Phishing

## Summary

Running a real-life phishing campaign requires an email server and domain you control. That level resources is beyond the scope of labs for this class.

The half of this lab will focus on SPF, DKIM, and DMARC controls. These controls allow an email recipient to assess the validity of the sender.

The second half of the lab will generate a phishing story to hook your victim.

## Tools/Resources

Parrot: dig

Websites:

SPF lookup <https://www.kitterman.com/spf/validate.html>

Dmarcian: <https://dmarcian.com/>

## Tasks (Email controls)

1. Use the dig command to locate SPF and DMARC records for the following domains. Provide screenshot of the command line interaction
   1. cs.unh.edu
   2. kengraf.com
   3. Some other domain of your choice
2. Use the Dmarcian web site to evaluate a web domain of your choice.

## Tasks (Phishing story)

1. Select target (kmh722@unh.edu)
2. Create phishing email story. The best stories are targeted and compelling. Google, LinkedIn, and social media are good sources. My social media engagement is limited. Given that there more than one Ken Graf in the world I was born in Buffalo, NY and attended schools in NY, FLA, SC, NH, and MA.
3. Email your story to the target, and copy it to your Canvas submission.

## Submission

Upload to Canvas a docx or pdf containing the control lookups and a copy of your phishing story.

## Walkthrough Guidance (Email controls)

Using the dig command (nslookup works too), return just SPF TXT records and no overhead text use:

dig txt domain-name.com | grep spf

SPF and DMARC records can also be found in DNS domains \_spf.mydomian.com and \_dmarc.mydomain.com

What IP addresses are allowed by SPF to send @unh.edu email? UNH leverages SPF references

dig txt unh.edu | grep spf

unh.edu. 300 IN TXT "v=spf1 include:%{i}.\_ip.%{h}.\_ehlo.%{d}.\_spf.vali.email ip4:54.240.121.247 ip4:54.240.121.248 ~all"

Which requires a second DNS lookup replacing the {i} {h} and {d} values. Vali.email is a vendor providing SPF and DMARC management services.

└──╼ $dig txt 132.177.4.32.\_ip.unh.edu.\_ehlo.unh.edu.\_spf.vali.email +short

"v=spf1 ip4:132.177.0.0/16 -all"

└──╼ $dig txt 132.177.4.32.\_ip.cs.unh.edu.\_ehlo.cs.unh.edu.\_spf.vali.email +short

"v=spf1 ip4:132.177.4.32 -all"

-all (hard fail) email is not authorized, reject.

~all (soft fail) email is probably not authorized, mark as suspicious or spam.

Email behavior can also be defined with DMARC

dig txt \_dmarc.unh.edu +short

"v=DMARC1; p=quarantine; rua=mailto:dmarc\_agg@vali.email;"

p=none, p=quarantine, p=reject

How do email campaign companies like mailchimp send valid email on the behalf of unh.edu? Each sending source has its own key pair. The email has a record pointing to a selector. The public key is managed in unh.edu DNS. The email recipient can download the public key and validate the signature in the email.

## Walkthrough Guidance (Phishing story)

An complete phishing attempt is NOT required. Just a good story/appeal.

Can use UNH or personal email to send the story.

Good stories: Something from my past, cyber industry related, or personal interests (Bills, Chess, Golf, Billiards)

Bad story: My late homework is attached, this assumes your email account has been compromised.