an email or landing page could say, mimic a new vendor for the company.
-Multiple campaigns can be run at once tto see if certain teams/ departments are more or less susceptible to attacks or if different types of emails are more likely to result in interaction.
-Clear, visual representation of data means you can take those results and present findings to the C-suite or any others who need to be included in updates regarding security of the company. They could also be integrated into future training initiatives to demonstrate the extent to which there are concerns within the organization since graphics are going to get the idea across better to someone who may not have the technical expertise to understand the raw data.
-And gophish gives you the ability to export and use the raw data with other visualization interfaces if you prefer a different layout or additional graphs.

Benefits of phishing simulations

- Knowledge Assessment
- Create Targeted Training Initiatives
- Heightened Awareness
- Strengthen Organizational Security Mindset

Simulating phishing attacks are useful, first of all, in defining the baseline of your organization's knowledge, awareness, and susceptibility to attack. Once that baseline is established, you can build a focused training program with the data to back up why you're training on the things you're training. You'll also be able to highlight successes to point out areas in which users are already doing well. ((I'm a big believer that positive reinforcement for successes goes further than punitive action for failure, because you don't want to discourage someone from speaking up if they fall victim to an attack, they need to let someone know asap)).

Conducting regular simulations keeps the threat front of mind for employees so they are less likely to fall victim to a real attack.

Overall, it is important for members of an organization to be aware of the threats out there so they can properly react and report suspicious activity. A company that has a strong security mindset is going to be a more difficult target for attackers. Human error is the most frequently exploited weakness, which is why social engineering attacks are as common as they are. So strengthening awareness and simulating attacks so employees know the process in the event of a real attack, make a significant impact to the overall security of an organization.

And that's it for me. Thank-you for your time.

Sources

https://ranjaniitian.medium.com/gophish-phishing-simulation-guide-linux-open-source-smtp-361a496ac7e0

https://docs.getgophish.com/user-guide/installation

https://phishgrid.com/blog/top-10-best-phishing-tools/#faq-question-1684146397500

https://go.dev/doc/install

https://www.youtube.com/watch?v=r-Q_rIlv6yo

https://github.com/gophish/gophish/issues/2813

https://www.inboxroad.com/email-deliverability/how-to-find-smtp-server-address-a-comprehensive-guide-for-email-configuration-and-troubleshooting/#:~:text=Log%20in%20to%20your%20email,the%20outgoing%20mail%20SMTP%20settings.

https://github.com/gophish/gophish/issues/2440

https://github.com/gophish/gophish/issues/2161

https://phishgrid.com/blog/how-to-design-a-phishing-email-simulation/