DIGITAL FORENSICS

Metadata & Steganography
Officer Applications

- Secretary
- Treasurer
- https://goo.gl/uexOyu
- Applications close this Friday (11/18)
Metadata

- “We kill people based on metadata.” - General Michael Hayden
- Data about data
- Potentially obscure, generally less well known, and frequently a wealth of knowledge
HTML Meta tags

- Author - who wrote the webpage
- Generator - what software the site is running
- Possible external verification - Google analytics
robots.txt

• Tells web crawlers what NOT to index
• Might be exactly what we want to look at
• https://google.com/robots.txt
404 Pages

- Shows when a requested URL doesn’t exist
- If a custom 404 isn’t set, leaks information about the web server
- [http://acmutd.co/awerlkasndfjsar](http://acmutd.co/awerlkasndfjsar)
.well-known

- Web directory designated for “well-known” URLs
- Uncommon, but in use
- [https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml](https://www.iana.org/assignments/well-known-uris/well-known-uris.xhtml)
Authentication Primer

• Primary way to authenticate identity is with public/private key pairs. With some clever math, I can prove I own a private key associated with a public key you own.

• Public keys are identifying information
HTTPS

• Utilizes SSL Certificates to verify websites
• Certificates, as such, can contain a wealth of information about the site they are issued for
• Commonly used in CTF Problems to hide the flag
Certificate Fields

Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: Texas
Locality Name (eg, city) []: Richardson
Organization Name (eg, company) [Internet Widgits Pty Ltd]: UTD Computer Security Group
Organizational Unit Name (eg, section) []: Password Inspection Bureau
Common Name (e.g. server FQDN or YOUR name) []: Chief Password Inspector
Email Address []: utdcs@gmail.com
csg.utdallas.edu Certificate

CN = csg.utdallas.edu
OU = General
O = The University of Texas at Dallas
Object Identifier (2 5 4 9) = 800 West Campbell Road
L = Richardson
ST = TX
Object Identifier (2 5 4 17) = 75080
C = US
Domain Name System (DNS)

- Maps easy to remember domain names (google.com) to hard to remember IP addresses (216.58.218.110)
- More than just web browsing!
- DNS Records - Specific types of mappings
Common DNS Records

- A - Standard record, maps to IPv4 address
- AAAA - IPv6 version of A
- CNAME - Canonical Name, an “alias” for another record
- MX - Mail exchange, directs to mail servers
- TXT - Arbitrary Text
dig (domain information groper)

- Performs DNS lookups
- `dig (@servername) domain (type)`
- Worth trying “any” as type
- `dig csg.kulinacs.com txt`
- Note: csg.kulinacs.com does not resolve in browser
WHOIS

- Maps a domain to WHOIS responsible for it
- Maybe hidden with services like WHOIS guard
- `whois utdallas.edu`
- `whois kulinacs.com`
OpenSSH

- Secure Shell (ssh)
- One of the most popular SSH implementations
- Utilized for remote administration
- Server authenticates with a key that is accepted at first connect
- Generally thought of as verifying the “fingerprint”
Enumerating SSH Keys

- `ssh-keyscan [host]`
  - Returns all keys offered by the server (generally ECDSA, RSA, and ED25519)
- `ssh-keygen -l`
  - Converts public keys to their fingerprints
SHODAN

• https://www.shodan.io
• Massive crawler of the internet
• From ekoparty CTF:
EXIF Data

• Primarily “cataloging” information for photo
• Can include, but is not limited to:
  • Date and time,
  • Settings
  • Location
EXIF Tool

- Prints metadata
- Software tag
- Creation Date
- GPS Location
- Camera Model Name
John McAfee (The Awful Antivirus guy)

- In 2012, wanted in Belize for questioning for possible involvement in a murder
- Flees to Guatemala
- VICE news interviews him, posts a picture on their website
- Picture contains EXIF GPS location
Steganography

• The foil to Cryptography
• Primary goal is to hide the fact information is being sent
• Current most practical usage is steganographic protocols used to bypass internet filters, i.e. Tor Relay Bridges (Pluggable Transports)
Goals of Steganography

- Maintain file entropy
- Make no change big enough to be recognized easily
- Maintain the data embedded. (Bad news for compression)
Outguess

- For JPEG images
- Bad with compression (DCT)
- Can be keyed
- `outguess -d secrettext.txt input.jpg secret.jpg`
- `outguess -r secret.jpg recovered.txt`
Comparison

ImageMagick

compare secret.jpg input.jpg -compose src composed.jpg
Steganography “in the wild”

https://imgur.com/gallery/hz4gva