Jordan Schalter

IT417

.TOMA

LAB8

#14

The acronym ICMP stands for internet control message protocol Which essentially sends information to check for connection problems, then sends a message back indicating that the connection is either fine or delivers a failure message if it cannot be reached.

#15

I anticipate that Wireshark would be a necessary tool for cybersecurity, and it possesses an assortment of purposes. The security tool Wireshark has proven useful in this lab as I am sure that it is also accurately useful in the professional cyber security environment. Analyzing suspicious activity, following connections, and additional objectives are available options.

#27

88.208.7.193

Reroutes to rig ek, and this is via connection to a bogus dating site that utilizes  hookads.

#28: datitngforllives.info

#29: 00:08:02:1c:47:ae

#30

185.56.233.186 traito.tivill.com  
88.208.7.196 datawebglobalgroup.com

#33a

Domain: [www.needgrow.info](http://www.needgrow.info) is being shown.

#34

It appears it also leads to rig ek. Although I can't find anything to suggest that it is currently functioning, the website is untrustworthy through my eyes by default.

#36  
Digital Signature Trust Co, DST Root CA x30  
<http://isrg.trustid.ocsp.identrust.com><http://apps.identrust.com/roots/dsroot><http://crl.identrust.com/DSTROOTCAX3CRL>

Encrypt authority x30 with the numbers 190104153927z  
<http://oscp.int-x3.letsencrypt.org><http://cert.int-x3.letsencryhpt.org><http://cps.letsencrypt.org>

When the danger is encrypted the blue team has to do more work (which they generally complain about doing, and the blue team prefers unoriginality in that aspect, lol ;) The danger is encrypted, and that is what would make this challenging (not like it would be any easier for blue team, maybe if they were red team, they would care more about originality, lol.)

#37

Although, I am not all that sure if I \*really\* believe it is legitimate, and I hope for the sake of the internet after doing this lab that it is, but, honestly, I think this is some weird fake dating site for freakishly large humans or something weird like that. No but really, the sole purpose of this site is to infect and extract information from unsuspecting, and hopefully innocent non subjective users.

#38:

Indication that the file has been downloaded to their computer is incoherently futile.

A screenshot of a computer

Description automatically generated

#65

“Photographer Evidence”

A screenshot of a computer

Description automatically generated

(This is my greatest photo ever)

#71

The hash is not particularly secure. There were signs of evil within pcap file previously in the lab. It might happen that the virus possesses a variant of the same hash throughout inclusion. The download in my opinion is harmful since at one point previously it includes malware, and it may still.

#72

The reason why blue team strives to study data from numerous sources, and analyze the same thing repetitively, is the same reason why I do not think they are full proof. ( 😊 )

#74

To validate a 128-bit hash code, an MD5sum is employed.

The only method is if it is downloaded from reputable sources, and the blue team should not be employing this.

#75

This lab sucked.