Mason Competitive Cyber

Antiforensics - Covering Your Tracks

Upcoming Competitions & Events

- PatriotCTF
  - Saturday
  - HUB rooms 1-5
  - patriotctf.gmu.io
- Shmoocon First Round of Tickets
  - Noon today (already sold out RIP)
  - DC in January
  - Schmooze a Student
- RUCTFE
  - Nov 10
  - Online Attack/Defense

Antiforensics

- Forensics
  - Logs
  - Forensic artifacts
  - Network Traffic/Logs
  - Malware Analysis
  - Timelining
- Antiforensics
  - Making that ^ more difficult

Antiforensics on your own systems

- Why?
  - Privacy
  - Sketchy things
  - Sensitive dat

Antiforensics on your own systems

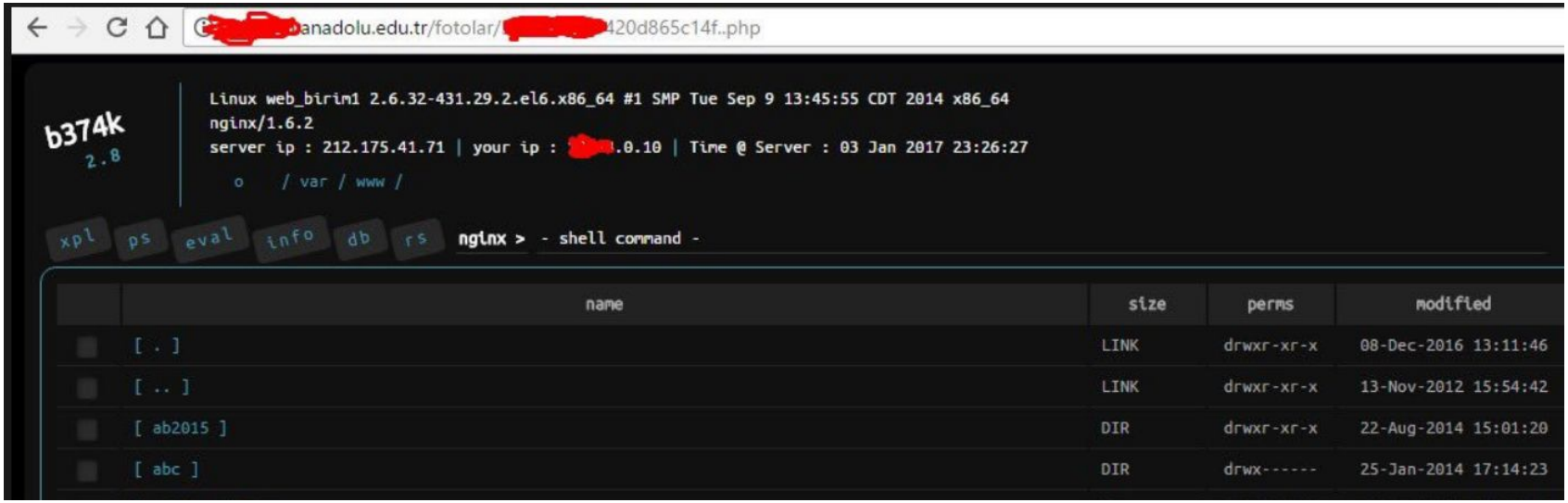
- Encryption
  - Local
    - sticky keys hack
    - mac single user mode
  - Network Protocols
    - sniffing, MiTM
    - Tor/VPN
- Data Destruction
  - Digital
  - Magnetic
  - Physical
- Don’t do things on main system
  - Raspberry Pi, server somewhere, compromised website
  - TAILS

Rookie Moves

- Binary that runs on startup
- Getting caught by AV
- Using RDP without clearing event logs
  - teamviwer, VNCs, etc.
- Renaming and/or moving files to keep secret
  - File Carving
- Move to Trash
  - U fool
  - Easily recovered. MacOS even stores the filepath where it came from
- Move to Trash + empty trash
  - File marked to be overwritten. Until that happens recoverable
- Leaving command history on Linux
  - Use a different shell for max sneakiness

Steganography

- Webshell in an image
- PHP in JPEG EXIF headers
  - exif_read_data



Fileless Malware

- Runs in memory
  - Doesn't exist when shut down
    - Can set to run on startup
  - Evade AV signatures
  - PS Empire, WMI
- Capturing RAM
  - Volatility

Forensic Artifact Fuckery

- Timestomping
  - NFTS
    - Created, Accessed, Modified, Metadata Changed
    - $STDINFO and $FILENAME
  - Disabling Last Accessed
    - HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate
- Deleting them
  - Files
    - Thumbnail cache, Bitmap cache, PSReadline
  - Registry, NTFS Reserved Folders ($Extend)

- Generate random activity
  - Some artifacts roll data

Destruction

- Encryption
- Wiping
  - overwrite files
  - overwrite Master Boot Record (MBR)
- Wipe patient 0
  - Initial method of compromise
  - Data exfiltration

Obfuscation

- Make code harder to read
  - Variable/function names
  - String manipulation

- Rookie Move: passing everything to one big IEX/eval/whatever
  - Eval + gzip + Base64 = PHP noob tier

- Invoke-Obfuscation
- Msfvenom
- Veil Framework

- Behavioral analysis

Practical Exercises

- New TCTF Challenges
  - Obfuscation Sensation (php)
  - Unzip
  - tctf.competitivecyber.club

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™

CRYPSIS™